SISTEMA DE GESTÃO INTEGRADO

Política de Segurança da Informação

PL-SGI-01 REV.02

Sumário

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

1. Introdução

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da **T2M – Test to Market** para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente PSI está baseada nas recomendações propostas na norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação e, orientações de Cyber Security Framework do NIST (CSF NIST), bem como está de acordo com as leis vigentes em nosso país.

2. Objetivos

Os objetivos da PSI são de estabelecer diretrizes que permitam aos colaboradores e clientes da **T2M** seguirem padrões comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da **T2M** quanto à:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Trata-se de um conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os sistemas informatizados críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

3. Aplicação da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. Requisitos da PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da **T2M** a fim de que a política seja cumprida dentro e fora da empresa.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação e, será designado como Comitê de Segurança da Informação.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos da **T2M** um anexo de Acordo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela empresa.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado, conforme o Plano de Resposta à Incidentes.

Um Plano Continuidade de Negócios deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas de gestão em uso na **T2M** ou por terceiros.

A **T2M** exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada na **T2M** por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI acarretará violação às regras internas da empresa e sujeitará o usuário às medidas administrativas e legais cabíveis.

5. Das responsabilidades especificas

5.1. Dos colaboradores

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da empresa.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **T2M** ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

5.2. Dos colaboradores em regime de exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa

de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

5.3. Dos gestores de pessoas e processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da **T2M**.

Exigir dos colaboradores a ciência desta PSI, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **T2M**.

Antes de conceder acesso às informações, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

6. Dos custodiantes de Informações

6.1. Da Gerência de Tecnologia

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes da **T2M**.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção exigindo o seu cumprimento dentro da empresa.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- *uso da capacidade instalada da rede e dos equipamentos;*
- *tempo de resposta no acesso à internet e aos sistemas críticos da T2M;*
- *incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);*
- *atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);*

6.2. Do Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período determinado pelos sócios da T2M.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

- *propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;*
- *propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;*
- *avaliar os incidentes de segurança e propor ações corretivas;*
- *definir as medidas cabíveis nos casos de descumprimento desta PSI.*

7. Do Ambiente Corporativo

Para garantir as regras mencionadas nesta PSI, a **T2M** poderá:

7.1. Do monitoramento dos ambientes de TIC

Para garantir as regras mencionadas nesta PSI, a **T2M** poderá:

- *implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede − a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;*
- *tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;*
- *realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;*
- *instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.*

7.2. Correio Eletrônico

O objetivo desta norma é informar aos colaboradores da **T2M** quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da **T2M** é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição.

A utilização desse serviço para fins pessoais não é permitida, assim como uso das credenciais corporativas **(@t2mlab.com**) em sites ou redes sociais de uso pessoal.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da **T2M**:

- *enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da empresa;*
- *enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;*
- *enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a T2M vulneráveis a ações civis ou criminais;*
- *divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;*
- *falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;*
- *apagar mensagens pertinentes de correio eletrônico quando estiver sujeita a algum tipo de investigação;*
- *produzir, transmitir ou divulgar mensagem que:*
    - *contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da T2M;*
    - *contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;*
    - *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;*
    - *vise obter acesso não autorizado a outro computador, servidor ou rede;*
    - *vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;*
    - *vise burlar qualquer sistema de segurança;*
    - *vise vigiar secretamente ou assediar outro usuário;*
    - *vise acessar informações confidenciais sem explícita autorização do proprietário;*
    - *vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;*
    - *inclua imagens criptografadas ou de qualquer forma mascaradas;*
    - *contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet) e*
    - *tenha conteúdo considerado impróprio, obsceno ou ilegal;*
    - *seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;*
    - *contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;*
    - *tenha fins políticos locais ou do país (propaganda política);*

- *inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.*

7.3. Internet

Todas as regras atuais da **T2M** visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da empresa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a **T2M**, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A **T2M**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

O uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Apenas os colaboradores autorizados pela empresa poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de

imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o *download* somente de programas ligados diretamente às suas atividades na **T2M** e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Gerência de Tecnologia.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Tecnologia.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da **T2M** para fazer o *download* ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar *upload* de qualquer software licenciado à **T2M** ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da **T2M** para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares *peer-to-peer* (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos desde que obtenham prévia autorização para o seu uso na Gerência de Tecnologia.

