SISTEMA DE GESTÃO INTEGRADO

Política de Segurança da Informação

DOCUMENTO PÚBLICO

PL-SGI-01 REV.04

Controle de Versões

N°	Data	Aprovado por	Histórico
00	05/01/2022	Airton Coelho	Emissão Inicial
01	15/01/2022	Arthur Barcelos	Primeira Revisão da Política
02	10/12/2023	Arthur Barcelos e Airton Coelho	Segunda Revisão da Política
03	30/09/2025	Carla Oliveira	Atualização geral da política, com revisão de diretrizes, princípios e adequação aos requisitos normativos vigentes.
04	23/03/2026	Carla Oliveira	Atualização da política com revisão das diretrizes gerais, inclusão de requisitos de privacidade, adequação à ISO 27001/27701 e melhoria dos controles e processos de segurança da informação.

Sumário

1. Introdução

A Política de Segurança da Informação (PSI) da **T2M – Test to Market** é o documento que define e orienta as diretrizes corporativas para a proteção dos ativos de informação, assegurando a confidencialidade, integridade e disponibilidade dos dados, bem como a prevenção de riscos legais e regulatórios para todos os usuários.

Sua observância é obrigatória em todas as áreas da empresa, devendo ser aplicada por colaboradores, prestadores de serviço e terceiros que tenham acesso às informações da **T2M**.

A presente PSI está fundamentada nas boas práticas internacionais de segurança da informação, especialmente nas recomendações da norma ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente como referência para a gestão da segurança da informação, e nas orientações do NIST Cybersecurity Framework (CSF). Além disso, encontra-se plenamente alinhada à Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) e às demais legislações vigentes no Brasil, assegurando conformidade regulatória e reforçando o compromisso da **T2M** com a proteção das informações e a mitigação de riscos.

2. Dos Objetivos

A Política de Segurança da Informação (PSI) da **T2M** tem como objetivos principais:

- **Estabelecer diretrizes** que orientem colaboradores, clientes, parceiros e terceiros a adotarem padrões de comportamento compatíveis com as necessidades do negócio, assegurando a proteção legal da empresa e dos indivíduos envolvidos.

- **Nortear a criação de normas, procedimentos e controles específicos**, promovendo sua efetiva implementação e garantindo a conformidade com os requisitos de segurança da informação.

- **Preservar as informações da T2M**, assegurando:

    - **Integridade**: manutenção da informação em seu estado original, protegendo-a contra alterações indevidas, sejam elas intencionais ou acidentais.
    - **Confidencialidade**: acesso restrito à informação, garantindo que somente pessoas autorizadas possam utilizá-la.
    - **Disponibilidade**: acesso contínuo e oportuno às informações e ativos, sempre que necessário, por usuários devidamente autorizados.

Desta forma, a PSI define um conjunto de ações preventivas e procedimentos de recuperação, destinados a proteger os sistemas críticos da **T2M** contra falhas de equipamentos, incidentes acidentais, ataques intencionais ou desastres naturais de grande impacto, assegurando a resiliência organizacional e a continuidade das operações.

Por fim, esta política informa a todos os colaboradores que os ambientes, sistemas, computadores e redes da **T2M** poderão ser monitorados e registrados, mediante comunicação prévia e em conformidade com a legislação brasileira aplicável.

3. Da Abrangência

Esta Política de Segurança da Informação aplica-se a todas as áreas, processos, sistemas e ativos sob responsabilidade da **T2M**. Seu cumprimento é obrigatório para todos que, de alguma forma, têm acesso às informações da empresa, sejam elas digitais, físicas ou verbais.

Estão incluídos no escopo desta política:

- **Colaboradores, estagiários, prestadores de serviço, fornecedores, consultores e parceiros de negócios**, independentemente do vínculo contratual ou do local de atuação;

- **Clientes** que, por meio de sistemas ou plataformas disponibilizadas pela **T2M**, tenham acesso, manipulem ou armazenem informações sob responsabilidade da empresa;

- **Todos os ativos de informação**, compreendendo dados, documentos físicos e digitais, sistemas, redes, dispositivos, softwares, hardwares, infraestrutura tecnológica e instalações físicas que suportam as operações da **T2M**.

A PSI é aplicável em qualquer ambiente em que as informações da **T2M** sejam tratadas, incluindo instalações internas, unidades externas, trabalho remoto e recursos hospedados em nuvem, refletindo o compromisso da empresa com a proteção da informação em todos os contextos.

4. Das Diretrizes Gerais

A organização compromete-se a identificar, analisar e atender continuamente aos requisitos legais, regulatórios, contratuais e demais obrigações aplicáveis à segurança da informação e à privacidade, assegurando sua adequada incorporação aos processos organizacionais.

A organização compromete-se com a melhoria contínua do Sistema de Gestão de Segurança da Informação e privacidade, promovendo a revisão e o aperfeiçoamento de seus processos, controles e práticas.

4.1 Dos Princípios da Segurança da Informação

A Política de Segurança da Informação da **T2M** está alicerçada em princípios que asseguram a proteção das informações e sustentam a continuidade dos negócios da organização. São eles:

- **Confidencialidade**: garantir que o acesso à informação seja permitido apenas a pessoas devidamente autorizadas, prevenindo o uso, a divulgação e o compartilhamento indevidos.
- **Integridade**: assegurar que a informação permaneça precisa, completa e fidedigna durante todo o seu ciclo de vida, protegendo-a contra alterações não autorizadas, intencionais ou acidentais.
- **Disponibilidade**: garantir que os usuários autorizados tenham acesso às informações e ativos correspondentes sempre que necessário, apoiando a eficiência operacional e a tomada de decisões.
- **Autenticidade**: assegurar a veracidade da origem das informações, confirmando a identidade de usuários, sistemas e dispositivos envolvidos em seu tratamento.
- **Responsabilidade**: atribuir a cada colaborador e terceiro a obrigação de zelar pelo uso adequado das informações, respondendo por suas ações no manuseio dos ativos da **T2M**.
- **Legalidade**: garantir que o tratamento das informações esteja em conformidade com a legislação vigente, com contratos firmados e com os regulamentos internos da organização.

Esses princípios orientam todas as decisões, processos e controles relacionados à gestão da segurança da informação na **T2M**, refletindo o compromisso da **T2M** com a proteção de seus ativos, a mitigação de riscos e a manutenção da confiança junto a clientes, parceiros e colaboradores.

4.2 Da Classificação da Informação

Para garantir a proteção adequada e proporcional ao valor e à sensibilidade dos ativos, todas as informações da **T2M** devem ser classificadas conforme seu nível de criticidade, impacto e necessidade de controle de acesso.

A classificação deve ser realizada no momento da criação da informação, revisada sempre que houver alteração de seu uso e respeitada por todos os colaboradores, prestadores de serviço e terceiros que a utilizarem, garantindo a aplicação de controles proporcionais ao nível de proteção exigido.

As categorias adotadas pela **T2M** são:

- **Pública**: informações cujo acesso é livre e irrestrito, podendo ser divulgadas sem risco para a empresa ou para terceiros. Exemplos: comunicados oficiais, materiais de marketing, informações institucionais publicadas no site.
- **Interna**: informações destinadas exclusivamente ao uso interno da **T2M**, cujo acesso não autorizado pode gerar impactos operacionais ou de imagem. Exemplos: políticas internas, procedimentos administrativos e manuais de operação.
- **Restrita**: informações de caráter sensível, cujo acesso deve ser restrito a grupos ou áreas específicas. A divulgação indevida pode gerar riscos financeiros, jurídicos, estratégicos ou de reputação. Exemplos: contratos e relatórios de clientes.
- **Confidencial**: informações altamente sensíveis, de acesso limitado a pessoas expressamente autorizadas pela diretoria. O uso indevido pode causar danos graves ou irreparáveis à **T2M**. Exemplos: segredos de negócio, estratégias corporativas, credenciais de sistemas críticos.

O manuseio, o armazenamento e a transmissão das informações devem seguir as medidas de proteção correspondentes a sua classificação, sendo vedado o rebaixamento ou compartilhamento sem autorização formal.

As informações que contêm dados pessoais ou dados pessoais sensíveis devem ser tratadas em conformidade com os princípios e requisitos estabelecidos pela Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/2018), garantindo a proteção dos direitos dos titulares e a adoção de medidas adequadas de segurança e privacidade.

