Política Geral de Segurança da Informação – Grupo TMT

1. Contexto e Compromisso da Direção

A Direção do **Grupo TMT**, empresa de tecnologia em identificação, declara seu total compromisso com a segurança da informação e a proteção de dados em todas as suas operações. Reconhecendo a criticidade da informação para o negócio e a confiança depositada por grandes clientes corporativos, a Direção assegura que serão disponibilizados os recursos e o apoio necessários para implementar, manter e aprimorar esta Política de Segurança da Informação. A empresa compromete-se a cumprir integralmente a legislação brasileira vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Marco Civil da Internet, bem como aderir às melhores práticas de mercado, referenciando normas como a ISO/IEC 27001. Além disso, a Direção garante que esta política será formalmente divulgada a todos os colaboradores, fornecedores e partes interessadas – por meio do site institucional e comunicados oficiais – e que todos deverão manifestar ciência e concordância (por exemplo, assinando termos de compromisso). Este comprometimento da liderança busca promover uma cultura organizacional de segurança, conformidade e rastreabilidade, mitigando riscos e protegendo os ativos de informação e os dados pessoais sob custódia do Grupo TMT.

2. Objetivo

O objetivo desta Política Geral de Segurança da Informação é estabelecer diretrizes e controles gerais para proteger os ativos de informação do **Grupo TMT**, garantindo **confidencialidade, integridade, disponibilidade, rastreabilidade e conformidade legal** em todas as atividades. Esta política busca assegurar que as informações corporativas e de clientes (incluindo dados pessoais) sejam adequadamente protegidas contra acesso não autorizado, uso indevido, divulgação indevida, alteração, destruição acidental ou qualquer forma de tratamento inadequado ou ilícito. Adicionalmente, visa orientar a organização no cumprimento das leis e regulamentos aplicáveis, em especial a LGPD, e na adoção das melhores práticas de segurança da informação reconhecidas internacionalmente (como as da ISO/IEC 27001), mesmo que o Grupo TMT ainda não possua certificações formais. Por meio desta política, o Grupo TMT pretende fortalecer a confiança dos clientes e parceiros, garantindo conformidade às exigências contratuais de grandes empresas (compliance), capacidade de auditoria e rastreabilidade de ações, bem como a redução de riscos operacionais e legais.

3. Escopo e Aplicabilidade

Esta política se aplica a **todos os setores, unidades de negócio e operações do Grupo TMT**, abrangendo todos os colaboradores (inclusive diretores, empregados, estagiários e terceirizados) e quaisquer outros que tenham acesso a informações do Grupo TMT ou sob sua guarda. Também se estende a **fornecedores, prestadores de serviço, parceiros de**

negócio ou consultores que manuseiem, processem ou armazenem informações do Grupo TMT, mediante contratos ou acordos de confidencialidade e segurança.

O escopo abrange **todos os ativos de informação** da empresa, incluindo, mas não se limitando a: dados corporativos internos, informações de clientes, dados pessoais coletados ou processados (especialmente aqueles contidos em crachás de identificação e sistemas de controle de acesso), documentos em meio físico ou digital, sistemas de informação, bancos de dados, infraestruturas de TI, dispositivos eletrônicos, redes corporativas e quaisquer outros recursos por onde transitem ou sejam armazenadas informações relevantes. Também estão incluídos no escopo os sistemas e soluções fornecidas pelo Grupo TMT a seus clientes (como softwares de controle de acesso), no que tange à proteção das informações neles contidas.

Em resumo, todos os indivíduos vinculados ao Grupo TMT e todos os recursos computacionais ou físicos que manipulam informação estão sujeitos a esta Política. O desconhecimento desta política não isenta colaboradores ou parceiros de cumprir suas diretrizes.

4. Definições

Para os fins desta política, adotam-se as seguintes definições:

- **Ativos de Informação:** Qualquer item que contenha, processe, armazene ou transmita informação da empresa. Pode incluir documentos físicos, arquivos digitais, sistemas, redes, bancos de dados, dispositivos móveis, etc.

- **Autenticação Multifator (MFA):** Mecanismo de segurança que exige **mais de um fator de autenticação** para validar a identidade do usuário, combinando algo que ele sabe (senha), algo que ele tem (token ou celular) ou algo que ele é (biometria).

- **Confidencialidade:** Princípio que garante que as informações sejam acessadas apenas por pessoas autorizadas.

- **Dado Pessoal:** Informação relacionada a uma pessoa natural identificada ou identificável, conforme definição da LGPD.

- **DPO (Data Protection Officer) / Encarregado de Dados:** Pessoa designada para atuar como canal entre a empresa, os titulares de dados e a ANPD, conforme exige a LGPD.

