

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**SEGURANÇA DA INFORMAÇÃO****PSM Company****Sumário**

1. OBJETIVO	2
2. REFERÊNCIA NORMATIVA.....	2
3. MISSÃO	2
4. CONTROLE DE ARMAZENAMENTO, LOCALIZAÇÃO E ACESSO	2
5. ÁREAS ENVOLVIDAS	2
6. APLICAÇÃO.....	2
7. TERMOS E DEFINIÇÕES.....	2
8. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO	3
9. PROCEDIMENTOS	4
10. AUTORIDADE E RESPONSABILIDADE	4
11. PROGRAMA DE SEGURANÇA DA INFORMAÇÃO	4
12. ORGANIZAÇÃO DA SEGURANÇA	5
12.1. DEFINIÇÃO COLABORADOR E USUÁRIO.....	5
12.2. VIOLAÇÕES	5
12.3. SANÇÕES.....	6
13. REGRAS GERAIS	7
14. REGRAS ESPECÍFICAS	8
14.1. ÁREA – SUPORTE A NEGÓCIOS	8
14.1.1. Área de Tecnologia da Informação	8
14.1.2. Sala de Servidores - Local de Acesso Restrito.....	9
14.1.3. Área de Segurança da Informação.....	9
14.2. ÁREA COMERCIAL / NEGÓCIOS	10
14.3. ÁREA OPERAÇÃO E ADMINISTRATIVA	10

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

1. Objetivo

Gerar regras abrangentes, factíveis para as Áreas de Negócios em geral.

2. Referência Normativa

- ISO 27000: Termos e definições aplicáveis a todas as normas da família 27000;
- ISO 27001:2022 – Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Sistemas de gestão de SI – Requisitos;
- ISO 27002:2022 - Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Controles de SI;
- ISO 27003:2020 – Tecnologia de informação – Técnicas de segurança – SGSI - Orientações;
- ISO 27004:2017 - Tecnologia de informação – Técnicas de segurança – SGSI – Monitoramento, medição, análise e avaliação;
- ISO 27005:2019 – TI – Técnicas de Segurança - Gestão de Riscos de Segurança da Informação;
- ISO 22301:2020 – gestão e resiliência – Sistema de gestão de continuidade de negócios – Requisitos;
- ISO 31000: Gerenciamento de Riscos.
-

3. Missão

Garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da **PSM Company**.

4. Controle de Armazenamento, Localização e Acesso

- Sharepoint

5. Áreas Envolvidas

- Todos os **colaboradores e/ou usuários** que estejam a serviço e disponibilizam de ativos da **PSM Company**;

6. Aplicação

Se aplica a todos os **colaboradores** interno, **colaboradores** externos e **usuários**;

7. Termos e Definições

- **SI**: Segurança da Informação;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

- **PSI:** Política de Segurança da Informação ou Programa Segurança da Informação;
- **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 ponta da rede.

8. Diretrizes de Segurança da Informação

Consulte o documento **DIR001-SI**, para realizar consulta completa sobre este tema.

Seu cumprimento é dever de todos os **colaboradores e/ou usuários** da **PSM Company**, os quais devem obedecer às seguintes Diretrizes de Segurança da Informação:

- ▲ Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
- ▲ Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela **PSM Company**;
- ▲ Garantir que as informações sob sua responsabilidade estejam adequadamente protegidas;
- ▲ Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- ▲ Atender as leis que regulamentam as atividades da **PSM Company** e seu mercado de atuação;
- ▲ Assegurar a confidencialidade, integridade e disponibilidade das informações da **PSM Company** selecionando os mecanismos de segurança da informação, equilibrando fatores de risco, tecnologia e custo;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

- ▲ Comunicar imediatamente à Diretoria da **PSM Company** qualquer descumprimento da Política de Segurança da Informação;

9. Procedimentos

Todo e qualquer procedimento oriundo desta Política de Segurança da Informação é de responsabilidade dos Gestores das respectivas Áreas de Negócios envolvidas;

10. Autoridade e Responsabilidade

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

Cabe a todos os **colaboradores e/ou usuários** cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; 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;

11. Programa de Segurança da Informação

Sendo a Política de Segurança da Informação a base para o estabelecimento de todos os padrões de normas e procedimentos de segurança da informação, sua abrangência é sobre todos os ambientes tecnológicos da **PSM Company** (como Redes Locais, Intranet, Internet).

Portanto, o compromisso de todos, **colaboradores e/ou usuários** no cumprimento das diretrizes estabelecidas, é fundamental para a efetiva implementação da Política de Segurança 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 segurança da informação, deverá ser submetida a Área de Segurança da Informação e Diretoria para apreciação e aderência à Política de Segurança da Informação.

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

	POLÍTICA SEGURANÇA DA INFORMAÇÃO	CÓDIGO: POL001-SI	
		Classificação: INTERNA	Página: 5 de 11

A Política de Segurança da Informação, seus documentos e formas de implementação devem ser mantidos no âmbito interno, não devendo ser divulgados a outros que não os terceiros diretamente envolvidos na operação da **PSM Company**.

12. Organização da Segurança

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

Na contratação do **colaborador** ou **usuário**, durante sua integração deve-se incluir tópicos referentes à segurança da informação, 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 seja cumprido na íntegra e, ainda, fixar as penalidades decorrentes de qualquer violação das regras de segurança definidas.