Além das classificações definidas nesta política, toda informação que contenha dados pessoais ou dados pessoais sensíveis deverá ser identificada de forma explícita, com a utilização das seguintes siglas:

- **DP** – para informações que contenham dados pessoais;
- **DPS** – para informações que contenham dados pessoais sensíveis.

Essa identificação é obrigatória e tem como objetivo reforçar os cuidados necessários quanto ao tratamento, armazenamento, compartilhamento e descarte dessas

informações, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com as políticas internas da **T2M**.

4.3 Do Controle de Acesso

O controle de acesso é um princípio fundamental para a proteção das informações e ativos da **T2M**, garantindo que apenas pessoas autorizadas possam acessar sistemas, dados e recursos de acordo com sua função e necessidade operacional.

O acesso às informações deve obedecer aos seguintes critérios:

- **Princípio do menor privilégio**: cada usuário recebe apenas os direitos estritamente necessários para desempenhar suas atividades, evitando acesso desnecessário ou indevido a informações sensíveis.
- **Autenticação segura**: todos os usuários devem possuir credenciais únicas e sigilosas, como senhas complexas ou métodos de autenticação multifator, que garantam a identidade do indivíduo que acessa os sistemas.
- **Autorização baseada em função**: os níveis de acesso devem ser definidos de acordo com cargos, responsabilidades e a classificação da informação, incluindo dados pessoais e dados sensíveis, que requerem proteção adicional.
- **Revisão periódica de acessos**: as permissões concedidas devem ser revisadas regularmente para garantir que estejam atualizadas, sendo removidas imediatamente em caso de desligamento de colaboradores, término de contratos ou mudança de função.
- **Monitoramento e registro**: todas as operações de acesso a sistemas e informações críticas devem ser monitoradas e registradas, permitindo auditoria, detecção de incidentes e investigação de eventuais irregularidades.
- **Segurança de dispositivos e redes**: computadores, dispositivos móveis e sistemas devem ser protegidos por controles técnicos, como criptografia, antivírus, firewalls e políticas de bloqueio automático, garantindo que acessos não autorizados sejam prevenidos.

O controle de acesso na **T2M** assegura que os dados corporativos, incluindo informações confidenciais e dados pessoais, sejam protegidos contra acessos indevidos, vazamentos e uso inadequado, fortalecendo a segurança da informação e a conformidade legal.

4.4 Da Proteção de Dados Pessoais

O tratamento de dados pessoais na **T2M** deve obrigatoriamente respeitar a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), a Políticas de Privacidade e demais políticas internas da **T2M**.

Os dados pessoais devem ser coletados apenas quando necessários, tratados com base legal adequada e protegidos durante todo o ciclo de vida, desde a coleta até a eliminação ou anonimização. Devem ser implementados controles técnicos e administrativos compatíveis com o risco envolvido, assegurando a confidencialidade, integridade e disponibilidade das informações.

O acesso aos dados pessoais deve ser restrito a colaboradores autorizados, de acordo com suas funções e responsabilidades, e qualquer compartilhamento com terceiros deve ocorrer somente mediante base legal e contratos que assegurem o cumprimento da LGPD.
Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar o "Privacy by Design / Privacidade desde a concepção e Privacy by Default / Privacidade por padrão".

O descumprimento das regras de proteção de dados pessoais configura violação da política interna e da legislação vigente, sujeitando os responsáveis a medidas administrativas, civis e criminais conforme a gravidade da infração.

4.5 Do Uso Aceitável dos Ativos de TI

Os ativos de tecnologia da informação da **T2M**, incluindo computadores, dispositivos móveis, sistemas, redes, softwares e demais recursos digitais, devem ser utilizados exclusivamente para fins profissionais, relacionados às atividades da empresa.

O uso dos ativos deve obedecer às seguintes diretrizes:

- **Instalação de softwares**: é expressamente proibida a instalação de programas ou aplicativos sem prévia autorização da área de TI, garantindo que todos os softwares utilizados estejam licenciados, atualizados e livres de vulnerabilidades.
- **Dispositivos pessoais (BYOD)**: a utilização de dispositivos pessoais para atividades da **T2M** só é permitida mediante autorização formal e a adoção de medidas de segurança, como criptografia, antivírus e autenticação segura, para proteger as informações corporativas.
- **Proteção da informação**: todos os usuários devem zelar pela confidencialidade, integridade e disponibilidade das informações acessadas ou armazenadas nos ativos de TI, evitando compartilhamento não autorizado, exposição de dados pessoais ou corporativos e práticas que possam comprometer a segurança.
- **Conduta responsável**: é proibido utilizar os recursos tecnológicos para fins ilegais, prejudiciais, discriminatórios ou que violem políticas internas, normas de conduta ou legislação vigente.

- **Monitoramento**: a **T2M** se reserva o direito de monitorar o uso dos ativos de TI, observando a conformidade com esta política, com comunicação prévia quando exigido por lei.

O cumprimento dessas diretrizes assegura que os recursos tecnológicos sejam utilizados de maneira segura, eficiente e alinhada aos objetivos da empresa, minimizando riscos de incidentes de segurança, perdas de informação ou impactos legais.

4.5.1 Dos Computadores e Recursos de TIC

Todos os equipamentos e recursos tecnológicos disponibilizados aos colaboradores são propriedade da **T2M**, devendo ser utilizados exclusivamente para atividades relacionadas aos interesses da empresa, em conformidade com esta Política de Segurança da Informação e os procedimentos operacionais definidos pelas gerências responsáveis.

É proibido realizar qualquer manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de equipamentos sem o conhecimento prévio e acompanhamento de um técnico da Gerência de Tecnologia, ou de pessoa por ela designada. As gerências que necessitarem realizar testes devem solicitar autorização prévia à Gerência de Tecnologia, permanecendo responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança de sistemas operacionais ou aplicativos devem ser implementadas apenas após validação no ambiente de homologação e disponibilização oficial pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter softwares antivírus instalados, ativados e atualizados permanentemente. Caso haja suspeita de vírus ou falhas de funcionamento, o usuário deve comunicar imediatamente à Gerência de Tecnologia.

A transferência ou divulgação de softwares, programas ou instruções de computador para terceiros só pode ser realizada com identificação formal do solicitante, verificação da necessidade e compatibilidade com a classificação da informação.

Arquivos pessoais ou não relacionados ao negócio da **T2M** (fotos, músicas, vídeos, etc.) não devem ser armazenados nos drives de rede. Caso sejam identificados, poderão ser excluídos, sem a necessidade de comunicação prévia ao usuário.

Documentos essenciais para atividades corporativas devem ser salvos em drives de rede, garantindo backup e segurança, pois arquivos armazenados localmente (ex.:

drive C:) são de responsabilidade do usuário e podem ser perdidos em caso de falha do equipamento.

Colaboradores com contas privilegiadas não devem executar comandos ou programas que possam sobrecarregar a rede corporativa sem autorização prévia da Gerência de Tecnologia.

Além das disposições acima, as diretrizes abaixo são imprescindíveis para uso dos computadores, equipamentos e recursos de informática da **T2M**:

- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo sem a previa autorização da Gerência de Tecnologia.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização previa.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela **T2M**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação, assumindo a responsabilidade como custodiante de informações.
- Todos os recursos tecnológicos adquiridos pela **T2M** devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

É expressamente proibido:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

4.5.2 Dos Dispositivos Móveis

Por "dispositivo móvel" entende-se qualquer equipamento eletrônico com mobilidade, como notebooks, smartphones, HDs e pendrives.
A **T2M** permite o uso de equipamentos portáteis pessoais para acesso a sistemas e dados corporativos. Qualquer colaborador que deseje utilizar equipamentos portáteis particulares ou conectar acessórios pessoais à rede da **T2M** deve submetê-los previamente ao processo de autorização da Gerência de Tecnologia, garantindo conformidade com esta política.