- **Disponibilidade:** Garantia de que os sistemas e dados estarão acessíveis quando necessários.

- **Integridade:** Garantia de que a informação está completa, precisa e não foi alterada indevidamente.

- **LGPD:** Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), legislação brasileira que regula o tratamento de dados pessoais.

- **RBAC (Role-Based Access Control):** Modelo de controle de acesso baseado em funções (cargos ou perfis de trabalho). Define permissões com base na função que o usuário ocupa na organização.

- **Titular de Dados:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- **Vazamento de Dados:** Exposição, acesso ou divulgação indevida de informações confidenciais ou pessoais.

5. Fundamentos Legais e Referências Normativas

Esta Política Geral de Segurança da Informação está embasada nas legislações brasileiras vigentes e em normas internacionais de segurança, garantindo alinhamento tanto com obrigações legais quanto com padrões de mercado aceitos. Os principais fundamentos incluem:

- **Lei Geral de Proteção de Dados Pessoais (LGPD – Lei Nº 13.709/2018):** estabelece diretrizes rigorosas para o tratamento de dados pessoais, incluindo a necessidade de adoção de medidas de segurança técnicas e administrativas aptas a proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas. Prevê direitos dos titulares (como acesso, correção e eliminação de dados), obrigação de notificação de incidentes de segurança (como vazamentos) à ANPD e aos afetados, e princípios de tratamento que devem ser observados, como licitude, finalidade, necessidade, adequação, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. A LGPD exige medidas de proteção de integridade e confidencialidade dos dados pessoais e prevê sanções em caso de descumprimento.

- **Marco Civil da Internet (Lei Nº 12.965/2014) e Decreto Regulamentador 8.771/2016:** estabelece princípios, garantias e direitos para o uso da Internet no Brasil, incluindo a proteção da privacidade e dos dados pessoais dos usuários. Determina que aplicativos de Internet tenham consentimento expresso dos usuários para coleta, uso e tratamento de dados pessoais, assegura a inviolabilidade e sigilo das comunicações e impõe obrigações de **segurança e guarda de registros de acesso** por períodos determinados. O Grupo TMT, ao fornecer sistemas online de identificação e controle de acesso, deve observar essas normas, garantindo a proteção dos dados trafegados pela internet e o atendimento a eventuais ordens judiciais relativas a registros (sempre em conformidade com a lei).

- **Demais Leis e Regulamentos Setoriais:** Outras normas legais pertinentes à segurança da informação e crimes digitais serão observadas, tais como a Lei Nº 12.737/2012 (Crimes Informáticos), que criminaliza a invasão de sistemas e roubo de dados, e legislações trabalhistas e civis aplicáveis em casos de violação de sigilo ou uso indevido de informações. Regulamentações específicas de clientes ou

setores também serão atendidas quando aplicáveis (por exemplo, requisitos de segurança estabelecidos pelo Banco Central do Brasil para instituições financeiras, que demandam políticas robustas de cibersegurança e reporte de incidentes).

- **Normas e Melhores Práticas de Segurança da Informação:** Esta política alinha-se aos princípios e controles preconizados nas normas ISO/IEC 27001 e ISO/IEC 27002 (normas internacionais de Sistema de Gestão de Segurança da Informação) e referências correlatas. Embora o Grupo TMT não possua certificação formal no momento, busca-se implementar as melhores práticas descritas nessas normas – tais como abordagem baseada em riscos, classificação da informação, controle de acessos, criptografia, gestão de incidentes e melhoria contínua – para garantir um nível de segurança compatível com organizações líderes de mercado. **Confidencialidade, integridade e disponibilidade** são tratadas como pilares, assim como responsabilidade (accountability) e conformidade com leis. A aderência a essas boas práticas internacionais facilita o cumprimento da LGPD, já que há forte convergência entre os requisitos da ISO 27001 e os da lei brasileira de proteção de dados.

Em suma, o Grupo TMT pauta sua Política de Segurança tanto nas obrigações legais (assegurando **legalidade** de todas as ações) quanto nas referências normativas reconhecidas, de modo a oferecer confiança aos clientes e partes interessadas de que a segurança e a privacidade da informação são tratadas com seriedade e rigor técnico.

6. Uso de Inteligência Artificial (IA)

O Grupo TMT adota o uso de Inteligência Artificial de forma ética, segura e em conformidade com a legislação brasileira, especialmente com a Lei Geral de Proteção de Dados Pessoais (LGPD). Reconhecendo os potenciais benefícios e riscos associados a tecnologias baseadas em IA, a empresa adota princípios de transparência, finalidade, segurança e responsabilidade no uso dessas soluções.

