POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. PROPÓSITO E ABRANGÊCIA

A Política de Segurança da Informação (PSI) da OMC GROUP Ltda. define regras e diretrizes para proteger os ativos de informação, garantir a conformidade legal (LGPD) e manter a confidencialidade, integridade e disponibilidade dos dados.

Baseia-se nas normas ISO/IEC 27001:2022, 27002:2005 e na Lei Geral de Proteção de Dados (Lei nº 13.709/18).

Aplica-se a todos os colaboradores, clientes e fornecedores.

2. SISTEMA DE GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

A OMC GROUP mantém um Sistema de Gestão de Segurança da Informação (SGSI) apoiado por políticas, procedimentos e controles aprovados pela Alta Direção.

Todos os colaboradores devem conhecer, compreender e cumprir os requisitos estabelecidos pela organização para proteção das informações.

Os documentos aplicáveis permanecem disponíveis para consulta por meio dos canais corporativos autorizados.

3. OBJETIVOS DO SGSI

O Sistema de Gestão de Segurança da Informação possui os seguintes objetivos:

- Proteger os ativos de informação da organização;
- Garantir a confidencialidade, integridade e disponibilidade das informações;
- Atender requisitos legais, contratuais e regulatórios;
- Reduzir riscos relacionados à segurança da informação;
- Garantir a continuidade das operações;
- Promover a conscientização dos colaboradores;
- Assegurar a melhoria contínua do SGSI.

4. REQUISITOS PRINCIPAIS

Todos os colaboradores e terceiros devem:

- Cumprir a Política de Segurança da Informação e os documentos complementares;
- Assinar os termos de confidencialidade aplicáveis;
- Reportar imediatamente incidentes de segurança da informação;
- Proteger adequadamente os ativos de informação sob sua responsabilidade;
- Seguir os controles definidos para acesso, tratamento e compartilhamento de informações;
- Cooperar com atividades de auditoria, monitoramento e conscientização.

5. TREINAMENTO E CONSCIENTIZAÇÃO

A OMC GROUP promove treinamentos periódicos de Segurança da Informação para todos os colaboradores, bem como ações de conscientização voltadas à proteção das informações e ao cumprimento dos requisitos internos, legais e contratuais.

6. CONTROLE DE ACESSO

O acesso aos sistemas, informações e recursos tecnológicos é concedido de acordo com a necessidade de trabalho e mediante autorização apropriada.

Os acessos são controlados, monitorados e revisados periodicamente, respeitando o princípio do menor privilégio.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação deve ser classificada e tratada conforme seu nível de sensibilidade.

Quando diferentes classificações estiverem presentes em um mesmo documento ou conjunto de informações, deverá prevalecer a classificação de maior criticidade.

8. GESTÃO DE CRISES E CONTINUIDADE

A OMC GROUP mantém processos de Gestão de Crises, Continuidade de Negócios e Recuperação de Desastres para preservar suas operações e proteger suas informações em situações que possam afetar a organização.

9. RESPONSABILIDADES

Colaboradores

- Cumprir os requisitos da PSI.
- Proteger as informações sob sua responsabilidade.
- Comunicar incidentes e situações de risco.

Gestores

- Garantir que suas equipes conheçam e cumpram a PSI.
- Apoiar ações de conscientização e segurança.

Tecnologia da Informação

- Implementar e manter controles técnicos de segurança.
- Monitorar e proteger os ativos tecnológicos.

Segurança da Informação

- Definir metodologias, controles e processos de segurança.
- Coordenar ações de conscientização.
- Apoiar a gestão de riscos, incidentes e crises.

10. UTILIZAÇÃO DOS RECURSOS TECNOLÓGICOS

Os recursos tecnológicos disponibilizados pela OMC GROUP destinam-se prioritariamente às atividades corporativas.

São proibidas atividades que possam comprometer a segurança das informações, a disponibilidade dos serviços ou o cumprimento de requisitos legais e contratuais.

11. SEGURANÇA FÍSICA

A organização mantém controles de acesso físico às suas instalações, incluindo áreas com diferentes níveis de restrição, além de regras para visitantes, registro de acessos e proteção de áreas críticas.

12. BACKUP E CONTINUIDADE

Os dados e sistemas corporativos são protegidos por processos de backup e recuperação que visam assegurar a disponibilidade das informações e a continuidade das operações.

13. CONDUTA E CONFIDENCIALIDADE

Todos devem adotar práticas seguras no tratamento de informações, incluindo:

- Política de mesa limpa;
- Proteção de documentos e telas;
- Uso adequado dos recursos corporativos;
- Não divulgação de informações confidenciais sem autorização.

14. DOCUMENTOS COMPLEMENTARES

Esta Política é complementada por procedimentos, normas e instruções de trabalho do Sistema de Gestão de Segurança da Informação, incluindo classificação da informação, controle de acessos, backup, gestão de incidentes, gestão de fornecedores, continuidade de negócios e demais documentos aplicáveis.

15. PENALIDADES

O descumprimento dos requisitos desta Política poderá resultar em medidas disciplinares, administrativas e legais, conforme a gravidade da ocorrência e a legislação aplicável.

16. REFERÊNCIAS LEGAIS

- Lei Geral de Proteção de Dados (LGPD);
- ISO/IEC 27001;
- ISO/IEC 27002;
- Requisitos TISAX (VDA ISA).

24. HISTÓRICO DAS ALTERAÇÕES

DATA	REVISÃO	HISTÓRICO
10/11/2025	0000	Elaboração
24/09/2026	0001	Revisão e atualização da versão de divulgação, incluindo Objetivos do SGSI, Gestão de Crises e Continuidade, responsabilidades revisadas e documentos complementares.



MARCIO SILVEIRA CAMPOS