É obrigação do colaborador que utilize dispositivos móveis:

- Realizar cópias de segurança (backup) periódicas dos dados armazenados no dispositivo móvel, mantendo os backups separados do próprio equipamento;
- Utilizar senhas de bloqueio automático em todos os dispositivos móveis;
- Não alterar configurações de sistemas operacionais, especialmente relacionadas à segurança e geração de logs, sem autorização formal da Gerência de Tecnologia;
- Não instalar ou manter programas ou aplicativos não autorizados;
- Não realizar reprodução não autorizada de softwares instalados nos dispositivos fornecidos, constituindo o uso indevido do equipamento e sob pena de infração legal aos direitos autorais do fabricante;
- Notificar imediatamente seu gestor direto e a Gerência de Sistemas em caso de furto ou roubo do dispositivo, além de registrar boletim de ocorrência junto às autoridades policiais.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, fornecedores e clientes.

O colaborador assume total responsabilidade pelo uso adequado do dispositivo móvel, respondendo por quaisquer danos diretos ou indiretos, presentes ou futuros, causados à **T2M** ou a terceiros em decorrência de uso indevido.

4.5.3 Do Uso do Correio Eletrônico Corporativo

O correio eletrônico da **T2M** destina-se exclusivamente a fins corporativos, vinculados às atividades do colaborador dentro da empresa. O uso para fins pessoais é proibido, assim como o uso das credenciais corporativas (@t2mlab.com) em sites ou redes sociais de caráter pessoal.

É expressamente proibido aos colaboradores da **T2M**:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto quando relacionadas a atividades legítimas da empresa;
- Enviar mensagens utilizando o endereço eletrônico de seu departamento ou qualquer outro, o nome de usuário de outra pessoa ou qualquer endereço eletrônico não autorizado;
- Enviar mensagens que exponham o remetente e/ou a **T2M** a riscos legais, civis ou criminais;
- Divulgar informações não autorizadas, imagens de tela, documentos, sistemas ou quaisquer ativos de informação sem permissão formal e expressa do proprietário;
- Falsificar informações de endereçamento ou adulterar cabeçalhos com o objetivo de ocultar a identidade de remetentes ou destinatários;
- Apagar mensagens pertinentes quando estas estiverem sujeitas a investigação interna ou legal;
- Produzir, transmitir ou divulgar mensagens que:

    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da **T2M**;
    - o contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    - o contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - o vise obter acesso não autorizado a outro computador, servidor ou rede;
    - o vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - o vise burlar qualquer sistema de segurança;
    - o vise vigiar secretamente ou assediar outro usuário;
    - o vise acessar informações confidenciais sem explícita autorização do proprietário;
    - o vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - o inclua imagens criptografadas ou de qualquer forma mascaradas;

- o contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet) e
- o tenha conteúdo considerado impróprio, obsceno ou ilegal;
- o seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- o contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- o tenha fins políticos locais ou do país (propaganda política);
- o inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

O cumprimento desta norma é obrigatório, sendo parte integrante das políticas de segurança da informação da **T2M**. Violações podem resultar em medidas disciplinares, incluindo sanções administrativas e legais, garantindo a proteção das informações, ativos digitais e da reputação da empresa.

4.5.4 Do Uso da Internet

O uso da internet na **T2M** deve ser pautado por comportamento ético, profissional e responsável, equilibrando os benefícios da conectividade com a proteção dos ativos de informação da empresa. Embora a conexão permanente da rede corporativa com a internet ofereça inúmeras vantagens, ela também expõe a empresa a riscos significativos de segurança e integridade das informações.

Toda informação acessada, transmitida, recebida ou produzida por meio da internet está sujeita a auditoria e monitoramento. Nesse sentido, a **T2M**, em plena conformidade com a legislação brasileira, reserva-se o direito de monitorar e registrar todos os acessos, assegurando a segurança, integridade e disponibilidade dos dados e sistemas.

Os equipamentos, tecnologias e serviços fornecidos para acesso à internet são propriedade da empresa. A **T2M** pode analisar, bloquear ou restringir o uso de arquivos, sites, domínios, correios eletrônicos ou aplicativos, seja em discos locais, estações de trabalho ou áreas privadas da rede, sempre com o objetivo de garantir o cumprimento desta Política de Segurança da Informação.

Toda tentativa de alteração de parâmetros de segurança sem credenciamento e autorização prévia será considerada inadequada, com os riscos informados ao colaborador e ao gestor responsável. O uso indevido dos recursos para atividades ilícitas poderá gerar medidas disciplinares e responsabilização civil e criminal, com a cooperação da empresa junto às autoridades competentes.

A internet disponibilizada pela **T2M** pode ser utilizada para fins pessoais, desde que não comprometa a produtividade, a banda de rede em horários comerciais ou gere conflito de interesse com os objetivos do negócio. O acesso a sites de notícias e serviços é permitido, observando sempre estas restrições.

A cópia, captura de tela, impressão ou envio de imagens da tela para terceiros só é permitida a colaboradores autorizados, respeitando normas internas, legislação de direitos autorais, proteção à imagem prevista na Constituição Federal e demais dispositivos legais. É proibido o compartilhamento indevido de informações administrativas em listas de discussão, sites, comunidades online, salas de bate-papo, comunicadores instantâneos ou tecnologias correlatas.
O download de programas deve estar estritamente ligado às atividades da **T2M** e possuir autorização da Gerência de Tecnologia, incluindo regularização de licenças e registros. É expressamente proibido o uso, instalação, cópia ou distribuição de softwares com direitos autorais, marca registrada ou patente, bem como o download ou distribuição de software ou dados pirateados. Programas não autorizados serão removidos pela Gerência de Tecnologia.

Materiais de cunho sexual não podem ser armazenados, distribuídos, editados, impressos ou gravados em qualquer recurso da empresa. Exceções poderão ser criadas apenas mediante definição de grupos de segurança especiais, autorizados pelos gestores responsáveis.

É proibido efetuar upload de softwares licenciados à **T2M** ou dados da empresa para parceiros e clientes sem autorização expressa do responsável. Também é proibida a utilização dos recursos corporativos para propagar vírus, worms, cavalos de Troia, spam, assédio, perturbações ou programas de controle não autorizados de outros computadores.

O uso de softwares peer-to-peer (como Kazaa, BitTorrent e similares) não é permitido. Serviços de streaming (rádios online, canais de broadcast, entre outros) só podem ser utilizados mediante autorização prévia da Gerência de Tecnologia.

O monitoramento e as regras aplicadas ao uso da internet visam garantir a integridade, confidencialidade e disponibilidade das informações, proteger os ativos de TI e assegurar que os recursos corporativos sejam utilizados de maneira ética e eficiente, em conformidade com a legislação vigente.

4.5.5 Dos Servidores e Equipamentos de Rede

O acesso aos servidores e equipamentos de rede da **T2M** deve ocorrer exclusivamente mediante autorização prévia da Gerência de Tecnologia, e deve seguir as seguintes diretrizes:

I. O usuário com privilégios de administrador permanece sob a responsabilidade exclusiva da Gerência de Tecnologia e não pode ser compartilhado com outros colaboradores, exceto quando autorizado formalmente pelo Comitê de Segurança da Informação.
II. O acesso de visitantes ou terceiros só poderá ser realizado na presença e com acompanhamento de um colaborador autorizado pela **T2M**.
III. A sala de servidores deve ser mantida limpa, organizada e livre de qualquer tipo de lixo ou sujeira. Qualquer procedimento que possa gerar resíduos ou impactar a limpeza do ambiente só poderá ser realizado com autorização prévia da Gerência de Tecnologia.
IV. É expressamente proibida a entrada de alimentos, bebidas, produtos fumígenos ou inflamáveis na sala de servidores.
V. A entrada, retirada ou movimentação de qualquer equipamento da sala de servidores deve ocorrer somente com autorização prévia e registro formal junto à Gerência de Tecnologia, garantindo rastreabilidade e controle de ativos críticos da **T2M**.

4.5.6 Da Rede Sem Fio (Wireless)

A **T2M** fornece infraestrutura de acesso à rede e à Internet por meio de rede sem fio (Wireless), operando nos padrões 2.4 GHz e 5 GHz. Essa rede é segregada, monitorada continuamente e protegida por mecanismos de segurança, incluindo Wireless Intrusion Prevention System (WIPS), com o objetivo de impedir acessos não autorizados e proteger os dispositivos conectados.