6.1 Finalidade de uso

Atualmente, o uso de IA no Grupo TMT está restrito ao processo de validação e tratamento de fotos de colaboradores de clientes, no contexto da emissão de crachás corporativos. A finalidade é:

- Avaliar se a imagem enviada atende aos requisitos técnicos (ex: resolução, iluminação, enquadramento);
- Remover o fundo e aplicar formatação padronizada (como fundo transparente e proporções específicas) para adequação ao padrão de identidade visual da empresa.

6.2 Tecnologia empregada

Essa funcionalidade é executada por meio da **API do ChatGPT (OpenAI, modelo GPT-4)**, utilizada exclusivamente em chamadas programadas com envio de imagem para validação

e transformação. O processamento ocorre de forma automatizada, com os dados trafegando por servidores da OpenAI, sob padrões internacionais de segurança e privacidade.

6.3 Garantias de proteção e conformidade

- As imagens são **processadas apenas para fins técnicos específicos** e não são armazenadas permanentemente nos sistemas da OpenAI.
- Nenhuma imagem é utilizada para fins de treinamento do modelo.
- Não há tratamento de dados biométricos ou uso de IA para análise comportamental.
- A operação é acompanhada pelo Encarregado de Proteção de Dados (DPO) e mapeada no Relatório de Impacto à Proteção de Dados (RIPD).

6.4 Transparência

O Grupo TMT informa os clientes e colaboradores sobre o uso da IA nos processos internos, sempre que a atividade envolver dados pessoais. Os titulares são comunicados durante o envio da imagem e podem solicitar esclarecimentos junto ao DPO da empresa.

6.5 Expansão futura

Qualquer ampliação do uso de IA que envolva:

- decisões automatizadas com efeitos jurídicos ou relevantes;
- coleta ou análise de dados biométricos;
- correlação com bases de dados pessoais;

será previamente avaliada quanto ao impacto jurídico, ético e técnico, e submetida aos mecanismos de governança internos, com registro e validação da conformidade com a LGPD.

7. Princípios e Diretrizes Gerais

Os seguintes **princípios fundamentais** norteiam todas as ações de segurança da informação no Grupo TMT, servindo como base para esta política e para os procedimentos decorrentes:

- **Confidencialidade:** Garantir que as informações sejam acessíveis apenas por pessoas explicitamente autorizadas, preservando o **sigilo** dos dados sensíveis e estratégicos. Nenhuma informação confidencial deve ser divulgada ou compartilhada indevidamente, assegurando conformidade com acordos de confidencialidade e com a LGPD na proteção de dados pessoais. Este princípio visa evitar vazamentos de dados, espionagem industrial e uso não autorizado de informações restritas.

- **Integridade:** Proteger a **exatidão e completeza** das informações, assegurando que os dados não sejam alterados de forma não autorizada ou acidental. Devem ser implementados controles para prevenir modificações indevidas e garantir que qualquer alteração legítima seja rastreável. Assim, decisões baseadas nas

informações serão confiáveis, e os registros manterão valor legal e operacional.

- **Disponibilidade:** Assegurar que as informações, sistemas e serviços estejam **disponíveis** aos usuários autorizados sempre que necessário, evitando interrupções desnecessárias nos negócios. Isso inclui implementar mecanismos de redundância, backups periódicos, planos de continuidade de negócio e recuperação de desastres, de modo que a empresa possa operar sem paralisações significativas mesmo diante de falhas, ataques cibernéticos ou outros incidentes. A disponibilidade é crucial dada a natureza dos serviços do Grupo TMT (identificação e controle de acesso), que precisam funcionar ininterruptamente para os clientes.

- **Rastreabilidade (Accountability):** Garantir a **rastreabilidade de ações** e a responsabilidade individual no uso da informação. Todas as ações relevantes em sistemas críticos devem ser registradas em logs seguros (por exemplo, acessos, alterações, consultas e transmissões de dados), possibilitando a auditoria e a identificação de "quem, quando, onde e o quê" foi feito. Este princípio permite detectar uso indevido ou não autorizado de informações, suportar investigações internas ou externas e cumprir exigências de clientes quanto à auditabilidade. A rastreabilidade reforça a accountability, de forma que cada colaborador ou terceiro seja responsável por suas ações no manuseio da informação.

- **Legalidade e Conformidade:** As atividades de tratamento de informação devem estar em **conformidade com as leis, regulamentações e obrigações contratuais** aplicáveis. Isso inclui respeitar os direitos de privacidade dos titulares de dados sob LGPD, seguir requisitos do Marco Civil ao lidar com dados em aplicações web, e aderir a contratos que demandem níveis específicos de segurança ou confidencialidade. Nenhum colaborador deve praticar atos que violem legislação (por exemplo, reproduzir software de forma ilícita, vender ou fornecer dados confidenciais a terceiros sem autorização, etc.). A empresa enfatiza que a segurança da informação não é apenas uma questão interna, mas também um dever legal; portanto, o princípio da legalidade permeia todos os demais princípios, assegurando que a proteção da informação ocorra dentro dos parâmetros da lei e que o Grupo TMT possa demonstrar conformidade (accountability) às autoridades e clientes.

