1. OBJETIVO

Esse manual de gestão tem como objeto sintetizar a estrutura do Sistema de Gestão implementado na **PSM Company** em conformidade com os requisitos da ISO 27001:2022 e ISO 27701:2019.

1.1. Documentos de referência

- Não se aplica

1.2. Definições

- **SGPI - S**istema de **G**estão da **P**rivacidade da **I**nformação;
- **LGPD -** Lei Geral de Proteção de Dados – no Brasil;
- **GDPR –** ***G****eneral* ***D****ata* ***P****rotection* ***R****egulation* (em inglês) ou
  Regulamento Geral de Proteção de Dados (em português);
- **PII (DP)** - ***P****ersonally* ***I****dentifiable* ***I****nformation*.
- **DP – D**ados **P**essoais**;**
- **TI** – **T**ecnologia da **I**nformação;
- **SI** – **S**egurança da **I**nformação;
- **PDCA -** ***P****LAN* – ***D****O* – ***C****HECK* – ***A****CT* (em inglês)
  PLANEJAR – EXECUTAR – CHECAR – AGIR (em português;
- **SWOT** - ***S****trengths,* ***W****eaknesses,* ***O****pportunities e* ***T****hreats* (em inglês) ou
  Forças, Fraquezas, Oportunidades e Ameaças (em português);
- **NC**s - **N**ão **c**onformidade(s);
- **OM**s - **O**portunidades de **m**elhoria(s).

2. CONTEXTUALIZAÇÃO

O SGPI da **PSM Company**, se tornou crucial com o aumento das preocupações com a privacidade dos dados no mundo e a implementação de leis rigorosas de proteção de dados, LGPD.

O SGPI surgiu em um cenário onde a coleta, armazenamento e processamento de DP se tornaram essenciais para as operações comerciais, governamentais e sociais. Com o avanço da tecnologia e a proliferação de serviços digitais, enormes volumes de dados são gerados e compartilhados diariamente, o que cria desafios significativos em relação segurança das informações e à privacidade.

O SGPI é uma resposta estratégica e operacional à necessidade crescente de proteger a privacidade e a segurança dos DP em um mundo digital cada vez mais complexo e interconectado. Ele desempenha um papel fundamental na construção da confiança do público, na mitigação de riscos e na promoção de práticas de tratamento de dados éticas e responsáveis.

Nesse contexto, temos:

- **Compliance Legal:** as leis de proteção de dados estabelecem requisitos rigorosos para o tratamento de informações pessoais. O não cumprimento dessas leis pode resultar em multas substanciais e danos à reputação;
- **Expectativas dos Consumidores:** Os consumidores estão cada vez mais conscientes sobre a importância da privacidade e exigem que as empresas protejam seus DP de forma adequada;
- **Riscos de Segurança:** Os DP são alvos frequentes de hackers e cibercriminosos, representando um risco significativo de violações de segurança e vazamentos de informações;
- **Reputação e Confiança:** Incidentes de segurança e violações de dados podem ter um impacto devastador na reputação de uma organização e na confiança do público;
- **Complexidade Tecnológica:** Com a crescente variedade de sistemas e plataformas utilizados pelas organizações, é desafiador garantir uma proteção consistente e eficaz dos DP.

Diante dessas pressões, o SGPI surge como uma abordagem sistemática para lidar com essas questões. Ele envolve a implementação de políticas, normas, procedimentos (controles, informativos) e tecnologias destinadas a garantir a conformidade com as leis de privacidade, proteger os DP contra ameaças e violações, e promover uma cultura de responsabilidade e transparência em relação ao tratamento de dados.