O uso da rede corporativa (SSID) é restrito a notebooks e computadores para fins corporativos. Há uma rede específica (SSID) destinada exclusivamente à conexão de dispositivos móveis dos colaboradores, como tablets e smartphones, para acesso à Internet corporativa.

Todos os dispositivos que se conectarem à rede sem fio devem ser previamente cadastrados e autorizados pela Gerência de Tecnologia, garantindo rastreabilidade e conformidade com a política de segurança da informação.

Para visitantes, a **T2M** disponibiliza uma rede separada, cujo tráfego é totalmente segregado da rede corporativa. O acesso a esta rede exige o registro de dados pessoais

do usuário, em conformidade com o Marco Civil da Internet, garantindo a legalidade e segurança do uso.

O monitoramento contínuo e os controles de segurança aplicados à rede sem fio visam garantir a integridade, confidencialidade e disponibilidade das informações corporativas, além de proteger os dispositivos e a infraestrutura de rede contra acessos indevidos.

4.6 Do Monitoramento dos Ambientes de TIC

Para assegurar o cumprimento das diretrizes estabelecidas nesta PSI, a **T2M** poderá adotar medidas de monitoramento e proteção dos seus ambientes de Tecnologia da Informação e Comunicação (TIC), incluindo:

- **Implementação de sistemas de monitoramento** nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis, redes wireless e demais componentes de TI, de modo a gerar informações capazes de identificar usuários, acessos efetuados e materiais manipulados;
- **Divulgação das informações obtidas** pelos sistemas de monitoramento e auditoria quando houver exigência judicial, solicitação formal de gerente ou superior hierárquico, ou determinação do Comitê de Segurança da Informação;
- **Inspeção física dos equipamentos** de propriedade da **T2M**, realizada a qualquer momento, com o objetivo de verificar conformidade e segurança dos ativos de TI;
- **Instalação de sistemas de proteção**, preventivos e detectáveis, destinados a assegurar a segurança das informações e a proteção dos perímetros de acesso, prevenindo incidentes e minimizando riscos à confidencialidade, integridade e disponibilidade dos dados.

O monitoramento será conduzido de forma ética e proporcional, respeitando a legislação brasileira vigente, especialmente no que se refere a proteção de dados pessoais e a privacidade dos colaboradores, garantindo a segurança das operações e a integridade das informações corporativas.

4.7 Da Autenticação e Identificação

Os dispositivos de identificação e senhas são mecanismos essenciais para proteger a identidade dos colaboradores da **T2M**, prevenindo que terceiros se passem por usuários legítimos perante a empresa ou parceiros. O uso indevido de credenciais de outra pessoa configura crime de falsa identidade, nos termos do Art. 307 do Código Penal Brasileiro.

Todos os dispositivos de identificação, incluindo número de registro, crachás, acessos a sistemas, certificados e assinaturas digitais, bem como dados biométricos, devem estar associados inequivocamente a uma pessoa física e vinculados a documentos oficiais reconhecidos pela legislação brasileira.

O usuário é responsável pelo uso correto de seus dispositivos de identificação, bem como pelo cumprimento da legislação civil e criminal. É proibido compartilhar dispositivos ou senhas, salvo em situações específicas autorizadas formalmente pelo gestor competente. No caso de logins compartilhados previamente autorizados, a responsabilidade pelo uso correto será dos usuários que dele se utilizarem, bem como do agente autorizador. É expressamente proibido o compartilhamento de logins com privilégios administrativos.

A Gerência de Tecnologia é responsável pela criação, gerenciamento e manutenção das identidades lógicas dos colaboradores na **T2M**. Devem ser diferenciados visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviço, físicos ou jurídicos. No primeiro acesso à rede, o usuário deve alterar imediatamente sua senha conforme as orientações da Gerência de Tecnologia.

As senhas devem obedecer aos seguintes critérios:

- **Usuários comuns:** mínimo de 12 caracteres, incluindo combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
- **Usuários administradores ou com acesso privilegiado:** mínimo de 16 caracteres, obedecendo aos mesmos critérios de complexidade.

Além disso, é obrigatória a utilização de autenticação multifator (MFA) para todos os acessos a sistemas críticos, aplicações sensíveis ou ambientes que contenham dados pessoais e confidenciais.

As senhas devem ser memoráveis e protegidas adequadamente, sendo vedado:

- Anotar em papel ou armazenar em formato eletrônico legível.
- Utilizar informações pessoais (nome, data de nascimento, CPF, endereço etc.).
- Utilizar sequências triviais ou previsíveis (ex.: “123456”, “abcdefg”).
- Reutilizar credenciais corporativas em sistemas externos.

A troca periódica de senhas não é mais obrigatória, exceto em casos de:

- Suspeita ou evidência de comprometimento.
- Solicitação de auditoria ou investigação de incidente.
- Determinação da Gerência de Tecnologia ou do Comitê de Segurança da Informação.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, incluindo usuários de testes e credenciais temporárias. A área de Gente e Gestão deve comunicar de forma tempestiva à Gerência de Tecnologia quaisquer desligamentos, encerramento de contratos ou término de prestação de serviços, garantindo o bloqueio imediato dos acessos correspondentes.

Em caso de esquecimento de senha, o usuário deverá solicitar formalmente a redefinição por meio do canal oficial ou comparecer pessoalmente à Gerência de Tecnologia, responsável por verificar a identidade do solicitante e cadastrar uma nova senha.

O cumprimento rigoroso destas diretrizes garante a proteção da informação, a integridade dos sistemas e a conformidade da **T2M** com as melhores práticas internacionais de autenticação, incluindo as recomendações do NIST SP 800-63 e da ISO/IEC 27002:2022, em consonância com o modelo de Zero Trust.

4.8 Da Segurança Física

O acesso físico a áreas críticas da **T2M** deve ser restrito a colaboradores autorizados e monitorado continuamente, garantindo a proteção de informações, equipamentos e ativos estratégicos. Todos os acessos devem ser registrados e supervisionados, de acordo com procedimentos internos de controle de entrada e saída.

Documentos impressos contendo informações sensíveis ou confidenciais devem ser armazenados em locais seguros, como armários trancados ou salas de arquivo com controle de acesso. Quando não forem mais necessários, esses documentos devem ser descartados de forma segura, preferencialmente por meio de fragmentadoras ou outro método que garanta a impossibilidade de recuperação ou leitura indevida.

A implementação e manutenção de controles de segurança física visam prevenir acessos não autorizados, perdas, danos ou furtos de informações e ativos da empresa, protegendo a **T2M** e seus colaboradores contra riscos operacionais, legais e de reputação.

4.9 Da Segurança em Redes e Sistemas

Todas as estações de trabalho, servidores e dispositivos móveis da **T2M** devem possuir softwares de proteção atualizados, incluindo antivírus, firewall e demais mecanismos de segurança, bem como receber regularmente atualizações e patches fornecidos pelos fabricantes, a fim de garantir a proteção contra ameaças cibernéticas e vulnerabilidades conhecidas.

O tráfego de rede corporativa deve ser continuamente monitorado por sistemas de detecção e prevenção, visando identificar atividades suspeitas ou não autorizadas, prevenir incidentes de segurança e assegurar a integridade e disponibilidade dos ativos de informação.

O uso de redes públicas para acesso a sistemas ou dados corporativos somente é permitido mediante a utilização de VPN corporativa, garantindo a confidencialidade e integridade das informações transmitidas e prevenindo acessos indevidos.

Todos os colaboradores são responsáveis por seguir as diretrizes de segurança na utilização de redes e sistemas, garantindo o cumprimento desta política e minimizando riscos à **T2M** e aos seus ativos de informação.

4.10 Da Continuidade do Negócio

A **T2M** deve manter plano de continuidade de negócios**,** incluindo backup de dados, recuperação de desastres e manutenção operacional de sistemas críticos, de forma a garantir a disponibilidade, integridade e resiliência das informações e serviços essenciais da empresa.

Todos os procedimentos relacionados à continuidade de negócios devem ser documentados, periodicamente revisados e testados de forma sistemática, garantindo que os planos sejam eficazes e possam ser executados rapidamente em caso de incidentes, falhas de sistemas, desastres naturais ou qualquer evento que comprometa a operação da empresa.

É responsabilidade da Gerência de Tecnologia, em conjunto com o Comitê de Segurança da Informação, assegurar que os testes de continuidade sejam realizados, registrados e que eventuais não conformidades ou melhorias identificadas sejam implementadas de maneira tempestiva.