- **Classificação da Informação:** Todas as informações devem ser classificadas de acordo com seu nível de sensibilidade e criticidade (por exemplo: **Pública**, **Interna**, **Confidencial**, **Restrita**). A classificação orientará o tratamento adequado de cada tipo de informação. Informações confidenciais e restritas exigem controles mais rigorosos de acesso, armazenamento e transporte. Os documentos e dados deverão ser rotulados conforme sua classificação sempre que possível, garantindo seu manuseio conforme requerido – por exemplo, documentos marcados como "Confidencial" devem ser criptografados ao serem enviados eletronicamente ou guardados em local seguro. Revisões periódicas da classificação deverão ocorrer, especialmente se a natureza ou sensibilidade da informação mudar.

- **Controle de Acesso:** O acesso às informações e sistemas do Grupo TMT deve obedecer ao princípio do **menor privilégio** e da necessidade de saber. Isso significa que cada usuário (colaborador ou terceirizado) terá apenas as permissões

estritamente necessárias para desempenhar suas funções. Mecanismos robustos de autenticação (como senhas fortes, autenticação multifator, MFA, onde cabível) e autorização devem ser implementados em todos os sistemas. É obrigatório o uso de contas individuais e intransferíveis; acessos compartilhados ou genéricos são desaconselhados ou restritos a casos excepcionais com devidos controles. Também deve ser adotado **Controle de acesso baseado em funções (RBAC)** ou perfil de funções, de forma a facilitar a gestão de permissões de acordo com cargos e responsabilidades. O acesso a dados especialmente sensíveis (por exemplo, bases de dados de identificação com informações pessoais) deve requerer autorizações adicionais. Todos os acessos privilegiados (administradores de sistema, por exemplo) devem ser estritamente controlados e monitorados. A revisão de acessos deve ser feita regularmente (por exemplo, trimestralmente), revogando prontamente permissões de colaboradores que mudem de função ou deixem a empresa.

- **Proteção de Dados e Criptografia:** Devem ser empregadas medidas técnicas para proteção dos dados em todas as camadas. Informações sensíveis ou pessoais **devem ser criptografadas** tanto em repouso (armazenadas em bases de dados, discos, dispositivos móveis) quanto em trânsito (durante comunicações eletrônicas, transmissões em rede), utilizando algoritmos e protocolos criptográficos fortes, alinhados às recomendações atuais do mercado. Chaves criptográficas devem ser gerenciadas de forma segura, com acesso restrito e troca periódica conforme políticas internas. Além da criptografia, outras medidas incluem: uso de firewalls e sistemas de prevenção de intrusão para proteger as redes; softwares antivírus/antimalware atualizados em todos os servidores e estações; controles de segurança em dispositivos móveis e mídias removíveis (como pen-drives criptografados, políticas de uso de dispositivos pessoais, etc.). Dados pessoais podem, sempre que possível, ser anonimizados ou pseudonimizados (mascarados) de forma a minimizar riscos em caso de vazamento, em conformidade com os princípios da LGPD e técnicas recomendadas. Qualquer desenvolvimento de software ou sistema dentro do Grupo TMT deve seguir padrões seguros de codificação (Security by Design), a fim de evitar vulnerabilidades.

- **Segurança Física e Ambiental:** A proteção da informação abrange também o ambiente físico. Instalações do Grupo TMT (escritórios, data centers, centros de produção de crachás) devem contar com **controles de segurança física**, tais como controle de acesso aos prédios e salas (ex: crachás ou biometria para entrar em áreas restritas), vigilância por CFTV, alarmes e proteção contra incêndio e desastres. Apenas pessoas autorizadas podem ter acesso a locais onde existam ativos de informação sensíveis (como servidores ou arquivos confidenciais). Equipamentos servidores devem ficar em ambientes com acesso controlado. Documentos em papel classificados como confidenciais devem ser armazenados em armários trancados. Deve-se evitar deixar informações sensíveis expostas em mesas ou impressoras (política de mesa limpa e tela limpa). A segurança ambiental (ar condicionado adequado, nobreaks, geradores) deve ser mantida para garantir disponibilidade e integridade dos equipamentos e dados.

