

## 1. OBJETIVO

A Política de Tecnologia da Informação (TI) da PSM Company tem como objetivo estabelecer diretrizes e princípios para a gestão da Segurança da Informação e privacidade, garantindo a confidencialidade, integridade e disponibilidade das informações críticas da organização.

### 1.1. Missão

Garantir a disponibilidade, integridade, confidencialidade, e da informação necessária para a realização de trabalhos, referentes ou dependentes da área de Tecnologia da Informação da PSM Company.

Esta missão reflete o compromisso da PSM Company em assegurar que a informação crítica relacionada à Tecnologia da Informação seja tratada com o mais alto padrão de cuidado, em conformidade com os princípios essenciais de Segurança da Informação e privacidade. Ao buscar esses objetivos, a organização reforça sua responsabilidade em proteger os ativos de TI, garantindo que a informação seja acessada, utilizada e compartilhada de maneira segura e em conformidade com os requisitos legais aplicáveis.

### 1.2. Diretrizes da Tecnologia da Informação

A PSM Company reconhece a importância estratégica da Tecnologia da Informação (TI) para seus processos e operações diárias. Para garantir a utilização segura e eficaz dos recursos de TI, a organização estabelece as seguintes diretrizes:

- **Segurança da Informação e privacidade:** Priorizamos a Segurança da Informação e privacidade em todos os aspectos da operação, adotando práticas e controles alinhados com os padrões da ISO 27001. A confidencialidade, integridade e disponibilidade da informação são fundamentais. Para mais detalhes consultar: Política de Segurança da Informação e Privacidade.
- **Governança de TI:** Implementamos uma estrutura de governança de TI que alinha os objetivos de TI aos objetivos estratégicos da organização. A tomada de decisões é orientada por políticas claras e alinhadas com as melhores práticas de governança.
- **Gestão de Riscos:** Adotamos uma abordagem proativa para a gestão de riscos de TI, identificando, avaliando e tratando os riscos de Segurança da Informação e privacidade de forma contínua.
- **Continuidade de Negócios:** Implementamos planos de continuidade de negócios que asseguram a resiliência dos sistemas de TI em situações de emergência.

- **Conformidade Legal e Contratual:** Mantemos conformidade com as leis e regulamentações aplicáveis à Segurança da Informação e privacidade, assim como com requisitos contratuais. Nossas práticas de TI são desenvolvidas considerando normas como a ISO 27001 e ISO 27002.
- **Acesso e Controle:** Implementamos políticas de controle de acesso baseadas no princípio do mínimo privilégio. Garantimos que apenas pessoal autorizado tenha acesso aos recursos de TI necessários para suas funções.
- **Conscientização e Treinamento:** Promovemos a conscientização em Segurança da Informação e privacidade entre os colaboradores, proporcionando treinamentos regulares sobre práticas seguras e as políticas de TI.
- **Inovação Responsável:** Buscamos a inovação na utilização de tecnologias emergentes, sempre considerando os impactos na Segurança da Informação e privacidade. A avaliação e teste rigorosos precedem a implementação de novas soluções de TI.
- **Responsabilidade Ambiental:** Adotamos práticas de TI sustentáveis, buscando reduzir o impacto ambiental de nossas operações tecnológicas.

Essas diretrizes refletem o compromisso da PSM Company em utilizar a Tecnologia da Informação como um recurso estratégico, promovendo a eficiência operacional, a Segurança da Informação e privacidade e a inovação sustentável. Todos os colaboradores são incentivados a aderir a essas diretrizes em suas atividades diárias para fortalecer a postura de TI da organização.

## 2. APLICAÇÃO

Se aplica a os colaboradores interno, colaboradores externos e usuários.

## 3. REFERÊNCIAS

N/A.