Todos os colaboradores devem conhecer e seguir as orientações previstas nos planos de continuidade, garantindo a proteção dos ativos da empresa e a manutenção da operação em situações de emergência.

4.11 Da Gestão de Incidentes de Segurança

A **T2M** deverá manter um Plano de Resposta a Incidentes de Segurança da Informação e Privacidade (PRISIP) que estabeleça diretrizes e procedimentos formais para identificação, registro, classificação, tratamento, comunicação e mitigação de incidentes.

Todo incidente que comprometa ou possa comprometer a segurança da informação deverá ser imediatamente comunicado pelos colaboradores, terceiros ou prestadores de serviços aos responsáveis designados, garantindo uma resposta ágil, coordenada e eficaz.

4.11.1 Da Classificação e Severidade

Os incidentes deverão ser classificados em níveis de severidade, considerando impacto, criticidade dos ativos envolvidos e abrangência do evento:

- **Severidade Baixa:** incidentes sem impacto relevante em dados ou operações (ex.: falha pontual contida sem indisponibilidade).
- **Severidade Média:** incidentes que afetam processos ou usuários de forma limitada, sem comprometer informações sensíveis.
- **Severidade Alta:** incidentes que comprometem dados corporativos relevantes, geram indisponibilidade significativa ou afetam terceiros.
- **Severidade Crítica:** incidentes que envolvem vazamento de dados pessoais, indisponibilidade de sistemas críticos ou impactos legais/regulatórios.

4.11.2 Das SLAs de Resposta e Comunicação

O Plano de Resposta a Incidentes deverá definir tempos máximos de resposta (SLAs) para cada nível de severidade, contemplando:

- **Registro inicial:** até 1 hora após a detecção ou reporte.
- **Análise preliminar:** até 4 horas para incidentes críticos e até 8 horas para incidentes de alta severidade.
- **Mitigação inicial:** até 24 horas para incidentes críticos, ou conforme definido no plano para os demais níveis.
- **Comunicação ao Comitê de Segurança da Informação:** imediata em incidentes críticos e em até 24 horas nos demais casos.

4.11.3 Da Notificação Regulatória e a Titulares de Dados

Nos incidentes que envolvam dados pessoais, a **T2M** deverá assegurar o cumprimento dos prazos legais para comunicação à ANPD e aos titulares afetados, conforme gravidade e impacto do evento, garantindo a transparência e a conformidade com a LGPD.

4.11.4 Do Registro e Lições Aprendidas

Cada incidente deverá ser registrado, analisado e tratado de acordo com sua gravidade, com documentação mantida para fins de rastreabilidade, auditoria e conformidade regulatória.

As lições aprendidas deverão ser sistematicamente incorporadas às políticas, processos e controles da **T2M**, promovendo melhoria contínua e resiliência organizacional.

4.11.5 Das Responsabilidade

Para assegurar uma resposta eficiente a incidentes de segurança da informação, é fundamental que cada papel envolvido compreenda suas responsabilidades específicas, garantindo rápida comunicação, análise técnica adequada e supervisão estratégica. A seguir, detalham-se as responsabilidades de cada grupo:

- **Colaboradores e Terceiros:** reportar imediatamente qualquer incidente, real ou suspeito, garantindo rápida comunicação e suporte às ações de contenção.
- **Gerência de Tecnologia:** conduzir a análise técnica dos incidentes, aplicar medidas de contenção apropriadas e coordenar a recuperação dos sistemas e dados afetados.
- **Comitê de Segurança da Informação:** supervisionar o gerenciamento de incidentes, aprovar comunicações externas relacionadas e propor melhorias estruturais para reduzir a recorrência e o impacto de futuros incidentes.

4.12 Do Uso de Inteligência Artificial (IA)

A **T2M** reconhece o potencial da Inteligência Artificial (IA) como ferramenta estratégica para apoiar decisões, otimizar processos e gerar insights para o negócio. Contudo, o uso de IA deve ser responsável, seguro e alinhado à legislação vigente, às políticas internas de segurança da informação e às normas de proteção de dados pessoais.

Todos os sistemas e ferramentas de IA utilizados pela **T2M** devem ser avaliados previamente quanto a:

- **Segurança da informação:** garantindo que os dados utilizados, processados ou gerados pela IA estejam protegidos contra acessos não autorizados, alterações indevidas ou vazamentos;
- **Privacidade:** garantindo que informações pessoais e sensíveis sejam tratadas em conformidade com a LGPD e demais normas aplicáveis;
- **Transparência e rastreabilidade:** possibilitando auditoria das decisões e recomendações fornecidas por sistemas de IA, sempre que aplicável;

- **Uso ético:** evitando qualquer forma de discriminação, viés ou decisão automatizada que possa comprometer indivíduos, colaboradores ou terceiros.

É responsabilidade de cada colaborador que utilize ferramentas de IA garantir que:

- Apenas dados autorizados e necessários sejam inseridos nos sistemas;
- Resultados e recomendações provenientes de IA sejam verificados criticamente antes de qualquer decisão corporativa;
- Ferramentas de IA sejam utilizadas exclusivamente para fins profissionais e em conformidade com as diretrizes da **T2M**.

O uso indevido de sistemas de IA, incluindo manipulação de dados, violação de segurança ou exploração para fins pessoais, poderá sujeitar o responsável a medidas disciplinares, civis e criminais, conforme a legislação vigente e as políticas internas da **T2M**.

4.13 Do Monitoramento e Auditoria

A **T2M** reserva-se o direito de monitorar, inspecionar e auditar, de forma contínua e sistemática, todos os ambientes, sistemas, equipamentos e redes sob sua responsabilidade, com o objetivo de preservar a segurança da informação, a conformidade legal e a proteção de seus ativos.

As atividades de monitoramento e auditoria deverão observar os seguintes princípios:

- **Abrangência**: o monitoramento poderá incluir estações de trabalho, servidores, dispositivos móveis, correio eletrônico, acessos à Internet, sistemas corporativos e quaisquer outros recursos tecnológicos da **T2M**.
- **Finalidade**: os registros e informações coletados deverão ser utilizados exclusivamente para fins de segurança, conformidade normativa, prevenção e investigação de incidentes, bem como para atender determinações legais, regulatórias ou de autoridades competentes.
- **Privacidade e Proporcionalidade**: as atividades de monitoramento respeitarão a legislação vigente, incluindo a Lei Geral de Proteção de Dados (LGPD), garantindo que o tratamento de dados seja realizado de forma ética, proporcional e transparente.
- **Registro e Rastreabilidade**: todos os acessos, alterações e eventos relevantes deverão ser devidamente registrados em logs, armazenados em ambiente seguro e preservados conforme as normas internas e requisitos legais.
- **Auditorias Periódicas**: serão realizadas auditorias internas e, quando necessário, auditorias externas, para avaliar a eficácia dos controles de

segurança, a aderência a esta Política e a conformidade com legislações e regulamentos aplicáveis.

- **Acesso aos Registros**: as informações obtidas por meio do monitoramento e auditoria somente poderão ser acessadas por pessoas autorizadas, mediante necessidade comprovada e sob confidencialidade.

O não cumprimento das normas identificadas por meio das atividades de monitoramento e auditoria poderá resultar em medidas corretivas, ações disciplinares e responsabilização conforme a gravidade da ocorrência.

4.14 Do Backup

A **T2M** adota procedimentos formais de cópia de segurança (backup) para garantir a disponibilidade, integridade e recuperação de informações críticas em caso de falhas, incidentes ou desastres.