2.1. Premissas do SGPI

São os princípios fundamentais que norteiam a sua concepção, implementação e operação. Essas premissas são essenciais para garantir que o SGPI atenda aos objetivos de proteção de dados e privacidade da **PSM Company** de forma eficaz e consistente. Algumas das principais premissas de um SGPI incluem:

- **Conformidade:** garantir que o tratamento de DP esteja em conformidade com as leis, regulamentos, políticas e normas aplicáveis relacionadas à privacidade e proteção de dados, incluindo a LGPD - Lei Geral de Proteção de Dados - no Brasil;

- **Transparência e Informação:** promover a transparência no tratamento de DP, informando os titulares sobre como seus dados são coletados, usados e protegidos, bem como quais são seus direitos em relação aos seus dados;
- **Princípio da Finalidade:** garantir que os DP sejam coletados e tratados para finalidades específicas, legítimas e explícitas, e que não sejam utilizados de forma incompatível com essas finalidades;
- **Minimização de Dados:** garantir que apenas os DP necessários para a realização das finalidades pretendidas sejam coletados, e que sejam mantidos apenas pelo tempo necessário para alcançar essas finalidades;
- **Segurança da Informação e Privacidade:** implementar medidas técnicas e organizacionais adequadas para proteger os DP contra acessos não autorizados, vazamentos, perdas, alterações, retenção, exclusão;
- **Responsabilidade e Prestação de Contas:** atribuir responsabilidades aos envolvidos no tratamento de DP e garantir que os processos sejam documentados, monitorados e auditados regularmente para garantir conformidade e transparência;
- **Respeito aos Direitos dos Titulares:** garantir que os direitos dos titulares dos dados sejam respeitados e que mecanismos adequados estejam em vigor para permitir que os titulares exerçam seus direitos, como o direito de acesso, retificação, exclusão e portabilidade de seus DP;
- **Melhoria Contínua:** ser continuamente revisado, avaliado e aprimorado para garantir sua eficácia e conformidade contínuas com as leis e melhores práticas em proteção de dados e privacidade da informação.

Essas premissas formam a base sobre a qual um SGPI é construído e operado, garantindo que a **PSM Company** esteja em conformidade com as leis de proteção de dados, proteja os direitos dos titulares de dados e promova uma cultura de respeito segurança da informação e à privacidade.

2.2. Perfil

A **PSM Company** atua há mais de 15 anos na contratação e alocação de profissionais para as seguintes atividades:

- Desenvolvimento de sistemas;
- Infraestrutura e servidores;
- Redes e sistemas operacionais;

- Banco de dados;
- Suporte – *Service desk e field service*;
- Processos de negócio;
- Qualidade e testes;
- Segurança da informação e privacidade;
- Aplicações.

2.3. Missão, Visão e Valores

2.3.1. Missão

Oferecer soluções em tecnologia e gestão de Recursos Humanos gerando valor a nossos Clientes

2.3.2. Visão

Sermos reconhecidos como referência na prestação de serviços em tecnologia e gestão de Recursos Humanos

2.3.3. Valores

Acreditamos nas Pessoas e nelas investimos seguindo diretrizes como: Ética, Valorização da Diversidade, Transparência e Companheirismo.

Nota: A missão, a visão e os valores da **PSM Company** estão documentados na Análise do Contexto Organizacional.

3. POLÍTICA

A política de segurança da informação e privacidade as políticas específicas por tema foram definidas, aprovadas pela direção, publicadas, comunicadas e reconhecidas pelo pessoal pertinente e partes interessadas pertinentes, e analisadas criticamente em intervalos planejados e quando ocorrem mudanças significativas.

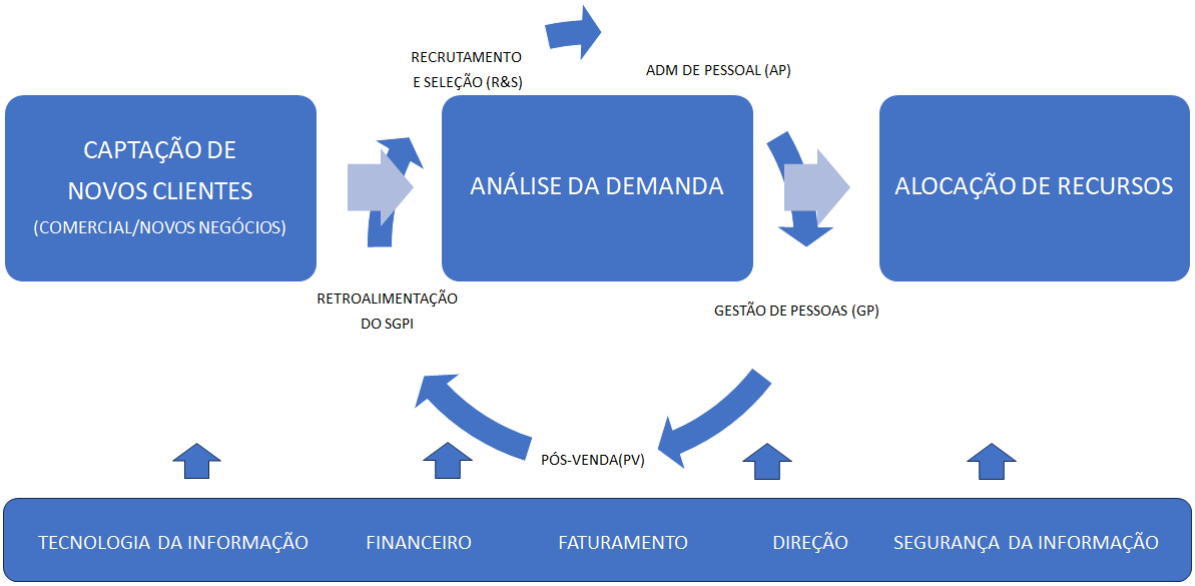
A política do sistema de gestão encontra-se descrita na Análise do Contexto Organizacional.