7.4. Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a **T2M** e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na **T2M**, como o número de registro do colaborador, ou crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a **T2M** e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Gerência de Tecnologia responde pela criação da identidade lógica dos colaboradores na empresa.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 14 (quatorze) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade). Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 60 (sessenta) dias, não podendo ser repetidas as 3 (três) últimas senhas.

Os sistemas críticos e sensíveis da **T2M** e os logins com privilégios administrativos devem exigir a troca de senhas a cada 45 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, a área de Gente e Gestão deverá imediatamente comunicar tal fato à Gerência de Tecnologia, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à Gerência de Tecnologia, responsável para cadastrar uma nova.

7.5. Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da **T2M**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Tecnologia, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Tecnologia, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar à Gerência de Tecnologia.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da **T2M** (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os *drives* de rede dos servidores da **T2M**. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores na empresa deverão ser salvos em *drives* de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da **T2M** detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Tecnologia.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- *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.*

Algumas situações em que é proibido o uso de computadores e recursos tecnológicos da **T2M**:

- *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.*

7.6. Dispositivos Móveis

A **T2M** permite o uso de equipamentos portáteis pessoais para acesso à sistemas e/ou dados corporativos.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da **T2M**, ou aprovado e permitido pelos gestores, como: notebooks, *smartphones* e *pendrives*.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A **T2M**, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na **T2M**, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (*backup*) dos dados de seu dispositivo móvel. Deverá, também, manter estes *backups* separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade da **T2M** e aos seus usuários deverá seguir o mesmo fluxo de suporte já existente e prestado pela Gerência de Tecnologia.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença da Gerência de Tecnologia.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela Gerência de Tecnologia.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela **T2M** constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

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

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela **T2M**, notificar imediatamente seu gestor direto e a Gerência de Sistemas.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à **T2M** e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da **T2M** deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Tecnologia.

7.7. Servidores e equipamentos de rede

O acesso aos servidores e equipamentos de rede somente deverá ser feito com previa autorização da Gerência de Tecnologia.

O usuário "administrador" do ficará de posse da Gerência de Tecnologia exclusivamente e não poderá ser compartilhada com outros colaboradores, a não ser que o Comitê de Segurança da Informação assim o autorize.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

A sala de servidores deverá ser mantida limpa e organizada. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com autorização previa da Gerência de Tecnologia.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável na sala de servidores.

A entrada ou retirada de quaisquer equipamentos da sala de servidores somente se dará com autorização previa e registro da Gerência de Tecnologia.

7.8. Rede sem fio

A **T2M** provê uma infraestrutura de acesso à rede e Internet através de uma rede sem fio (Wireless), utilizando os padrões 2.4GHz e 5GHz. Esta rede é segregada e monitorada continuamente.

A rede corporativa (SSID) somente poderá ser utilizada para a conexão de notebooks e computadores com finalidades corporativas. Existe uma rede (SSID) específica para a conexão de dispositivos móveis dos colaboradores e, esta, deverá ser utilizada somente com este propósito – conexão de dispositivos móveis (*tablets, smartphones*) para acesso à Internet.

Toda a rede sem fio é monitorada e possui sistema de *Wireless Intrusion Prevent System* ativo afim de monitorar e não permitir acessos indevidos à rede e aos dispositivos dos seus usuários.

Todos os dispositivos que farão uso da rede sem fio, deverão ser previamente cadastrados na Gerência de Tecnologia para o registro e autorização.

Existe uma rede para fornecer o acesso à Internet para visitantes e, para acesso à esta rede, os usuários deverá fazer os registros dos dados pessoais do usuário com a finalidade de atender o Marco Civil da Internet. O tráfego da rede de visitante é segregado da rede corporativa.

7.9. Backup

A política de Backup está detalhada no Plano de Continuidade de Negócios, assim como as políticas relacionadas a Proteção de Dados da **T2M**.

Aprovado em 12 de dezembro de 2023.

Arthur Barcelos
Compliance Officer