As diretrizes gerais de backup incluem:

- **Periodicidade**: as cópias de segurança devem ser realizadas de forma rotineira, conforme cronograma definido no Plano de Continuidade de Negócios (PCN).
- **Abrangência**: todos os sistemas, bancos de dados e informações classificadas como críticas ou essenciais para a operação da **T2M** devem estar contemplados nos procedimentos de backup.
- **Armazenamento Seguro**: as cópias devem ser armazenadas em locais seguros, preferencialmente em ambientes segregados da infraestrutura principal, podendo incluir soluções de nuvem ou armazenamento externo.
- **Proteção dos Dados**: os backups devem estar protegidos por criptografia, controles de acesso e demais mecanismos de segurança aplicáveis, assegurando que somente pessoas autorizadas tenham acesso.
- **Testes Periódicos**: deverão ser realizados testes regulares de restauração dos dados, a fim de validar a eficácia do processo e garantir a confiabilidade dos procedimentos.
- **Responsabilidades**: a Gerência de Tecnologia é responsável por planejar, executar, monitorar e documentar o processo de backup, mantendo registros atualizados das cópias realizadas e restauradas.
- **Integração com a Política de Proteção de Dados**: os procedimentos de backup devem estar alinhados à LGPD e às normas internas de proteção de dados, garantindo que informações pessoais sejam tratadas conforme sua classificação e base legal.

O detalhamento técnico das rotinas de backup, responsabilidades específicas, periodicidade e plano de restauração encontra-se descrito no Plano de Continuidade de Negócios da **T2M**.

4.15 Do Descarte de Informações

O descarte de informações, sejam físicas ou digitais, deve ser realizado de forma segura, garantindo que os dados não possam ser recuperados ou utilizados indevidamente, em conformidade com a Política de Segurança da Informação da **T2M**, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais legislações aplicáveis.

Diretrizes:

- Será elaborada e mantida uma Tabela de Temporalidade de Informações, que definirá os prazos de guarda e os procedimentos de descarte para cada tipo de informação, considerando critérios legais, regulatórios, contratuais e de negócio;
- Informações em meio físico (documentos impressos, mídias ópticas, entre outros) devem ser descartadas por métodos seguros, como fragmentação mecânica (trituradores) ou serviços especializados devidamente certificados.
- Informações em meio digital devem ser eliminadas por meio de técnicas que impossibilitem sua recuperação, como sobrescrita segura, destruição física de mídias ou ferramentas tecnológicas reconhecidas.
- É vedado o descarte de documentos, mídias ou dispositivos com informações confidenciais ou dados pessoais em lixo comum, sem a devida inutilização.
- O processo de descarte deve ser registrado, auditável e supervisionado, garantindo rastreabilidade quando aplicável.
- Sempre que envolver dados pessoais ou dados pessoais sensíveis, o descarte deve observar os princípios da necessidade, minimização, finalidade e segurança, previstos na LGPD.
- A Gerência de Tecnologia, em conjunto com as áreas gestoras da informação, será responsável por orientar, supervisionar e garantir a correta aplicação dos métodos e prazos de descarte definidos na Tabela de Temporalidade.
- Todos os colaboradores e terceiros têm o dever de cumprir as regras de descarte estabelecidas, sendo responsabilizados por eventuais desvios ou descumprimentos.

4.16 Da Gestão de Riscos de Segurança da Informação

A **T2M** manterá um processo estruturado, contínuo e sistemático de Gestão de Riscos de Segurança da Informação, em conformidade com a ISO/IEC 27005 e integrado ao

Sistema de Gestão da Segurança da Informação (SGSI) e ao processo corporativo de gestão de riscos.

Esse processo visa assegurar que os riscos relacionados a ativos de informação sejam identificados, avaliados, tratados e monitorados de forma consistente, possibilitando a priorização de investimentos e a resposta tempestiva a ameaças emergentes.

4.16.1 Dos Objetivos

A gestão de riscos de segurança da informação na **T2M** tem como propósito orientar todas as atividades para proteger os ativos críticos, avaliar riscos de forma estruturada e apoiar a tomada de decisões estratégicas da Alta Administração, considerando critérios claros de probabilidade, impacto e conformidade regulatória. Os principais objetivos são:

- Proteger os ativos de informação críticos da **T2M** contra ameaças internas e externas.
- Avaliar riscos considerando probabilidade, impacto e contexto regulatório (incluindo LGPD e normas setoriais aplicáveis).
- Definir estratégias de tratamento (mitigação, aceitação, transferência ou eliminação), com base em critérios objetivos de apetite ao risco.
- Apoiar a Alta Administração na tomada de decisões estratégicas sobre investimentos em segurança e priorização de controles.

4.16.2 Dos Princípios

Esta seção apresenta os princípios que orientam a gestão de riscos de segurança da informação na **T2M**, garantindo que o processo seja contínuo, centrado nos ativos críticos, de responsabilidade compartilhada entre todos os colaboradores e plenamente integrado a outros processos estratégicos, como o Plano de Continuidade de Negócios e a Gestão de Incidentes de Segurança.

Os princípios adotados pela gestão de riscos da segurança da informação são:

- **Ciclo Contínuo:** a gestão de riscos será revisada periodicamente ou sempre que houver mudanças significativas no ambiente tecnológico, regulatório ou de negócio.
- **Base em Ativos:** cada risco será avaliado em relação a dados, processos, pessoas, tecnologias e infraestrutura que suportam as operações.
- **Responsabilidade Compartilhada:** todos os gestores de processo e colaboradores são responsáveis por identificar riscos e apoiar sua mitigação.

- **Integração:** a gestão de riscos de SI estará alinhada ao Plano de Continuidade de Negócios e à Gestão de Incidentes de Segurança, garantindo coerência entre prevenção, resposta e recuperação.

4.16.3 Das Etapas do Processo

O processo de gestão de riscos de segurança da informação na **T2M** segue uma sequência estruturada de etapas, abrangendo desde a definição do contexto e a identificação de ameaças até a avaliação, tratamento, aceitação e monitoramento dos riscos. Essa abordagem assegura consistência, rastreabilidade e efetividade nas ações de mitigação, promovendo a proteção contínua dos ativos de informação. São elas:

I. **Contextualização** – definição do escopo, critérios de aceitação de riscos e metodologias de avaliação.
II. **Identificação de Riscos** – mapeamento de ativos de informação, ameaças, vulnerabilidades e cenários de risco.
III. **Análise de Riscos** – atribuição de níveis de probabilidade e impacto, considerando aspectos financeiros, operacionais, regulatórios e reputacionais.
IV. **Avaliação de Riscos** – comparação com critérios estabelecidos, priorizando riscos significativos em matriz de riscos.
V. **Tratamento de Riscos** – definição e implementação de controles técnicos, administrativos, legais e físicos.
VI. **Aceitação de Riscos** – formalização dos riscos residuais aceitos pela Alta Administração ou Comitê de Segurança da Informação.
VII. **Monitoramento e Revisão** – acompanhamento contínuo dos riscos, avaliação da eficácia dos controles e atualização periódica do registro de riscos.

4.16.4 Das Responsabilidade

Abaixo, encontram-se estabelecidos os papéis e responsabilidades de cada área e função envolvida na gestão de riscos, assegurando que todos os stakeholders, desde o Comitê de Segurança da Informação até os gestores de processos, contribuam de forma coordenada para identificação, análise, tratamento e monitoramento dos riscos:

- **Comitê de Segurança da Informação (CSI):** supervisionar o processo, aprovar critérios e revisar relatórios de risco.
- **Gerência de Tecnologia:** identificar vulnerabilidades técnicas, recomendar medidas corretivas e monitorar riscos operacionais.
- **Gestores de Processos:** mapear riscos em suas áreas, apoiar análise e garantir implementação de controles.
- **Compliance / DPO:** assegurar que riscos envolvendo dados pessoais sejam avaliados conforme a LGPD e demais legislações aplicáveis.

4.16.5 Da Periodicidade

As avaliações e revisões do processo de gestão de riscos, devem ser revisadas periodicamente, de forma a garantir que o monitoramento seja contínuo e que ajustes sejam realizados sempre que necessário, seja por mudanças no ambiente, incidentes ou auditorias. Sendo assim, a revisão dar-se-á:

- **Avaliação formal:** ao menos uma vez ao ano.
- **Revisão extraordinária:** após incidentes relevantes, auditorias externas ou mudanças regulatórias/tecnológicas significativas.

4.16.6 Das Evidências e Registros

Os riscos, planos de tratamento, responsáveis e prazos deverão ser registrados em Matriz de Riscos de Segurança da Informação, mantida pela Gerência de Tecnologia e auditável pelo Comitê de Segurança da Informação.

Esse registro servirá como insumo para auditorias internas, certificações, planejamento estratégico e prestação de contas a órgãos reguladores.