4. ESCOPO

O escopo define a abrangência do SGPI da **PSM Company** e pode ser evidenciado no documento na Análise do Contexto Organizacional.

4.1. Interação dos Processos

O processo de oferta de serviços consiste na captação de novos clientes pela área de Novos Negócios, análise da demanda e alocação de recursos, pela área de Recrutamento e Seleção, identificação de eventuais necessidades de treinamento, pela área de Gestão de Pessoas, suporte relacionado às questões de documentação, pela área de Administração de Pessoal e suporte ao cliente pela área de Pós-Venda, contando ainda com o apoio das áreas de TI, SI (Compliance), Financeiro (Compras), Faturamento e Direção.



5. ANÁLISE DE RISCOS E OPORTUNIDADES

A **PSM Company** considera estratégicas para o negócio as questões externas e internas que possam resultar em risco ou oportunidade e que afetem ou possam impactar a segurança da informação e privacidade, as partes interessadas e a eficácia do SGPI, com efeitos sob os ativos físicos, financeiros, operacionais, imagem, marca e a sua reputação.

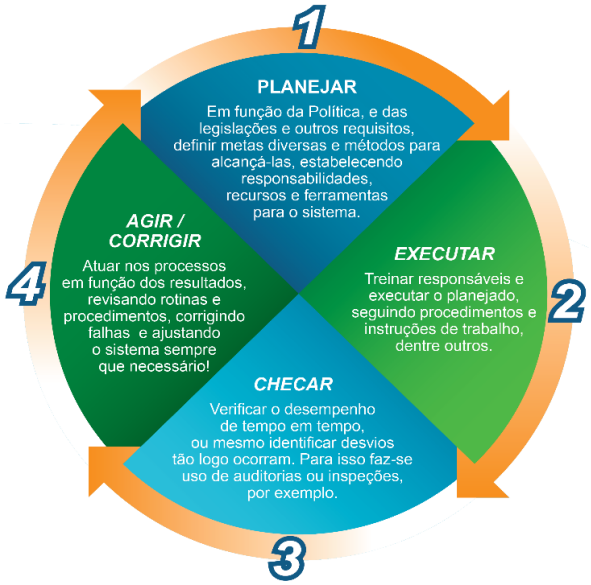
A identificação de riscos e oportunidades pode advir da análise crítica, análise de atendimento ao Procedimento de Requisitos Legais e Outros Requisitos, manifestações de partes interessadas, avaliação de riscos, e a metodologia utilizada para a registro e acompanhamento é a matriz SWOT no documento Análise do Contexto Organizacional.

6. ELEMENTOS DO SGPI

São os componentes fundamentais que constituem a estrutura e operação do sistema - SGPI. Eles são essenciais para garantir que a privacidade dos dados pessoais seja

adequadamente protegida e gerenciada dentro da **PSM Company**, seus principais elementos incluem: Política de Privacidade e Proteção de Dados; Atribuição de Responsabilidades; Avaliação de Riscos; Controles de Segurança da Informação; Procedimentos de Coleta e Consentimento; Gestão de Direitos dos Titulares; Treinamento e Conscientização; Monitoramento e Auditoria; Resposta a Incidentes; Melhoria Contínua. Esses elementos formam a estrutura essencial de um SGPI, fornecendo as bases para uma gestão eficaz da privacidade da informação dentro de uma organização, conforme exigido pelas leis e regulamentos de proteção de dados.