- **Conscientização e Treinamento:** O Grupo TMT promoverá **programas regulares de treinamento** e conscientização em segurança da informação e proteção de

dados para todos os colaboradores. Os colaboradores receberão orientações desde a integração (onboarding) e treinamentos periódicos sobre políticas internas, melhores práticas de segurança (como construção de senhas seguras, identificação de e-mails maliciosos, engenharia social, etc.) e sobre as responsabilidades individuais no manuseio de informações e dados pessoais conforme a LGPD. Sessões específicas serão conduzidas para equipes técnicas ou que lidam com informações altamente sensíveis, conforme apropriado. A efetividade desses treinamentos será avaliada e reforços serão feitos sempre que necessário (por exemplo, campanhas de conscientização, comunicados via intranet). A alta direção reforça a importância de uma cultura organizacional de segurança, onde todos entendam que a segurança da informação é parte intrínseca de suas funções.

- **Proteção de Dados Pessoais (Privacidade):** Em consonância com a LGPD, todo dado pessoal coletado ou manuseado pelo Grupo TMT (por exemplo, dados de funcionários de clientes para confecção de crachás de acesso) **deve ser tratado com estrita observância aos princípios de privacidade**. Isso implica: coletar apenas os dados pessoais estritamente necessários para a finalidade prevista (princípio da minimização); informar claramente aos clientes e titulares a finalidade da coleta e obter consentimento quando exigido ou assegurar outro embasamento legal válido; não utilizar dados para finalidades incompatíveis com aquela informada originalmente; garantir a qualidade (exatidão) dos dados e mantê-los atualizados; armazenar os dados pelo tempo necessário para cumprir a finalidade ou exigência legal, eliminando-os de forma segura após isso. Medidas de segurança apropriadas, conforme já delineadas (como criptografia, controle de acesso, pseudonimização), devem ser aplicadas especificamente a bancos de dados contendo informações pessoais, visando prevenir acessos não autorizados ou vazamentos. Os direitos dos titulares, tais como acesso aos próprios dados, retificação ou exclusão, devem ser atendidos conforme procedimentos definidos pela empresa, sob coordenação do Encarregado de Dados (DPO). Qualquer incidente de segurança envolvendo dados pessoais deverá ser comunicado conforme descrito na seção de Gestão de Incidentes abaixo.

- **Gestão de Incidentes de Segurança:** O Grupo TMT deverá manter um **Plano de Resposta a Incidentes** formal, com procedimentos para identificar, reportar, conter, investigar e resolver incidentes de segurança da informação. Todos os colaboradores têm a obrigação de reportar **imediatamente** ao time responsável (e/ou ao Encarregado de Proteção de Dados, se envolver dados pessoais) qualquer incidente ou suspeita (como perda de dispositivo contendo informações da empresa, suspeita de invasão, recebimento de phishing, vazamento de dados, etc.). A equipe de Segurança da Informação conduzirá a investigação e tomará as medidas de mitigação cabíveis, documentando o ocorrido e as ações tomadas. Em casos de **incidente de violação de dados pessoais (data breach)** que atendam aos critérios de notificabilidade da LGPD, a empresa irá notificar tempestivamente a **Autoridade Nacional de Proteção de Dados (ANPD)** e os titulares afetados, nos termos da lei. O plano de resposta deve incluir fluxos de comunicação (interna e externa), definição de times de resposta (por exemplo, envolvendo TI, Jurídico, Comunicação) e ações de correção e prevenção para evitar recorrências. Testes e simulações (como *drills* de incidentes) devem ser realizados periodicamente para garantir que a

equipe esteja preparada para reagir de forma eficaz.

- **Continuidade de Negócios e Recuperação de Desastres:** A fim de garantir a disponibilidade e a resiliência dos serviços prestados, o Grupo TMT deve manter planos de continuidade de negócios e procedimentos de recuperação de desastres. Isso inclui: realização de **backups regulares** de dados críticos (e verificação periódica de sua restauração); manutenção de infraestrutura redundante ou alternativas em caso de falha de componentes essenciais; planejamento de contingências para cenários como indisponibilidade prolongada de sistemas, desastres naturais, incêndios ou outras calamidades que afetem as operações. Os planos de continuidade devem ser testados (pelo menos anualmente) e atualizados conforme necessário. Em caso de interrupção significativa, a prioridade será restaurar as operações críticas de identificação e controle de acesso dos clientes no menor tempo possível, minimizando impactos. Todos os colaboradores chave devem conhecer seus papéis nesses planos.