5. Das Responsabilidades Específicas

A responsabilidade em relação à segurança da informação deverá ser explicitamente comunicada já na fase de contratação dos colaboradores ou prestadores de serviço e fornecedores, em geral. Todos os profissionais, ao serem admitidos, deverão receber orientação formal sobre os procedimentos de segurança, bem como sobre o uso correto e responsável dos ativos corporativos, a fim de reduzir riscos operacionais e de segurança.

Para formalizar esse compromisso, todo colaborador deverá assinar, como condição imprescindível para acesso aos ativos de informação da **T2M**, um Termo de Responsabilidade, no qual reconhece suas obrigações e compromete-se a cumprir integralmente a Política de Segurança da Informação e demais normas internas, bem como a não utilizar, revelar ou divulgar a terceiros qualquer informação obtida em razão de suas funções, seja confidencial ou não, mesmo após o término do vínculo contratual.

5.1 Dos Colaboradores

Todos os colaboradores da **T2M**, incluindo funcionários, prestadores de serviços, estagiários e similares, em qualquer nível hierárquico, são responsáveis por cumprir e

zelar pela efetiva aplicação das normas e princípios de Segurança da Informação, observando especialmente os critérios legais, éticos e regulatórios aplicáveis à **T2M**.

É de inteira responsabilidade de cada colaborador qualquer prejuízo ou dano causado à **T2M** ou a terceiros, decorrente do descumprimento das diretrizes e normas estabelecidas nesta Política.

Cabe a todos os colaboradores adotar as seguintes práticas:

- Cumprir integralmente as políticas, normas e procedimentos de Segurança da Informação, incluindo as disposições desta Política;
- Buscar orientação de seu superior ou da área responsável em caso de dúvidas relacionadas à Segurança da Informação;
- Assinar o Termo de Responsabilidade, formalizando ciência e compromisso com o cumprimento da Política de Segurança da Informação e demais normas internas;
- Proteger as informações contra acesso, modificação, divulgação ou destruição não autorizados;
- Assegurar que os recursos tecnológicos sejam utilizados exclusivamente para fins profissionais aprovados e de interesse da **T2M**;
- Zelar pela segurança das informações confidenciais, incluindo todos os dados pessoais aos quais tiverem acesso;
- Cumprir a Lei Geral de Proteção de Dados (LGPD), garantindo que o tratamento de dados pessoais seja realizado em conformidade com as normas da **T2M**;
- Comunicar imediatamente à Gerência de Tecnologia da Informação (GTI) qualquer descumprimento ou violação desta Política, bem como a áreas responsáveis, quando necessário, incluindo questões administrativas ou de conformidade.

5.2 Dos Gestores de Pessoas e Processos

Os gestores de pessoas e processos devem adotar uma postura exemplar em relação à segurança da informação, servindo como modelo de conduta para todos os colaboradores sob sua supervisão.

Cabe a eles:

- Atribuir responsabilidades aos colaboradores durante a contratação ou formalização de contratos de trabalho, prestação de serviços ou parcerias, garantindo que compreendam e se comprometam a cumprir a Política de Segurança da Informação (PSI) da **T2M**;

- Exigir a ciência e assinatura da PSI pelos colaboradores, assegurando que compreendam suas obrigações, incluindo o dever de manter sigilo e confidencialidade sobre todos os ativos de informação, mesmo após o término do vínculo com a empresa;
- Solicitar a assinatura do Termo de Confidencialidade para colaboradores temporários ou prestadores de serviços que não estejam cobertos por contrato existente, como durante levantamentos para propostas comerciais;
- Adaptar normas, processos, procedimentos e sistemas sob sua responsabilidade para assegurar conformidade com a PSI, promovendo a aplicação efetiva das diretrizes de segurança da informação na operação de suas áreas;
- Monitorar o cumprimento da PSI pelos colaboradores sob sua gestão e apoiar ações corretivas em caso de descumprimento, reforçando a cultura de segurança da informação na **T2M**.

5.3 Da Gerência de Tecnologia

A Gerência de Tecnologia é responsável por planejar, implementar, operar e monitorar todos os sistemas, equipamentos e ativos de informação da **T2M**, garantindo a conformidade com a Política de Segurança da Informação (PSI) e demais normas internas.

Entre suas atribuições estão:

- Testar a eficácia dos controles de segurança e informar os gestores sobre os riscos residuais, acordando com eles os níveis de serviço e os procedimentos de resposta a incidentes;
- Configurar equipamentos, sistemas e ferramentas fornecidos aos colaboradores, garantindo todos os controles necessários para atender aos requisitos de segurança da PSI;
- Permitir que administradores e operadores de sistemas acessem arquivos e dados de outros usuários apenas quando necessário para execução de atividades operacionais, como manutenção, backups, auditorias ou testes;
- Segregar funções administrativas, operacionais e educacionais para minimizar privilégios, evitando que usuários possam alterar logs ou trilhas de auditoria de suas próprias ações;
- Garantir segurança especial para sistemas com acesso público, mantendo evidências que permitam rastreabilidade para auditorias ou investigações;
- Gerar e manter trilhas de auditoria com nível de detalhe suficiente para rastrear falhas e fraudes, aplicando controles de integridade para validação jurídica;
- Administrar, proteger e testar backups de programas e dados relacionados a processos críticos;

- Implantar controles auditáveis para retirada e transporte de mídias, garantindo a supervisão completa da TI;
- Informar o gestor da informação sobre o fim do prazo de retenção para permitir alterações antes do descarte definitivo;
- Garantir que, em movimentações internas de ativos de TI, informações de usuários anteriores não sejam removidas de forma irrecuperável antes de disponibilizar o ativo a outro usuário;
- Planejar, implantar e monitorar capacidade de armazenamento, processamento e transmissão, garantindo a segurança exigida pelas áreas de negócio;
- Atribuir responsabilidades claras sobre contas e dispositivos de acesso:
  - Usuários individuais de funcionários serão responsabilidade do próprio colaborador;
  - Usuários de terceiros serão responsabilidade do gestor da área contratante.
- Proteger continuamente os ativos de informação contra código malicioso, permitindo que novos ativos sejam integrados ao ambiente somente após verificação de segurança;
- Garantir que mudanças em ambiente de produção não introduzam vulnerabilidades, aplicando auditoria de código e cláusulas contratuais de responsabilização quando houver terceiros envolvidos;
- Definir regras formais para instalação de software e hardware em produção, assegurando cumprimento rigoroso;
- Responsabilizar-se pelo uso, guarda e manuseio de assinaturas e certificados digitais;
- Garantir, mediante solicitação formal, o bloqueio imediato de acessos de usuários em casos de desligamento, incidentes ou investigações;
- Assegurar que todos os servidores, estações e dispositivos com acesso à rede operem com o relógio sincronizado com servidores oficiais de tempo do governo brasileiro;
- Monitorar continuamente o ambiente de TI, gerando indicadores e históricos sobre:
  - Uso da capacidade instalada de rede e equipamentos;
  - Tempo de resposta no acesso à internet e aos sistemas críticos;
  - Incidentes de segurança (vírus, trojans, acessos indevidos, furtos, etc.);
  - Atividade de colaboradores durante acessos às redes externas, incluindo internet, e-mails e transferência de arquivos.

5.4 Do Comitê de Segurança da Informação, Privacidade e Proteção de Dados

O Comitê de Segurança da Informação, Privacidade e Proteção de Dados (CSIPPD) será composto pelos seguintes membros permanentes:

I. Chief Executive Officer (CEO).

II. Chief Compliance Officer (CCO).
III. Encarregado de Dados (DPO).
IV. Chief Information Security Officer (CISO).

O CSI poderá contar com o apoio de especialistas internos ou externos, sempre que houver necessidade de conhecimento técnico específico para análise, auditoria ou implementação de medidas de segurança.

Poderão ser convidados, conforme a pauta e a critério do Comitê, representantes de outras áreas da empresa, como Jurídico, Tecnologia da Informação, Recursos Humanos, Auditoria Interna, entre outros, cuja participação se revele necessária ou estratégica.

