MANUAL DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

ABNT NBR ISO 27001:2022

1. OBJETIVO

Apresentar o Sistema de Gestão de Segurança da Informação (SGSI), descrevendo seu escopo e os elementos que o compõe.

1.2 SOBRE O MANUAL

O Manual do SGSI descreve a estrutura de requisitos para que o sistema de gestão possa ser operacionalizado e mantido junto à estratégia de gestão organizacional, em alinhamento aos requisitos legais e corporativos, como referência para todo empregado, contratado ou outras partes interessadas. Visa subsidiar a gestão do SGSI embasada pelas melhores práticas, focada também nos princípios da melhoria contínua.

Para isto, este Manual:

- Apresenta o funcionamento do SGSI e a sistemática de gerenciamento dos riscos e oportunidades associados ao escopo, por meio da sua estrutura e documentação, visando criar também o ambiente para promoção da melhoria contínua.
- Descreve os elementos de gestão do SGSI e documentos associados.
- Demonstra como o SGSI incorpora requisitos associados à identificação e gerenciamento de impactos reais, bem como prevenção dos potenciais, associados às operações do empreendimento.

1.3 PREMISSAS DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

O SGSI é estabelecido com o intuito de promover, no ambiente corporativo, estímulos à melhoria continua de processos e do desempenho organizacional, sempre em conjunto com a melhor e mais profícua relação entre a empresa e suas partes interessadas.
Seu desenho integra a estratégia corporativa, reflexo da visão da direção, de estabelecer um ambiente de expectativas compartilhadas, que fomente o desenvolvimento sustentável. No modelo sobre o qual se desenha o SGSI, a excelência operacional, refletida no atendimento às expectativas dos clientes, do mercado e de instituições reguladoras, está acompanhada da boa reputação corporativa, da transparência e ética nos relacionamentos que conduzem e mantém a organização no patamar de uma empresa de referência em sua área de conhecimento técnico.

2. PERFIL DA ORGANIZAÇÃO

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;
- Aplicações.

2.1 MISSÃO, VISÃO E VALORES

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

2.3 POLÍTICA DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

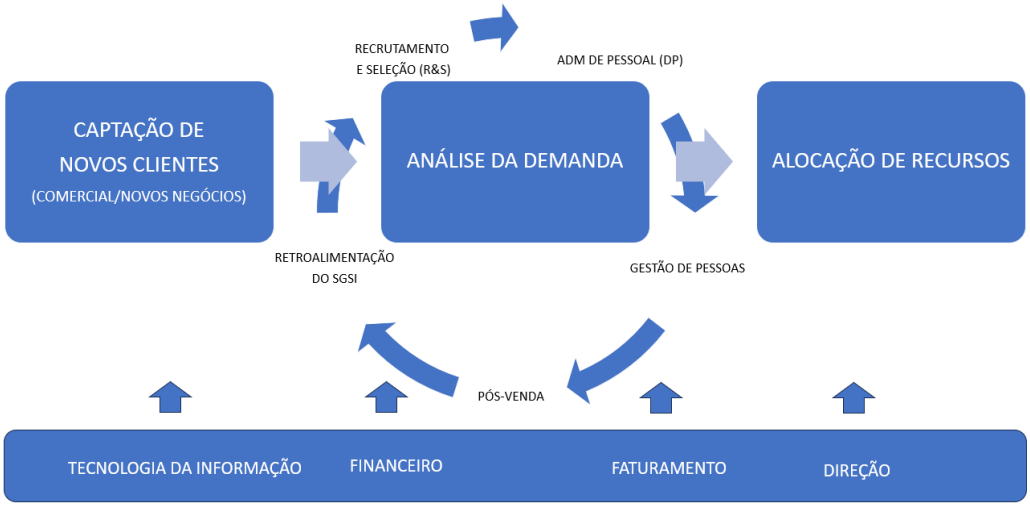
A Política de Segurança da Informação (POL001-SI - Politica Seguranca da informação) é a expressão do compromisso corporativo, validado pela direção, frente às expectativas das partes interessadas no que tange à segurança da informação e atendimento aos requisitos legais e outros requisitos.
"Realizar a gestão de serviços de Tecnologia da Informação com o comprometimento de atender os requisitos aplicáveis, proteger devidamente dados e informações pertinentes e promover a melhoria contínua."