## 4. DEFINIÇÕES

**PSI:** Política de Segurança da Informação e privacidade ou Programa Segurança da Informação e privacidade;

**TI:** Tecnologia da Informação;

**Backup / Restore:** é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado (restore) em caso de perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

**Software:** é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos **colaboradores e/ou usuários** de computadores é realizada através dele;

**Mídias Removíveis:** dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória e HD externo entre outros;

**USB:** é um tipo de conexão “ligar e usar” que permite a conexão de periféricos sem a necessidade de desligar o computador;

**Modem 3G:** é um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets (com suporte 3G), notebooks, netbooks, etc., objetivando conexão com a internet. O modem 3G recebe e decodifica o sinal digital de alta velocidade transmitindo pelas operadoras de celulares para aparelhos portáteis smartphones e notebooks compatíveis com esta tecnologia.

**Firewall:** é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

## 5. RESPONSABILIDADES

A responsabilidade pela proteção dos ativos corporativos de informação não é apenas da Área da Tecnologia da Informação, mas sim de os colaboradores e/ou usuários. Cada um, colaborador ou usuário, tem de assegurar a confidencialidade, integridade e disponibilidade, , , responsabilidade, não repúdio e confiabilidade das informações, bem como pelo cumprimento da presente Política de Segurança da Informação e privacidade.

Cabe a os colaboradores e/ou usuários cumprir fielmente a Política de Tecnologia da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à Segurança da Informação e privacidade; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à disposição sejam utilizados apenas para as finalidades aprovadas pela PSM Company; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a Organização quando do descumprimento ou violação desta política.

## 6. PROCEDIMENTOS

Todo e qualquer procedimento oriundo desta Política de Tecnologia da Informação é de responsabilidade da gestão da área de tecnologia da informação.

### 6.1. Programa de Segurança da Informação e privacidade

Sendo a Política de Tecnologia da Informação a base para o estabelecimento de todos os padrões de normas e procedimentos, sua abrangência é sobre todos os ambientes tecnológicos da **PSM Company** (como Redes Locais, Intranet, Internet), no qual é estruturado para impulsionar a eficiência operacional, inovação sustentável e a Segurança da Informação e privacidade em todos os aspectos do negócio. Este programa é projetado para atender às necessidades específicas da organização, alinhando-se com os objetivos estratégicos e promovendo uma cultura de excelência em TI.

Portanto, o compromisso de todos, **colaboradores e/ou usuários** no cumprimento das diretrizes estabelecidas, é fundamental para a efetiva implementação da Política de Tecnologia da Informação na **PSM Company**.

Toda e qualquer iniciativa relacionada à definição de normas ou procedimentos, bem como contratação de empresas, aquisição de produtos ou serviços inerentes à tecnologia da informação, deverá ser submetida a Área de Tecnologia da Informação e Diretoria para apreciação e aderência à Política.

### 6.2. Organização

O objetivo da organização da Tecnologia da Informação é promover a gestão corporativa da Segurança da Informação e privacidade para toda **PSM Company**, proporcionando uma proteção efetiva dos ativos tecnológicos e de informação.

Na contratação do **colaborador** ou **usuário**, durante sua integração deve-se incluir tópicos referentes à Segurança da Informação e privacidade, ou mesmo referir-se aos documentos oficiais da **PSM Company** sobre o tema. O contrato, deve, necessariamente, estabelecer que o documento Política de Segurança da Informação e privacidade seja cumprido na íntegra e, ainda, fixar as penalidades decorrentes de qualquer violação das regras de segurança definidas.

A Política de Tecnologia da Informação define as responsabilidades e competências relacionadas às áreas supracitadas.