Compete ao Comitê de Segurança da Informação:

I. Estabelecer e revisar diretrizes, políticas e normas relacionadas à segurança da informação e à proteção de dados;
II. Avaliar riscos, ameaças e vulnerabilidades associados aos ativos de informação da organização, propondo e acompanhando a implementação de medidas técnicas e organizacionais adequadas;
III. Apoiar a implementação e o monitoramento contínuo de controles administrativos, técnicos e jurídicos que visem à mitigação de riscos;
IV. Supervisionar ações de resposta a incidentes de segurança da informação, incluindo a análise de causas, impactos e definição de medidas corretivas;
V. Garantir a aderência às legislações e regulamentações vigentes, em especial a Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018);
VI. Promover a cultura organizacional voltada à segurança da informação e privacidade de dados;
VII. Apoiar a Alta Administração em decisões estratégicas que envolvam riscos e investimentos em segurança e proteção da informação.

6. Da Gestão de Terceiros

A **T2M** reconhece que a segurança da informação não se limita ao ambiente interno da organização, mas também depende do nível de proteção adotado por fornecedores, parceiros e prestadores de serviços. Assim, estabelece-se que:

6.1 Dos Requisitos Contratuais

Todos os contratos com terceiros deverão conter cláusulas específicas de segurança da informação, prevendo:

- Obrigação de conformidade com esta Política, legislações aplicáveis (incluindo a LGPD) e normas técnicas relevantes.
- Compromisso de confidencialidade e proteção de dados.
- Dever de notificação imediata de incidentes de segurança que possam afetar a **T2M** ou seus clientes.
- Garantias de continuidade de serviços críticos em caso de falhas ou incidentes.
- Permissão para auditorias, avaliações ou solicitações de evidências de conformidade, quando necessário.

6.2 Do Due Dilligence de Segurança

A contratação de novos fornecedores dependerá de processo formal de due diligence, que deverá contemplar:

- Avaliação do nível de criticidade do serviço ou produto em relação aos ativos de informação da **T2M**.
- Análise da postura de segurança do fornecedor, incluindo políticas internas, certificações (ex.: ISO 27001, SOC 2, PCI DSS) e histórico de conformidade.
- Verificação da localização geográfica de data centers e subcontratados, com atenção a legislações de proteção de dados aplicáveis.
- Exigência de controles mínimos de proteção, como criptografia, gestão de acessos e plano de resposta a incidentes.

6.3 Do Monitoramento Contínuo

Fornecedores considerados **críticos ou de alto risco** deverão ser submetidos a processos periódicos de monitoramento e avaliação, que poderão incluir:

- Questionários de conformidade.
- Auditorias técnicas ou documentais.
- Indicadores de desempenho e conformidade com SLAs de segurança definidos contratualmente.

6.4 Das Responsabilidades

A gestão de riscos associados a terceiros exige atuação coordenada entre diferentes áreas da **T2M**. Cada unidade envolvida deve assumir papéis específicos, garantindo que os processos de contratação, monitoramento e auditoria de fornecedores sejam conduzidos de forma eficaz e alinhada às diretrizes desta Política.

- **Gestores de Contratos:** devem garantir que cláusulas de segurança sejam incorporadas em todos os contratos relevantes.

- **Gerência de Tecnologia:** deve avaliar riscos técnicos e acompanhar a conformidade dos fornecedores críticos.
- **Comitê de Segurança da Informação:** responsável por revisar a estratégia de gestão de terceiros, priorizar fornecedores de maior impacto e propor medidas corretivas quando necessário.

7. Do Desenvolvimento Seguro (DevSecOps / SDLC)

A **T2M** assegurará que a segurança da informação esteja incorporada em todas as fases do ciclo de vida de desenvolvimento de software (SDLC), adotando práticas de DevSecOps para garantir que sistemas, aplicações e soluções tecnológicas sejam projetados, implementados e mantidos com níveis adequados de proteção.

7.1 Dos Objetivos

O processo de desenvolvimento seguro deve:

- Prevenir vulnerabilidades desde a fase inicial de concepção das soluções.
- Assegurar conformidade com legislações e normas aplicáveis.
- Reduzir riscos de falhas em sistemas internos e externos.
- Promover a cultura de security by design e privacy by design.

7.2 Das Boas Práticas

Para garantir a aplicação efetiva desses objetivos, deverão ser seguidas as seguintes práticas:

- Integração de ferramentas automatizadas de segurança no pipeline de DevSecOps (SAST, DAST, SCA).
- Revisão obrigatória de código por pares antes da promoção a ambientes produtivos.
- Adoção de frameworks reconhecidos, como o OWASP Top 10 e o NIST SSDF (Secure Software Development Framework).
- Implementação de modelagem de ameaças (threat modeling) já na fase de requisitos.
- Registro de todas as medidas de segurança aplicadas em cada etapa do ciclo de vida, garantindo rastreabilidade.

7.3 Das Normas e Frameworks de Referência

O processo de desenvolvimento seguro da **T2M** deverá observar, de forma obrigatória, as seguintes normas e frameworks de referência:

- **ISO/IEC 27034** – Segurança em Aplicações;
- **ISO/IEC 27002:2022** – Controles de segurança da informação;
- **NIST SSDF (Secure Software Development Framework)** – Estrutura para desenvolvimento seguro;
- **OWASP Top 10** – Práticas recomendadas de segurança para aplicações web.

Essas referências deverão ser utilizadas como base mínima de conformidade, podendo ser complementadas por outras normas ou boas práticas reconhecidas pelo mercado e aplicáveis ao contexto da **T2M**.

7.4 Das Diretrizes de Aplicação por Fase

Para assegurar a incorporação efetiva de controles de segurança no ciclo de vida de desenvolvimento de software, a **T2M** adota as seguintes diretrizes por fase:

- **Requisitos:** identificar riscos de segurança e privacidade relacionados à solução, documentando medidas preventivas e requisitos de conformidade (ex.: LGPD, padrões de criptografia).
- **Desenvolvimento:** utilizar ferramentas de análise estática de código (SAST) e revisar o código obrigatoriamente por pares, garantindo aderência a padrões seguros de programação.
- **Testes:** executar testes dinâmicos (DAST) e simulações de ataque (pentests), validando a resiliência contra vulnerabilidades conhecidas e emergentes.
- **Implantação e Operação:** adotar monitoramento contínuo de vulnerabilidades, gestão proativa de patches e revisões periódicas de segurança, assegurando a manutenção de níveis adequados de proteção.

8. Do Treinamento e Conscientização

A **T2M** manterá um programa contínuo de treinamento e conscientização em segurança da informação, estruturado para transformar o conhecimento em prática diária e reforçar a cultura de segurança em toda a organização.

O programa contemplará:

- **Treinamentos obrigatórios** sobre segurança da informação, cibersegurança e proteção de dados pessoais, assegurando que todos os colaboradores compreendam as políticas, normas e procedimentos internos.
- **Campanhas periódicas de conscientização**, promovendo lembranças contínuas sobre boas práticas e comportamento seguro.

- **Simulações práticas**, como testes de phishing e exercícios de resposta a incidentes, permitindo que os colaboradores apliquem o conhecimento em situações reais.
- **Iniciativas de gamificação**, estimulando engajamento, motivação e aprendizado contínuo de forma interativa.

A participação é obrigatória e será monitorada e registrada, permitindo avaliação constante da efetividade do programa e ajustes para aumentar o engajamento e a aplicabilidade prática das ações. O objetivo final é garantir que os colaboradores não apenas conheçam, mas atuem de forma proativa na proteção dos ativos de informação e na conformidade com a legislação vigente, incluindo LGPD.

9. Das Disposições Finais

O descumprimento das disposições desta Política de Segurança da Informação poderá resultar em medidas disciplinares internas, sanções contratuais e responsabilização legal, conforme a gravidade da infração e a legislação vigente. As penalidades podem incluir advertências, suspensão de acessos, responsabilização civil ou criminal, e outras ações cabíveis para garantir a proteção dos ativos de informação e a conformidade da **T2M**.

Esta política deve ser revisada periodicamente, no mínimo uma vez ao ano, ou sempre que ocorrerem mudanças significativas nos processos, na legislação aplicável ou no ambiente tecnológico da **T2M**. Revisões e atualizações devem ser aprovadas pelo Comitê de Segurança da Informação e pela Diretoria, garantindo que a política permaneça atual, eficaz e alinhada aos objetivos estratégicos da empresa.

Aprovado em 23 de março de 2026.

Arthur Barcelos
Compliance Officer