2.4 ESCOPO DO SGSI
"Sistema de Gestão da Segurança da Informação na prestação de *serviços em Tecnologia da Informação com terceirização de profissionais especializados, com o suporte das atividades de Gestão de Pessoas, Recrutamento e Seleção, Administração de Pessoal, financeira, faturamento, Novos Negócios e Pós-Venda, conforme* Declaração de Aplicabilidade R01 de 18/01/2024"

Site incluído no escopo:
- PSM Company – Professional Services Management Informática Ltda.
Rua Luiz Seráphico Junior, 511 – Cj. 181 – Jardim Caravelas – São Paulo/SP.

Declaração de Aplicabilidade: DOC-Anexo A - Declaração de Aplicabilidade_R01

2.5 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, Financeiro, Faturamento e Direção.



2.6 ANÁLISE DE RISCOS E OPORTUNIDADES
A organização 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, as partes interessadas e a eficácia do SGSI, com efeitos sob os ativos físicos, financeiros, operacionais, imagem e a reputação da empresa.

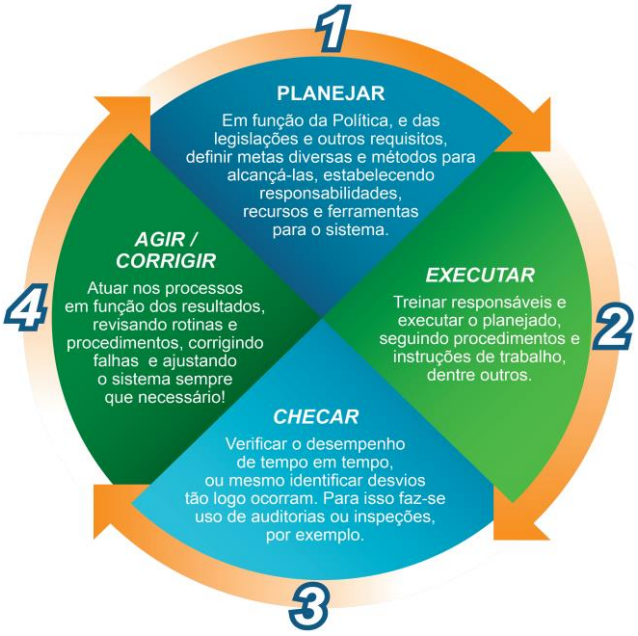
A identificação de riscos e oportunidades pode advir da análise crítica sistêmica, da análise de atendimento aos requisitos legais e outros requisitos, manifestações de partes interessadas, avaliação de riscos, dentre outros.

A análise de riscos e oportunidades é realizada por meio da Matriz SWOT, que está disponível no Sharepoint.

Os riscos e oportunidades são anualmente avaliados pela direção durante a reunião de análise crítica do sistema de gestão, ou conforme necessidade.

2.7 ELEMENTOS DO SGSI

O SGSI é um conjunto de processos definidos, que permitem à empresa gerenciar de forma sistemática suas oportunidades, seus riscos e impactos relacionados à segurança da informação. Para tal, é estabelecido um processo sistêmico, refletido em documentos, rotinas de trabalho e registros que visam auxiliar a organização para o melhor desempenho do SGSI. Este se baseia no conceito da melhoria contínua e utiliza o ciclo de PDCA, do inglês *PLAN – DO – CHECK – ACT* (traduzido para PLANEJAR – EXECUTAR – CHECAR – AGIR), para estruturar suas fases e processos. De maneira resumida, entende-se o ciclo PDCA do SGSI da seguinte maneira:



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 SGSI. Estabelece, assim, as bases para a melhoria contínua. Cada uma das etapas do ciclo de gestão do SGSI é descrita nos respectivos procedimentos. A seguir, os elementos integrantes do SGSI.

3. DESCRIÇÃO DOS ELEMENTOS

3.1 CICLO PDCA – PLANEJAR

A ORGANIZAÇÃO

3.1.1 CONTEXTO DA ORGANIZAÇÃO – RISCOS E OPORTUNIDADES

A organização analisa seu contexto e identifica riscos e oportunidades de negócio por meio da Matriz SWOT, do inglês *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças), disponível no Sharepoint.

3.1.2 REQUISITOS LEGAIS E OUTROS REQUISITOS

A gestão dos requisitos legais promove a aderência do SGSI 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 SGSI.
Os monitoramentos associados ao atendimento a requisitos legais são realizados e registrados no REG-SGSI-003 - Requisitos Legais e Outros Requisitos, disponível no Sharepoint. Sua atualização é realizada periodicamente, com verificação anual. O monitoramento do atendimento aos requisitos é realizado conforme PROC-SGSI-003 - Requisitos Legais e Outros Requisitos.