O SGPI é um conjunto de processos definidos que permitem que a **PSM Company** gerencie de forma sistemática suas oportunidades, seus riscos e impactos relacionados à segurança da informação e privacidade. Para tal, é estabelecido um processo sistêmico, refletido em documentos, rotinas de trabalho e registros que visam auxiliar seu melhor desempenho, baseado no ciclo PDCA, para estruturar suas fases e processos. Graficamente, temos:



Este ciclo envolve desde o planejamento de ações à execução, medição do desempenho, correções e melhorias, visando a leitura constante e aperfeiçoamento dos processos, planos de trabalho e demais elementos que constituem o SGPI. Estabelece, assim, as bases para a melhoria contínua, através de lições aprendidas. Cada uma das etapas do ciclo de gestão do SGPI é descrita nos respectivos procedimentos.

6.1. Ciclo PDCA

6.1.1. Planejar

6.1.1.1. Contexto da Organização

A organização analisa seu contexto e identifica riscos e oportunidades de negócio por meio da matriz SWOT no documento Análise do Contexto Organizacional.

6.1.1.2. Requisitos legais e outros requisitos

Sua gestão promove a aderência do SGPI e dos processos organizacionais ligados ao mesmo frente às exigências de legislações em nível federal, estadual e municipal aplicáveis. Por essa razão, também servem de referência na definição dos elementos do SGPI.

Os monitoramentos associados ao atendimento a requisitos legais são realizados e registrados conforme Procedimento de Requisitos Legais e Outros Requisitos.

6.1.1.3. Partes interessadas

Estão definidas na Análise do Contexto Organizacional no documento Análise do Contexto Organizacional.

6.1.1.4. Objetivos, metas e indicadores

Os Objetivos, metas e Indicadores, baseados na Política do SGPI, Procedimento de Requisitos Legais e Outros Requisitos, são estabelecidos de modo a promover e estimular um ambiente de melhoria contínua nos processos considerados significativos e críticos. Além disso, são também elaborados com a expectativa de gerar comprometimento da organização e bom desempenho do próprio sistema. Tal processo está definido no documento Análise do Contexto Organizacional.

Os Objetivos, Metas e Indicadores do SGPI, resumem o conjunto de informações necessárias à gestão e acompanhamento dos indicadores. Os indicadores são gerenciados pela área de Compliance.

6.1.1.5. Recursos, funções, responsabilidades e autoridades

O SGPI conta com o apoio das áreas de negócios para gestão. Entretanto, ressalta-se que a manutenção e contribuição para melhoria contínua do SGPI são atribuições dos envolvidos. No conjunto de documentos do SGPI estão descritas as responsabilidades específicas, no Procedimento de Descrição de cargo e na Declaração de Aplicabilidade que contém a matriz RACI.

6.1.2. Executar

6.1.2.1. Competência, Treinamento, treinamento e conscientização

A **PSM Company** identifica as necessidades de competência, treinamento e conscientização, sendo que o SGPI identifica as necessidades aplicáveis frente aos requisitos legais e normativos, conforme Procedimento de Planejamento de Treinamentos Anuais.

Este esforço é complementado com ações de comunicação que visam contextualizar os elementos do SGPI na rotina dos empregados e contratados, bem como sensibilizá-los para a importância de promover a melhoria contínua de processos.

6.1.2.2. Comunicação

A organização prevê esforços de comunicação no ambiente interno e externo. As comunicações visam gerar atendimento e alinhamentos frente aos elementos do SGPI e/ou identificar expectativas diversas.

No ambiente interno, comunicações visam sensibilizar colaboradores e fornecedores para atendimento e contribuição frente aos elementos do SGPI, bem como identificar situações diversas que evidenciem oportunidades de melhoria ou desvios frente ao sistema. A comunicação interna pode ser realizada via e-mail, reuniões e/ou *WhatsApp*.