- **Controle de Fornecedores e Terceiros:** Sempre que o Grupo TMT contratar fornecedores ou parceiros que possam ter acesso a dados ou sistemas da empresa (por exemplo, empresas de suporte de TI, processamento em nuvem, consultores), deverá ser garantido que tais terceiros atendam a requisitos equivalentes de segurança da informação. Contratos com terceiros devem incluir **cláusulas de confidencialidade** e de proteção de dados, bem como previsões de conformidade com a LGPD quando envolver dados pessoais. Fornecedores críticos devem passar por avaliações de segurança (due diligence) antes da contratação e periodicamente, podendo ser exigidas evidências de suas práticas de segurança (como certificações, relatórios de auditoria). O acesso de terceiros aos sistemas do Grupo TMT deve ser controlado, concedido apenas conforme necessário e supervisionado. Em caso de encerramento de contrato, o acesso do fornecedor aos ativos da empresa deve ser revogado e garantir-se o retorno ou deleção adequada dos dados confidenciais ou pessoais compartilhados durante a prestação do serviço.

Todas estas diretrizes gerais devem ser complementadas por normas e procedimentos internos específicos (ex: Política de Controle de Acesso Lógico, Norma de Uso Aceitável dos Recursos de TI, Procedimento de Resposta a Incidentes, etc.), que detalharão sua execução no dia a dia. **Todos os colaboradores e parceiros devem observar estas diretrizes** em todas as atividades, pois elas representam a linha mestra para manter a segurança da informação no Grupo TMT.

8. Responsabilidades

A implementação eficaz desta política requer a definição clara de responsabilidades de todos os envolvidos na organização:

- **Alta Direção:** Aprovar e apoiar formalmente esta Política de Segurança da Informação, prover os recursos (financeiros, humanos, tecnológicos) necessários

para seu cumprimento e melhoria contínua, e exercer liderança visível em favor da segurança. A direção deve zelar para que a segurança da informação seja parte integrante da estratégia empresarial e para que haja a fiscalização do cumprimento das diretrizes aqui estabelecidas. Cabe também à Alta Direção designar ouvidores/responsáveis (como um Comitê de Segurança da Informação ou um Gestor de Segurança) e o **Encarregado de Proteção de Dados (DPO)** conforme exigido pela LGPD, garantindo que tais responsáveis tenham autonomia e condições para executar suas funções. Adicionalmente, a Alta Direção deve assegurar a **divulgação adequada desta política** em toda a empresa e para parceiros, reforçando continuamente seu compromisso (conforme declarado no item 1) e exigindo adesão de todos.

- **Gestor de Segurança da Informação / Comitê de Segurança:** Coordenar a implementação das diretrizes desta política no dia a dia. Isso inclui desenvolver procedimentos e normas complementares, promover programas de conscientização e treinamento, conduzir análise de riscos periódicas e estabelecer planos de tratamento de riscos de segurança. Este gestor ou comitê também monitora o cumprimento da política, realizando auditorias internas ou verificações de conformidade, e reporta à Alta Direção sobre o estado da segurança da informação, incluindo eventuais incidentes relevantes. É responsável por recomendar melhorias e atualizar a política conforme necessário (em conjunto com o DPO no que tange a dados pessoais). Também supervisiona a atuação da equipe técnica de segurança (se existente) e a interação com outras áreas da empresa em assuntos de segurança.

- **Encarregado de Proteção de Dados (DPO):** Responsável, nos termos da LGPD, por atuar como canal de comunicação entre o Grupo TMT, os titulares de dados e a ANPD. O DPO deve zelar pela conformidade das práticas da empresa no tocante a dados pessoais, o que inclui: orientar colaboradores e os processadores de dados sobre as práticas a adotar, monitorar a aplicação dos programas de privacidade e segurança relacionados à proteção de dados pessoais, receber e gerir solicitações de titulares (como pedidos de acesso ou eliminação de dados) e preparar relatórios de impacto à proteção de dados quando necessário. Em caso de incidentes de segurança envolvendo dados pessoais, o DPO auxilia na avaliação do risco e na necessidade de comunicação à ANPD. O DPO também contribui para a revisão desta política, garantindo alinhamento com evoluções regulatórias em privacidade.

- **Gestores de Áreas/Departamentos:** Cada gestor ou gerente de área (por exemplo, TI, RH, Operações, etc.) é responsável por assegurar que seus subordinados conheçam e cumpram esta política e procedimentos relacionados. Devem incentivar uma postura proativa de segurança em suas equipes, garantindo que informações sob responsabilidade do departamento sejam classificadas adequadamente, armazenadas de forma segura e acessadas somente por pessoal autorizado. Gestores devem reportar incidentes ou não conformidades de que tenham conhecimento e colaborar com o comitê de segurança ou DPO na implementação de controles específicos em sua área. Em processos de negócio críticos ou projetos, devem engajar a área de segurança desde o início (segurança por design). No caso específico do departamento de TI, além do papel gerencial, há a responsabilidade

técnica de implementar e manter os controles de segurança lógicos e de infraestrutura (controles de acesso, backups, antivírus, atualizações de patches, etc.), conforme diretrizes desta política.