3.1.3 PARTES INTERESSADAS

As partes interessadas estão definidas na Análise do Contexto Organizacional, disponível no Sharepoint.

3.1.4 OBJETIVOS, METAS E INDICADORES

Os Objetivos, Metas e Indicadores, baseados na Política do SGSI, 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 PROC-SGSI-002 - Objetivos, Metas e Indicadores.
Os Objetivos, Metas e Indicadores do SGSI, com conteúdo aprovado junto à direção, resumem o conjunto de informações necessárias à gestão e acompanhamento dos indicadores. Os indicadores são gerenciados e registrados pela área de TI.

3.1.5 RECURSOS, FUNÇÕES, RESPONSABILIDADES E AUTORIDADES

O SGSI conta com o apoio das áreas de Gestão de Pessoas e TI para gestão. Entretanto, ressalta-se que a manutenção e contribuição para melhoria contínua do SGSI são atribuições de todos os envolvidos. No conjunto de documentos do SGSI estão descritas as responsabilidades específicas, conforme definido na Matriz RACI.

3.2 CICLO PDCA – EXECUTAR

3.2.1 COMPETÊNCIA, TREINAMENTO E CONSCIENTIZAÇÃO

A organização identifica as necessidades de competência, treinamento e conscientização, sendo que o SGSI identifica as necessidades aplicáveis frente aos requisitos legais e normativos, conforme PROC-SGSI-010 - Gestão de Treinamentos, Competências e Conscientização.

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

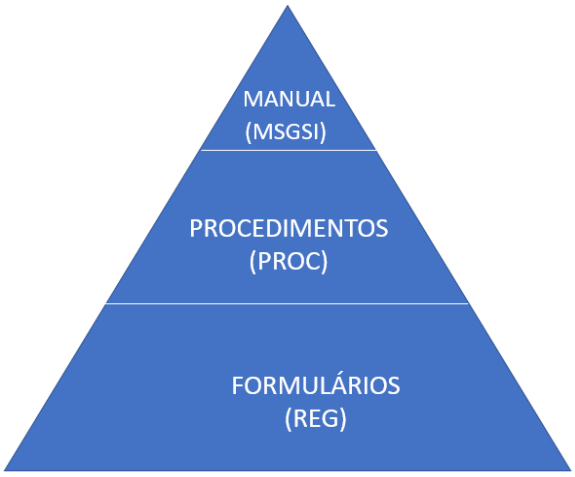
3.2.2 COMUNICAÇÃO

A organização prevê esforços de comunicação no ambiente interno e externo. As comunicações visam gerar atendimento e alinhamentos frente aos elementos do SGSI e/ou identificar expectativas diversas.
No ambiente interno, comunicações visam sensibilizar funcionários e fornecedores para atendimento e contribuição frente aos elementos do SGSI, bem como identificar situações

diversas que evidenciem oportunidades de melhoria ou desvios frente ao sistema. A comunicação interna é realizada via e-mail, reuniões, Sharepoint e WhatsApp.
No ambiente externo, a organização disponibiliza website corporativo, onde constam os canais para contato. A sistemática estabelecida para comunicação está descrita no PROC-SGSI-006 - Gestão da Comunicação Interna e Externa.

3.3.3 DOCUMENTAÇÃO

Os documentos que estruturam o SGSI, incluindo este Manual, seguem a esquematização abaixo:



Além dos documentos específicos para o sistema de gestão, a PSM conta também com Políticas, Normas e Procedimentos que descrevem as estratégias e processos de cada atividade.

Este Manual descreve todos os elementos do SGSI e, sempre que aplicável, direciona à documentação correlata. Toda elaboração, aprovação, distribuição e controle dos documentos e registros associados ao SGSI é tratada no PROC-SGSI-001 - Controle de Informação Documentada. Documentos de origem externa e outros requisitos aplicáveis ao SGSI são também tratados neste mesmo procedimento.

3.3.4 CONTROLE OPERACIONAL

Em função da identificação de riscos de segurança da informação, são estabelecidos e implementados, junto àqueles considerados significativos ou críticos, controles operacionais.
Todos os controles visam garantir o atendimento às premissas da Política de Segurança da Informação, 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 SGSI. O acompanhamento é conforme PROC-SGSI-007 - Controle Operacional e Gestão de Riscos. O PROC-SGSI-005 - 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.

