POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO (TI)

POL.TCM.005.COMP REV.01-10/25

1. INTRODUÇÃO

A Política de Tecnologia da Informação (TI) do **GRUPO TCM** tem como propósito estabelecer as diretrizes e responsabilidades para o uso adequado dos recursos tecnológicos, assegurando a **proteção dos ativos de informação**, a **continuidade operacional**, a **conformidade legal e regulatória** e a **prevenção de riscos** relacionados à segurança da informação e à privacidade de dados.

Esta política é de **cumprimento obrigatório** por todos os colaboradores, prestadores de serviços, parceiros e terceiros que utilizem os recursos tecnológicos e informações sob responsabilidade do GRUPO TCM.

2. OBJETIVOS

a) Garantir o uso ético, seguro e eficiente dos recursos de tecnologia da informação;
b) Proteger os **ativos de informação** quanto à **confidencialidade**, **integridade** e **disponibilidade**;
c) Minimizar riscos de incidentes cibernéticos, vazamento de dados ou uso indevido dos sistemas corporativos;
d) Assegurar conformidade com a **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**, **Código Penal Brasileiro**, **leis trabalhistas**, **normas ISO 27001** e outras aplicáveis;
e) Definir responsabilidades e condutas esperadas de todos os usuários de tecnologia no GRUPO TCM;
f) Promover uma **cultura de segurança da informação** e de respeito às boas práticas digitais corporativas.

3. ABRANGÊNCIA

Esta Política aplica-se a **todos os colaboradores, prestadores de serviço, fornecedores, estagiários, consultores e parceiros** que utilizem recursos tecnológicos ou tenham acesso às informações do GRUPO TCM, independentemente de meio, formato ou local de armazenamento (físico ou digital).

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade:** apenas pessoas autorizadas podem acessar informações específicas.
- **Integridade:** as informações devem ser mantidas completas, íntegras e livres de alterações indevidas.
- **Disponibilidade:** os sistemas, dados e serviços devem estar acessíveis a usuários autorizados sempre que necessário.
- **Autenticidade:** os acessos e transações devem ser rastreáveis e associados a um usuário identificado.
- **Legalidade:** o uso da tecnologia deve respeitar a legislação vigente e os direitos de terceiros.

Elaborado por:	Revisado por:	Aprovado por:	
Departamento Auditoria e Qualidade	Rubens Copche	Thais Tucunduva	
Data: 01/10/2025	Data: 06/10/2025	Data: 07/10/2025	

- **Responsabilidade:** cada colaborador é responsável pelo uso correto e ético das ferramentas tecnológicas.

5. RESPONSABILIDADES

5.1. Dos Colaboradores

- Cumprir integralmente esta política e as normas complementares;
- Utilizar os recursos de TI exclusivamente para fins profissionais;
- Preservar a confidencialidade das informações acessadas;
- Não compartilhar senhas ou dispositivos de acesso;
- Comunicar imediatamente à área de TI qualquer incidente de segurança, perda ou suspeita de acesso indevido;
- Responsabilizar-se por prejuízos causados por uso indevido, negligente ou doloso dos recursos tecnológicos.

5.2. Dos Gestores

- Atuar como exemplo de conduta segura e ética;
- Garantir que os colaboradores sob sua gestão estejam cientes e cumpram esta Política;
- Exigir a assinatura de **Acordo de Confidencialidade (NDA)** antes de conceder acesso a informações sensíveis;
- Comunicar imediatamente à TI e ao RH desligamentos, transferências ou alterações de função que impliquem mudança de acesso;
- Apoiar as ações de conscientização, treinamento e auditoria em segurança da informação.

5.3. Da Área de Tecnologia da Informação

- Implementar e monitorar controles de segurança da informação e privacidade de dados;
- Configurar e manter os sistemas de forma segura, conforme padrões técnicos e legais;
- Garantir backups regulares e testados de dados críticos;
- Bloquear imediatamente acessos de usuários desligados ou sob investigação;
- Implantar mecanismos de detecção e resposta a incidentes;
- Monitorar o ambiente tecnológico, gerando relatórios e indicadores de desempenho, disponibilidade e segurança;
- Realizar auditorias técnicas periódicas e correções preventivas;
- Garantir que novos ativos (softwares, equipamentos, aplicações) sejam verificados contra códigos maliciosos antes da implantação;
- Definir regras formais para instalação de software, hardware e uso de dispositivos móveis;
- Manter registros auditáveis de retirada, transporte e descarte de mídias e ativos.