### 6.3. Violações

São consideradas violações à Política de Tecnologia da Informação as seguintes situações, não se limitando às mesmas:

- a) Quaisquer ações ou situações que possam expor a **PSM Company** à perda financeira ou de imagem, ou de marca, ou de reputação, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- b) Uso indevido de dados e equipamentos corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Gestor da Informação;
- c) Uso de dados, informações, equipamentos, software, sistemas ou recursos tecnológicos adicionais, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, código de ética, código de conduta ou de exigências de organismos reguladores da área de atuação da PSM Company;
- d) A não comunicação imediata de descumprimentos da Política de Segurança da Informação e privacidade, que porventura um colaborador ou usuário venha a tomar conhecimento ou chegar a presenciar;
- e) Efetuar declarações verbais, escritas ou de , em meios de comunicação seja ela mídia digital ou verbal em nome PSM Company ou ainda mencionando a mesma sem que tenha autorização formal para esse fim. Declaração estas de ;

### 6.4. Sanções

A violação a um controle de segurança e tecnologia ou a não aderência à Política de Tecnologia da Informação e suas definições são consideradas faltas graves ou violações, podendo ser aplicadas penalidades ou sanções de acordo com a deliberação, como segue:

- a) Aplicação de sanções trabalhistas previstas em legislação vigente, incluindo dispensa por justa causa;
- b) Abertura de Processo civil ou criminal;
- c) Término ou cessão do contrato de prestação de serviço ou relação comercial;
- d) Imediato ressarcimento dos prejuízos causados à **PSM Company**;
- e) Aplicação de outras ações punitivas constantes na legislação brasileira vigente ou nos códigos de ética, código de conduta e relacionamento, civis e comerciais;
- f) Quando a infração se der em outros países se aplicam as punições relativas ao mesmo além das punições constantes do **item e**;

**Classificação de Nível de Incidente – Contexto Trabalhista**

<b>Tipo</b>	<b>Sanção</b>
Grave	Advertência
Muito Grave	Suspensão
Gravíssimo	Desligamento

**Reincidência:**

- No caso de reincidência nos incidentes considerados Grave passa a ser Muito Grave;
- No caso de reincidência Muito Grave passa a ser, Gravíssimo.

**6.5. Regras Gerais**

As regras abaixo discriminadas aplicam-se a todas as áreas da **PSM Company** assim distribuídas: Área Administrativa, Operação, Comercial-Negócios e Suporte a Negócios.

- a) Atuar em conjunto com a Área de Segurança da Informação e privacidade na elaboração ou desenvolvimento de dispositivos de Segurança da Informação e privacidade, específicos, se necessário;
- b) Reavaliar, periodicamente, as autorizações de os colaboradores e/ou usuários que acessam os ativos de informação sob sua responsabilidade, cancelando os que não tenham mais necessidade de acessar os ativos de informação;
- c) Promover e garantir o treinamento adequado aos **colaboradores e/ou usuários** sob sua responsabilidade;
- d) Envolver a Área de Segurança da Informação e privacidade em qualquer incidente de segurança;
- e) Informar qualquer incidente de segurança a Área de Segurança da Informação e privacidade;
- f) Realizar ações de conscientização em Segurança da Informação e privacidade sob demanda, para toda **PSM Company**, ações estas delegadas pela Área de Segurança da Informação e privacidade;
- g) A **PSM Company** disponibiliza um único e exclusivo e-mail, para cada um de seus colaboradores e este, e somente este, deve ser utilizado pra trocas de informação entre os colaboradores e/ou usuários;
- h) Informar, quando cabível, a Área de Segurança da Informação e privacidade os resultados das revisões independentes e dos testes de acesso, de forma que possam ser elaboradas

as alterações necessárias no Programa de Segurança da Informação e privacidade e os planos de ação necessários para a correção dos desvios.

## **6.6. Regras Específicas**

### **6.6.1. Área – Suporte a Negócios**

Composta pelas áreas de Tecnologia da Informação e Segurança da Informação e privacidade.

A área de Segurança da Informação e privacidade está focada em governança enquanto a área de Tecnologia da Informação se foca em gestão.