3.3.5 AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Para avaliação de riscos de segurança da informação, a organização mantém planos cujo objetivo é proteger os funcionários, contratados, fornecedores e clientes, na eventualidade de uma ocorrência ou crise. Segue:

- **Declaração de Aplicabilidade –** São avaliados controles pertinentes para a mitigação de riscos relacionados à segurança da informação e as medidas tomadas em cada situação.
- **Análise de Riscos –** Análise e avaliação de riscos pertinentes para o sistema de gestão de segurança da informação.

Além da Declaração de Aplicabilidade, o SGSI conta também com o PROC-SGSI-007 - Controle Operacional e Gestão de Riscos.

3.4 CICLO PDCA – CHECAR

3.4.1 MONITORAMENTO E MEDIÇÃO

A organização define através dos procedimentos PROC-SGSI-002 - Objetivos, Metas e Indicadores, PROC-SGSI-004 - Auditorias Internas, PROC-SGSI-007 - Controle Operacional e Gestão de Riscos e PROC-SGSI-008 - Análise Crítica pela Direção a sistemática para monitorar e medir os principais elementos do SGSI, incluindo objetivos e operações que sejam críticas ou significativas. São exemplos de monitoramento:

- controle de documentos legais;
- auditorias internas;
- acompanhamento do desempenho dos indicadores do SGSI.

3.4.2 NÃO CONFORMIDADE, AÇÃO CORRETIVA E AÇÃO DE MELHORIA

A organização mantém o procedimento PROC-SGSI-005 - Gestão de Não Conformidades e Ações de Melhoria para registro, investigação e análise para tratamento de não conformidades reais e potenciais. Estes mesmos esforços podem tanto identificar a necessidade de ações corretivas, como oportunidades de ações de melhoria contínua.

3.4.3 AUDITORIAS INTERNAS

Estão previstas auditorias internas focando a verificação de eficácia do SGSI e cumprimento dos requisitos e procedimentos relacionados a este Manual, conforme PROC-SGSI-004 - Auditorias Internas.

Os resultados são documentados e constituem pauta para Reuniões de Análise Crítica. Independentemente deste processo, as eventuais NCs (não conformidades) ou OMs (oportunidades de melhoria) devem ser tratadas tão logo sejam identificadas, conforme PROC-SGSI-005 - Gestão de Não Conformidades e Ações de Melhoria.

3.5 CICLO PDCA – AGIR

3.5.1 ANÁLISE CRÍTICA

A Direção deve analisar o SGSI conforme PROC-SGSI-008 - 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 SGSI, em todos os seus elementos.

4. CONTROLES ANEXO A

4.7. Políticas de segurança da informação (Controle A.5)

As Políticas para atendimento aos controles são referenciadas no decorrer dos itens desse manual de gestão.

4.8. Papéis e responsabilidades pela segurança da informação (Controles A.5.2, 5.3, 5.4, 5.5, 5.6)

Para garantir que os processos estão sendo executados e controlados de maneira adequada e por pessoas devidamente cientes e capacitadas, A PSM Company definiu todas as responsabilidades e autoridades referentes ao sistema de gestão de segurança da informação no documento SGSI_Organograma x Matriz RACI e Descrição de Cargos SGSI e realiza o controle de atualização sempre que necessário.

Em todas as atividades, o conflito de interesse é evitado através da utilização de sistemas em diversas etapas dos processos. Além disso, existem as políticas que reforçam ainda mais os controles.

- Politica Anticorrupcao, Suborno ou Fraude
- PCN001 - TI PCN TI

Contatos apropriados com autoridades relevantes para o negócio da PSM Company são mantidos pelos responsáveis e registrados através de Grupos de WhatsApp, registro de Atas, invites de reuniões.

4.9. Inteligência de Ameaças (Controles A.5.7)

A PSM Company identifica as ameaças relacionadas a segurança da informação e analisa de forma a controlar conforme sistemáticas:

- PROC018-TI Gestão de incidentes
- PROC015-TI Gestão de Vulnerabilidades

4.10. Segurança da informação no gerenciamento de projetos (Controle A.5.8)

A gestão de projetos realizada pela PSM Company considera a questão de segurança da informação medindo os níveis de confidencialidade das informações que serão contidas em cada projeto. Todas a sistemática está documentada através do document PROC-001-GPro-Gerenciamento de Projetos.