No ambiente externo, a **PSM Company** disponibiliza website corporativo, onde constam os canais para contato. A comunicação é realizada conforme o de Plano de Comunicação.

6.1.2.3. Documentação

Os documentos do sistema de gestão contam com Políticas, Normas Procedimentos que descrevem as estratégias e processos de cada atividade.

A elaboração, distribuição e controle dos documentos e registros associados ao SGPI é tratada no Procedimento de Padronização da Informação Documentada. Documentos de origem externa e requisitos aplicáveis ao SGPI são também tratados neste mesmo procedimento.

6.1.2.4. Controle Operacional

Em função da identificação de riscos de segurança da informação e privacidade, são estabelecidos e implementados, junto àqueles considerados significativos ou críticos, controles operacionais.

Os controles visam garantir o atendimento às premissas da Política de Privacidade de Dados e a Política de Segurança da informação e Privacidade, Procedimento de Requisitos Legais e Outros Requisitos, aplicáveis. Ainda, contribuem para a organização dos elementos pertinentes às normas, para evidenciação dos mesmos e suporte à melhoria contínua do SGPI. O acompanhamento é conforme Procedimento de Gestão Operacional e Gestão de Riscos, Análise de Risco e planilha de Gestão de Operação de Dados Pessoais. O Procedimento de Gestão de Não Conformidades e Ações de Melhoria prevê ainda o tratamento para ocorrências que possam evidenciar desvios nos processos relacionados à gestão de segurança da informação e privacidade.

6.1.2.5. Avaliação de riscos de segurança da informação e privacidade

Para avaliação de riscos de segurança da informação e privacidade, a organização mantém a sistemática descrita no Procedimento de Gestão Operacional e Gestão de Riscos, cujo objetivo é proteger as partes interessadas na eventualidade de uma ocorrência ou crise.

6.1.2.6. Gestão de Projetos e Mudanças

A área de Compliance acompanha e controla as iniciativas de projetos e mudanças no ambiente organizacional. As alterações que envolvam sistemas, tecnologias, processos ou infraestrutura devem ser formalizadas por meio de solicitação, avaliadas quanto à criticidade, riscos e impactos, e acompanhadas até sua conclusão, conforme procedimento estabelecido.

- Procedimento de Registro de iniciativas de projetos e mudanças

6.1.3. Checar

6.1.3.1. Monitoramento e medição

A **PSM Company** define através dos documentos Análise do Contexto Organizacional, Procedimento de Auditoria do Sistema de Gestão e de Processos, Procedimento de Gestão Operacional e Gestão de Riscos e Procedimento de Análise Crítica pela Direção a sistemática para monitorar e medir os principais elementos do SGPI, incluindo objetivos e operações que sejam críticas ou significativas.

6.1.3.2. Não Conformidade, ação corretiva e ação de melhoria

A **PSM Company** mantém o procedimento de Gestão de Não Conformidades e Ações de Melhoria para registro, investigação e análise para tratamento de não conformidades. Estes mesmos esforços podem tanto identificar a necessidade de ações corretivas, como oportunidades de ações de melhoria contínua.

6.1.3.3. Auditorias internas

Estão previstas auditorias internas focando a verificação de eficácia do SGPI e cumprimento dos requisitos e procedimentos relacionados a este Manual, conforme o Procedimento de Auditoria do Sistema de Gestão e de Processos.

6.1.4. Agir

6.1.4.1. Análise Crítica

A Direção analisa o SGPI conforme o Procedimento de Análise Crítica pela Direção, para assegurar sua contínua adequação, suficiência e

eficácia. Essa análise deve incluir a avaliação de oportunidades para melhoria e necessidade de mudanças no SGPI, em seus elementos.

6.1.5. CONTROLES – ANEXOS

As evidências de atendimento relacionadas a cada controle dos Anexos da ISO 27001 e ISO 27701 podem ser verificadas na Declaração de Aplicabilidade.

- ISO 27001:2022 – Controles e objetivos de controle - Anexo A: Controles de Segurança da Informação e Privacidade;
- ISO 27701:2019 – Controles e objetivos de controle - Anexo A: Controladores de DP e Controles e objetivos de controle - Anexo B: Operadores de DP.

<FIM DO DOCUMENTO>