- **Todos os Colaboradores (empregados e contratados):** Cada membro do Grupo TMT, independentemente de cargo ou função, **tem a responsabilidade de cumprir integralmente esta Política de Segurança da Informação** e as normas dela decorrentes. Espera-se de todos: sigilo e discrição no trato das informações (não divulgar dados confidenciais a quem não deve recebê-los); uso adequado dos recursos de TI fornecidos (evitar instalar softwares não autorizados, acessar sites não permitidos ou utilizar e-mail corporativo para fins ilícitos); zelar pela proteção de senhas e credenciais (não compartilhar senhas, seguir políticas de criação de senhas seguras); reportar imediatamente qualquer incidente ou fraqueza de segurança observada; participar dos treinamentos obrigatórios e esclarecer dúvidas junto aos responsáveis quando necessário. Os colaboradores devem assinar (fisicamente ou eletronicamente) um termo de ciência e compromisso com esta política e com a Política de Privacidade/LGPD da empresa ao ingressar, e periodicamente em revisões significativas, formalizando sua adesão. O descumprimento das diretrizes por parte de colaboradores poderá sujeitá-los a medidas disciplinares conforme descrito adiante.

- **Fornecedores, Parceiros e Terceirizados:** Terceiros que tenham acesso a informações do Grupo TMT ou a sistemas corporativos (incluindo dados de clientes) têm a obrigação contratual de **proteger adequadamente essas informações**, em linha com esta política. Devem cumprir as cláusulas de confidencialidade e requisitos de segurança previstos nos contratos ou termos de serviço. Caso identifiquem incidentes ou vulnerabilidades envolvendo dados do Grupo TMT, devem notificar prontamente o ponto de contato na empresa, cooperando nas investigações e medidas corretivas. Fornecedores de tecnologia devem manter boas práticas de mercado (por exemplo, aplicar atualizações de segurança em softwares fornecidos, atender a padrões de continuidade de serviço). A não conformidade de fornecedores com os requisitos de segurança poderá resultar em sanções contratuais, incluindo possível encerramento da parceria, além de responsabilização legal se couber.

Em suma, a segurança da informação é responsabilidade de **todos** no Grupo TMT. Cada um deve entender seu papel na proteção dos ativos informacionais e atuar de forma diligente. A empresa promoverá um ambiente no qual seja possível reportar problemas de segurança sem retaliação, visando à rápida resolução. A colaboração entre as áreas (TI, Jurídico, RH, Operações, etc.) é essencial para o sucesso desta política, garantindo que segurança e negócios caminhem juntos.

9. Penalidades e Consequências

Esta Política de Segurança da Informação possui **aplicação obrigatória** e vinculante para todos os integrantes do Grupo TMT e terceiros abrangidos por seu escopo. O não cumprimento das diretrizes aqui estabelecidas, ou de normas associadas, constitui violação

das obrigações funcionais e contratuais, sujeitando o infrator às medidas disciplinares e legais cabíveis.

No âmbito **interno (administrativo)**, eventuais violações por colaboradores estarão sujeitas às penalidades previstas nas normas da empresa e na legislação trabalhista, proporcionais à gravidade da falta. Essas penalidades podem incluir advertência verbal ou escrita, suspensão e, em casos graves ou de reincidência, demissão por justa causa. No caso de terceiros, as sanções podem envolver notificação formal, rescisão de contrato e possíveis reivindicações de indenização por danos causados.

No âmbito **legal externo**, a empresa destaca que certas condutas podem configurar infrações a leis e regulamentos, podendo acarretar penalidades regulatórias ou criminais. Por exemplo, o vazamento de dados pessoais por negligência ou não adoção de medidas de segurança pode sujeitar o Grupo TMT a sanções da ANPD conforme a LGPD, incluindo multas que podem atingir **2% do faturamento da empresa**, bloqueio ou eliminação dos dados envolvidos, bem como dano à reputação corporativa. Adicionalmente, atos dolosos como apropriação indevida de segredos comerciais, invasão de sistemas ou fraude eletrônica podem incorrer em responsabilidade civil e criminal para os indivíduos envolvidos, nos termos da legislação (podendo levar a processos judiciais, multas penais e até pena de detenção, conforme os casos previstos em lei).