Destacamos, mas não se limitando, as principais atividades destas áreas que são: de suporte, manutenção, configuração de máquina, trocas de hardware, instalação de periféricos, instalação de sistema operacional para desktop e servidores (com seus programas), remoção de vírus, spyware e spam, instalação de antivírus para correção de falhas críticas, melhoria de performance e descarte, inventário do parque instalado atualizado para controle e gestão, instalação, configuração e manutenção de Rede Wi-Fi e Internet, rotinas de backup / restore, suporte remoto, telefônico ou presencial com controle, documentação de chamados e notificação aos usuários e manutenções preventivas e/ou corretivas além de gestão de local de restrito.

## **6.7. Regras estabelecidas:**

### **6.7.1. Área de Tecnologia da Informação**

Colaborador de Tecnologia da Informação da **PSM Company**, nomeado como ponto focal e que fornece todos os serviços de Tecnologia da Informação, suporte e manutenção.

#### **Descritivo das Atividades:**

- a) Administrar e monitorar os sistemas de identificação e de autorização de acesso aos sistemas da **PSM Company**;**
- b) Administrar o acesso lógico aos sistemas, rotina, sub-rotinas e programas;**
- c) Receber, diagnosticar, registrar e conduzir para solução os incidentes de segurança ocorridos no âmbito interno da **PSM Company**, reportados pelos **colaboradores** ou não;**
- d) Administrar os processos e ferramentas destinadas à proteção da infraestrutura tecnológica da **PSM Company**;**

- e) Fornecer, acesso e senha aos **colaboradores e/ou usuários** de acordo com as regras de acesso definidas.

#### **6.7.2. Sala de Servidores - Local de Acesso Restrito**

É a pessoa responsável por uma determinada área de acesso restrito e pela manutenção de medidas apropriadas de segurança, podendo delegar esta autoridade a outrem, porém nunca a responsabilidade.

**Descritivo das Atividades:**

- a) Manter controle efetivo do acesso ao local, estabelecendo, documentando e fiscalizando a regras de acesso. As regras de acesso devem, conforme o negócio, definir quais **colaboradores ou usuários** têm real necessidade de acesso;
- b) Manter atualizada a lista de pessoas autorizadas a entrar neste local;
- c) Reavaliar, periodicamente, as autorizações dos **colaboradores ou usuários** que acessam a sala de servidores, sob sua responsabilidade, cancelando a autorização dos que não tenham mais necessidade de acesso;
- d) Controlar, monitorar e manter acompanhamento de no mínimo um colaborador da **PSM Company** para acesso físico de usuário assinando lista e autorizando a entrar no referido local.

#### **6.7.3. Área de Segurança da Informação e privacidade**

A Área de Segurança da Informação e privacidade deve ser composto por pessoas com sólidos conhecimentos em Segurança da Informação e privacidade, inseridas na estrutura organizacional desta Área. Sua responsabilidade básica é manter o Programa de Segurança da Informação e privacidade adequado às necessidades da **PSM Company**, avaliando e determinando impactos de segurança, fornecendo alternativas de eliminação ou redução dos riscos e acolhendo orientações da Diretoria Executiva.

**Descritivo das Atividades:**

- a) Elaborar e manter a Política de Segurança da Informação e privacidade;
- b) Disponibilizar e divulgar a Política de Segurança da Informação e privacidade;
- c) Elaborar e manter as Normas de Segurança da Informação e privacidade;
- d) Criar e manter uma fonte única para todas as informações e documentos referentes ao assunto, de forma a garantir a integridade, coerência e atualização das informações de segurança, disponibilizando-as para toda Organização;

- e) Realizar ações de conscientização em Segurança da Informação e privacidade, para toda Organização, podendo, em alguns casos, delegar estas ações, se necessário;
- f) Reciclar, periodicamente, o treinamento em Segurança da Informação e privacidade para toda Organização;
- g) Emitir, no âmbito de Segurança da Informação e privacidade, parecer para novos projetos;
- h) Assessorar Diretoria no âmbito de Segurança da Informação e privacidade.

**< FIM DO DOCUMENTO >**