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

12.1. Definição Colaborador e Usuário

Consulte o documento **NOR001-SI**, para realizar consulta completa sobre este tema.

12.2. Violações

São consideradas violações à Política de Segurança 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 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 outros recursos tecnológicos, 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**;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

- d) A não comunicação imediata de quaisquer descumprimentos da Política de Segurança da Informação, que porventura um **colaborador ou usuário** venha a tomar conhecimento ou chegue a presenciar;
- e) Efetuar declarações verbais, escritas ou de qualquer ordem, em qualquer meio 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 qualquer ordem;

12.3. Sanções

A violação a um controle de segurança ou a não aderência à Política de Segurança 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

Tipo	Sanção
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.

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

13. 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 Tecnologia da Informação na elaboração ou desenvolvimento de dispositivos de Segurança da Informação, específicos, se necessário;
- b) Reavaliar, periodicamente, as autorizações de todos 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 Tecnologia da Informação em qualquer incidente de segurança;
- e) Informar qualquer incidente de segurança a Área de Segurança da Informação;
- f) Realizar ações de conscientização em segurança da informação sob demanda, para toda **PSM Company**, ações estas delegadas pela Área de Segurança da Informação;
- 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 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 os planos de ação necessários para a correção dos desvios;
- i) Solicitar a **todos** Colaboradores da base administrativa da **PSM Company** que **NÃO consomam, sob nenhuma hipótese, alimentos e/ou líquidos nas suas estações de trabalho, pois isto se configura uma violação gravíssima.**
Exceção: A única exceção a isso é a utilização de Garrafa / Squeeze apropriada para acondicionamento de água potável, possibilitando assim o consumo da mesma na estação de trabalho;
- j) Solicitar a todos Colaboradores da base administrativa da **PSM Company** que **desliguem** seus equipamentos que ficam ligados sem o uso imediato (filtros de linha, carregadores de celular, etc.) ou ao término da jornada de trabalho. Equipamentos ligados por tempo indeterminado podem causar princípios de incêndios;
- k) Assegurar que todos os Colaboradores da base administrativa da **PSM Company** usem de forma tempestiva o crachá em local visível;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

14. Regras Específicas

14.1. ÁREA – SUPORTE A NEGÓCIOS

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

A área de Segurança da informação 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.

Regras estabelecidas:

14.1.1. 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;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

14.1.2. 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;

14.1.3. Área de Segurança da Informação

A Área de Segurança da Informação deve ser composto por pessoas com sólidos conhecimentos em Segurança da Informação, inseridas na estrutura organizacional desta Área. Sua responsabilidade básica é manter o Programa de Segurança da Informação 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;
- b) Disponibilizar e divulgar a Política de Segurança da Informação;
- c) Elaborar e manter as Normas de Segurança da Informação;
- 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, para toda Organização, podendo, em alguns casos, delegar estas ações, se necessário;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

- f) Reciclar, periodicamente, o treinamento em segurança da informação para toda Organização;
- g) Emitir, no âmbito de Segurança da Informação, parecer para novos projetos;
- h) Assessorar Diretoria no âmbito de Segurança da Informação;

14.2. ÁREA COMERCIAL / NEGÓCIOS

Composta pelas áreas de Marketing, Prospecção e Vendas.

A principal característica desta área é focar-se totalmente no Cliente e/ou futuro Cliente, trazendo com isto a responsabilidade de comunicação com os mesmos.

Regras estabelecidas:

Descritivo das Atividades:

- a. Definir e atuar como ponto focal para a comunicação interna e externa;
- b. Elaborar textos específicos para divulgação em todos os canais, de forma uniforme, de uma eventual interrupção;
- c. Interagir com os Clientes, em qualquer canal de comunicação, para informá-los de interrupções, duração das mesmas, impactos e retomadas, ocorridos na PSM Company;

14.3. ÁREA OPERAÇÃO e ADMINISTRATIVA

A Área de Operação é composta pelas áreas de Recrutamento e Seleção, Departamento Pessoal e Gestão de Pessoas, enquanto a Área Administrativa é composta pelas áreas de Faturamento, Financeira e Compras-Contratos-Ativos.

Descritivo das Atividades:

- a. Informar tempestivamente área de Tecnologia da Informação sobre qualquer admissão, desligamento ou transferência de **colaboradores e/ou usuários**;
- b. Assegurar que, todos os **colaboradores e/ou usuários**, conheçam suas atribuições e responsabilidades estabelecidas na Política de Segurança da Informação;
- c. Reavaliar em conjunto com a área de Tecnologia da informação, periodicamente, as autorizações dos **colaboradores e/ou usuários** que acessam informação, cancelando os acessos que não tenham mais a necessidade de acessar a informação;
- d. Prover e garantir o treinamento adequado aos **colaboradores e/ou usuários** no ato de sua admissão, desligamento ou transferência;
- e. Aplicar as sanções disciplinares cabíveis, no caso da ocorrência de um incidente de segurança da informação;

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação

- f. Garantir, aos **colaboradores e/ou usuários**, os recursos necessários para manter a segurança física de equipamentos e dispositivos como: armários com trancas, dispositivos de segurança para equipamentos portáteis dentre outros;

<FIM DO DOCUMENTO>

ÁREA RESPONSÁVEL	Criado em	PERIODICIDADE	REVISÃO	VERSÃO	RESPONSÁVEL
Segurança da Informação	Jan/2018	Anual	NOV/2023	V.1.1.1	Segurança da Informação