Todo colaborador ou parceiro, ao aderir a esta política (vide assinatura de termo de compromisso), declara-se ciente de que a não observância de seus termos e da legislação correlata poderá resultar nas consequências mencionadas. O Grupo TMT, por sua vez, reserva-se o direito de investigar suspeitas de violação, utilizando meios lícitos de auditoria e monitoramento, respeitando os direitos individuais. Se for constatada uma violação, a empresa tomará as medidas apropriadas de forma objetiva e documentada. Em caso de incidente de segurança, além das ações corretivas internas, a empresa cooperará com autoridades governamentais e regulatórias conforme necessário, inclusive realizando as notificações obrigatórias (como à ANPD) dentro dos prazos legais.

Em suma, esta política tem força normativa interna e reflete obrigações legais externas; cumpri-la integralmente é condição indispensável para atuar no ambiente do Grupo TMT. As penalidades visam reforçar a seriedade da proteção da informação e não isentam a organização ou indivíduos de outras responsabilidades decorrentes de leis específicas.

10. Política de Revisão e Atualização

A segurança da informação é uma disciplina dinâmica, sujeita a novas ameaças, mudanças tecnológicas e atualizações regulatórias. Por isso, o Grupo TMT estabelece um processo de **revisão periódica** desta Política Geral de Segurança da Informação, a fim de mantê-la atualizada, eficaz e aderente às melhores práticas vigentes.

- **Periodicidade de Revisão:** Esta política deverá ser revisada, no mínimo, **anualmente**. Revisões extraordinárias poderão ocorrer sempre que houver mudanças significativas no ambiente interno ou externo da empresa, tais como: alterações relevantes na legislação (por exemplo, novas regulamentações da ANPD ou emendas à LGPD), evolução dos negócios da empresa que introduzam novos

riscos (lançamento de novos serviços, entrada em novos mercados), ocorrências de incidentes graves de segurança que revelem a necessidade de aprimoramento dos controles, ou ainda recomendações resultantes de auditorias de segurança.

- **Responsáveis pela Revisão:** A responsabilidade por coordenar o processo de revisão é do **Gestor de Segurança da Informação** em conjunto com o **Encarregado de Proteção de Dados (DPO)**, com o apoio do Comitê de Segurança (se existente) e participação de representantes de áreas chave. Eventuais atualizações na legislação de privacidade ou segurança devem ser acompanhadas de perto (consultando assessoria jurídica quando necessário) para assegurar que a política permaneça em conformidade. A Alta Direção deverá aprovar formalmente qualquer alteração substancial na política, demonstrando novamente seu compromisso.

- **Controle de Versão:** Cada versão revisada da política deve ser documentada com um controle de versão (incluindo data de vigência, resumo das alterações e aprovação da Direção). Versões anteriores devem ser arquivadas para fins de referência histórica e auditoria.

- **Comunicação de Mudanças:** Sempre que a política for atualizada, o Grupo TMT realizará a devida **comunicação a todos os colaboradores e partes aplicáveis**. A nova versão será divulgada pelos mesmos canais oficiais (intranet, e-mail corporativo, site, etc.). Poderá ser requerido que todos os colaboradores reafirmem sua ciência e concordância com a política atualizada, por meio de aceite eletrônico ou assinatura de um novo termo, especialmente se houver mudanças significativas nas diretrizes. Fornecedores e parceiros relevantes também devem ser notificados de alterações que impactem suas obrigações. Adicionalmente, poderão ser conduzidas sessões de treinamento ou comunicados explicativos para esclarecer as principais mudanças e assegurar a correta interpretação e implementação.

O compromisso do Grupo TMT é de manter esta Política Geral de Segurança da Informação como um documento **vivo**, que evolui conforme necessário para continuar eficaz frente aos novos desafios. A melhoria contínua em segurança da informação será perseguida, e a revisão periódica da política é parte integrante do ciclo de **melhoria contínua** (PDCA) do Sistema de Gestão de Segurança da Informação da organização. Desse modo, garantimos que as diretrizes aqui estabelecidas permanecem atuais, robustas e alinhadas com os objetivos estratégicos da empresa e requisitos de conformidade em vigor.

Publicação e Acesso: A versão vigente desta política estará sempre disponível para consulta na intranet corporativa do Grupo TMT e no site institucional (na seção de governança ou compliance), de forma a garantir transparência para clientes e partes interessadas. Cópias controladas poderão ser distribuídas às áreas, se necessário. Recomenda-se a todos os colaboradores que se mantenham informados sobre o conteúdo mais recente da política e integrem suas diretrizes às atividades diárias, contribuindo para um ambiente corporativo seguro e confiável.

Fonte: Esta política foi elaborada com base nas exigências da legislação brasileira (LGPD, Marco Civil da Internet e normas correlatas) e nas melhores práticas de segurança da informação (ISO/IEC 27001 e frameworks associados), visando atender às expectativas de grandes clientes quanto à segurança, conformidade e gestão de riscos em serviços de identificação e controle de acesso corporativo.