6. MONITORAMENTO E AUDITORIA

Para assegurar o cumprimento desta Política, o GRUPO TCM poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões de rede e dispositivos móveis;
- Registrar e auditar atividades de acesso e uso da rede, internet, e-mail e sistemas corporativos;
- Realizar inspeções físicas e lógicas em equipamentos da empresa;
- Bloquear, restringir ou suspender acessos e conteúdos considerados inadequados, ilícitos ou que representem risco de segurança;
- Fornecer informações obtidas por auditoria ou monitoramento quando solicitado judicialmente ou pela diretoria.

O uso dos recursos tecnológicos implica concordância integral com este monitoramento.

7. USO DO CORREIO ELETRÔNICO

É **proibido** utilizar o e-mail corporativo do GRUPO TCM para:

- Enviar mensagens que exponham a empresa a riscos legais, morais ou de imagem;
- Enviar ou divulgar informações confidenciais sem autorização;
- Utilizar identidade, login ou endereço de e-mail de terceiros;
- Transmitir mensagens com conteúdo ofensivo, discriminatório, obsceno, político ou ilegal;
- Enviar correntes, spam, arquivos executáveis ou materiais sem relação com o trabalho;
- Apagar mensagens que possam estar relacionadas a auditorias, investigações ou demandas legais.

As comunicações eletrônicas são patrimônio do GRUPO TCM e poderão ser auditadas.

8. USO DA INTERNET

A internet deve ser utilizada de forma ética, responsável e voltada exclusivamente a fins profissionais. São **vedadas** as seguintes condutas:

- Acessar sites com conteúdo ilegal, obsceno, discriminatório ou não relacionado às atividades da empresa;
- Instalar programas, extensões ou aplicativos sem autorização da TI;
- Compartilhar arquivos corporativos em plataformas externas sem aprovação;
- Tentar burlar mecanismos de segurança, proxy ou firewall;
- Realizar downloads de fontes não confiáveis.

O GRUPO TCM poderá restringir o acesso a sites e conteúdos, monitorar o tráfego e registrar logs para auditoria e conformidade.

9. IDENTIFICAÇÃO, SENHAS E ACESSOS

- Cada usuário possui uma identificação individual, pessoal e intransferível;
- É proibido compartilhar logins, crachás, tokens, senhas ou certificados digitais;
- As senhas devem ser complexas, trocadas periodicamente e nunca repetidas;
- O uso indevido ou falsificação de identidade constitui **crime (art. 307 do Código Penal)**;
- O RH deve comunicar imediatamente à TI os desligamentos para bloqueio de acessos;
- O colaborador que esquecer a senha deverá solicitar formalmente nova credencial.

10. PROTEÇÃO DE DADOS E LGPD

O GRUPO TCM compromete-se a cumprir integralmente a **Lei Geral de Proteção de Dados Pessoais (LGPD)**, adotando controles técnicos e administrativos adequados para proteger informações pessoais sob sua custódia.
Todos os colaboradores têm o dever de **zelar pela privacidade e proteção de dados pessoais** de clientes, fornecedores e demais partes interessadas.
O tratamento de dados deve observar os princípios de **finalidade, necessidade, transparência e segurança**.

11. DISPOSIÇÕES GERAIS

- A segurança da informação é responsabilidade de todos e deve ser incorporada à cultura organizacional;
- O descumprimento desta Política pode resultar em **advertência, suspensão, desligamento** e/ou **responsabilização civil e criminal**;
- Casos omissos ou dúvidas devem ser encaminhados à área de **Tecnologia da Informação** ou **Compliance**;
- Esta Política deve ser revisada periodicamente, no máximo a cada **12 (doze) meses**, ou sempre que houver alteração relevante em sistemas, legislações ou estrutura organizacional.