POLÍTICA DE GESTÃO DA INFORMAÇÃO, PROTEÇÃO DE DADOS E CIBERSEGURANÇA

A Broliveira reconhece que a informação, os dados pessoais a que tem acesso e os sistemas digitais constituem ativos essenciais ao desenvolvimento da sua atividade de transporte rodoviário internacional de mercadorias.

A proteção da informação, os dados pessoais e os sistemas digitais é determinante para assegurar a continuidade do negócio, a confiança das partes interessadas, a resiliência operacional e a sustentabilidade da organização.

A presente Política estabelece os princípios e compromissos da Broliveira em matéria de gestão da informação, proteção de dados pessoais, confidencialidade, segurança da informação e cibersegurança, em articulação com o Código de Ética e Conduta, com o Sistema de Gestão da Qualidade, Ambiente e Segurança (SGQAS), com os procedimentos internos aplicáveis e com os requisitos legais e regulamentares em vigor.

A Gerência assegura a implementação desta Política, disponibilizando os recursos necessários à sua aplicação e promovendo a melhoria contínua das práticas adotadas. A presente Política aplica-se a todas as atividades, serviços, instalações, sistemas de informação e trabalhadores da Broliveira, bem como, quando aplicável, a fornecedores, prestadores de serviços e parceiros que tratem informação ou acedam a sistemas da empresa.

COMPROMISSOS

A Broliveira compromete-se a:

1. Conformidade, governação e gestão de risco

- Cumprir a legislação aplicável e outros requisitos relevantes em matéria de proteção de dados pessoais, segurança da informação e cibersegurança;
- Definir responsabilidades adequadas à estrutura e atividade da empresa, assegurando a articulação entre a Gerência, o Departamento de Tecnologias e Sistemas de Informação, os responsáveis de departamento e os trabalhadores;
- Adotar uma abordagem baseada no risco relativamente à informação, aos sistemas de informação e aos dados pessoais, promovendo medidas proporcionais ao nível de risco identificado.

2. Proteção da informação

- Proteger a informação da empresa, dos trabalhadores, clientes, e outros parceiros, assegurando a sua confidencialidade, integridade e disponibilidade;
- Promover a utilização adequada da informação, restringindo o acesso apenas a quem dele necessite para o exercício das respetivas funções e responsabilidades;
- Prevenir a divulgação, perda, alteração, destruição ou acesso não autorizado a informação.

3. Proteção de dados pessoais

- Tratar os dados pessoais de forma lícita, leal, transparente e apenas para finalidades legítimas, em conformidade com o Regulamento Geral sobre a Proteção de Dados – RGPD e restante legislação aplicável;
- Implementar medidas técnicas e organizativas adequadas para proteger os dados pessoais tratados pela empresa;
- Respeitar os direitos dos titulares dos dados e promover uma gestão responsável da informação pessoal.

4. Segurança dos sistemas e cibersegurança

- Proteger os sistemas de informação e os equipamentos utilizados na atividade da empresa contra acessos indevidos, utilização inadequada, perda de dados, falhas técnicas, ciberataques ou outras ameaças relevantes;
- Manter medidas de prevenção, deteção, resposta e recuperação adequadas, incluindo controlos de acesso, proteção antivírus, firewall, VPN, cópias de segurança, atualizações, monitorização e outras medidas definidas internamente;
- Promover a continuidade da atividade, assegurando a disponibilidade dos sistemas de informação essenciais ao funcionamento da empresa;
- Promover a identificação, comunicação e tratamento de incidentes de segurança da informação e de cibersegurança.

5. Utilização responsável dos recursos tecnológicos

- Promover uma utilização responsável dos sistemas, equipamentos, contas de acesso, correio eletrónico, internet, plataformas digitais e demais recursos tecnológicos disponibilizados pela empresa;
- Incentivar a utilização de ferramentas digitais, incluindo novas soluções tecnológicas ou de inteligência artificial, de forma responsável, proporcional, segura e alinhada com as orientações internas aplicáveis;

- Reforçar a responsabilidade individual de cada trabalhador na proteção da informação e na comunicação de incidentes, suspeitas ou situações anómalas que possam comprometer a segurança dos dados ou dos sistemas.

6. Sensibilização, monitorização e melhoria contínua

- Sensibilizar os trabalhadores para boas práticas de proteção da informação, privacidade, utilização segura dos sistemas e prevenção de riscos de cibersegurança;
- Definir, acompanhar e rever indicadores, objetivos e ações associados à gestão da informação, proteção de dados e cibersegurança, através dos instrumentos de gestão e monitorização aplicáveis;
- Promover a implementação de medidas de prevenção, mitigação e melhoria contínua em matéria de segurança da informação.

A concretização destes compromissos é suportada pelo Plano de Gestão QAS, onde são definidos e monitorizados os objetivos, metas e indicadores relacionados com a gestão da informação, a proteção de dados e a cibersegurança. As medidas a implementar são estabelecidas nos procedimentos internos da organização.

A presente Política é comunicada a todos os trabalhadores e partes interessadas relevantes, estando disponível para consulta.

A Política é revista sempre que necessário e, no mínimo, de três em três anos, de forma a assegurar a sua adequação ao contexto da organização, à evolução das suas atividades e ao desempenho alcançado.

12 de agosto de 2026

Elaborado por DTSI

Aprovado pela Gerência

(Assinatura)