4.11. Gestão de Ativos (Controles A.5.9, 5.10, 5.11)

Os ativos são mapeados e controlados através no do inventário de ativos.

Os detalhes e informações de cada ativo são descritos para facilitar o processo de avaliação de riscos.

O inventário dos ativos é analisado criticamente para verificar a sua adequação e pertinência.

- CONT005-TI - Inventário
- PROC011-TI Inventario PSM
- PROC009-TI Procedimento de Solicitação e devolução de equipamentos
- PROC010-TI Procedimento Checklist
- PROC014-TI Controle Acesso Lógico
- TER001-TI Termo de Responsabilidade
- TER002-TI Termo Devolução
- PROC006-TI PSM-Procedimento de Descarte Seguro

4.12. Gestão de Documentos: Classificação, Rotulagem e Transferência das Informações (Controles A.5.12, 5.13, 5.14, 5.35, 5.37)

Todos os documentos necessários para a aperação do SGSI estão estabelecidos e novos documentos são criados de acordo com a necessidade.

O proprietário da informação é responsável por classificá-la adequadamente aplicando nível de proteção proporcional a sua importância e por rotulá-la com o nível de segurança adequado.
As informações só podem ser divulgadas externamente quando autorizadas pelo proprietário, salvo quando envolver ordens judiciais.
As informações, em especial dados pessoais (incluindo as sensíveis), devem ser utilizadas unicamente para a finalidade para a qual foram coletadas, conforme diretrizes da LGPD.
As informações da PSM Company, ou de sua responsabilidade, são classificadas de acordo com seu valor para o negócio e sensibilidade utilizando os níveis de segurança
O proprietário da informação é responsável por assegurar que as informações estejam controladas de forma a garantir que apenas as pessoas autorizadas possam acessá-las.

- NOR005-SI Classificacao da Informacao PSM
- PROC019-TI Gestão de diponibilidade de dados
- REG-SGSI-001
- PROC-SGSI-0001 - CONTROLE DE DOCUMENTOS
- LISTA MESTRA DE DOCUMENTOS_R00
- PROC- SGSI -001 - CONTROLE DA INFORMAÇÃO
- PROC013-TI Transferência de Arquivos
- PROC014-TI Controle Acesso Lógico

4.13. Controle de Acesso (Controles A.5.15, 5.16, 5.17, 5.18, 5.19)

Para garantir um nível de proteção adequado aos sistemas e informações da PSM Company, assim como para atendimento a regulamentações, foi definido que todos os acessos dos usuários devem ser devidamente registrados, aprovados pelos responsáveis e revisados periodicamente conforme estabelecido nos documentos abaixo.

- PROC014-TI Controle Acesso Lógico
- PROC-011-DIR-Acesso Fisico a PSM
- CONT001-TI ACESSOS SHAREPOINT
- NOR002-SI Senhas PSM
- MAN001-TI Uso dos Recursos de TI PSM
- PROC002-ADMFIN-CONTRATOS
- PROC003-ADMFIN-COMPRAS
- POL001-SI Politica Seguranca da informacao
- Sistema PSM Contratos
- Planilha de Analise de Riscos de fornecedores – SGSI

4.14. Gestão de Fornecedores (Controles A.5.20, 5.21, 5.22)

A PSM Company realiza o controle dos fornecedores que possuem relação com os ativos e recursos de segurança da informação da empresa, para que estes estejam conscientes sobre o tipo de acesso que possuem em cada ambiente, bem como a utilização de forma apropriada de cada recurso, determinando regras e normas para as melhores práticas de compliance, além de realizar monitoramentode cada um deles através das diretrizes descritas nos documentos abaixo

- NOR003-ADMFIN PSM
- PROC002-ADMFIN-CONTRATO
- PROC003-ADMFIN-COMPRAS
- Sistema PSM Contratos
- Planilha de Analise de Riscos de fornecedores - SGSI
- PCN001-TI PCN TI
- PROC018-TI Gestão de incidentes

- PROC019-TI Gestão de Disponibilidade de Dados
- PROC018-TI Gestão de incidentes

4.15. Segurança da informação para uso de serviços em nuvem (Controles A.5.23)

A PSM realiza a gestão dos serviços em nuvem desde a aquisição, uso, gestão e saída de serviços de forma consistente através dos procedimentos de gestão NOR006-TI Serviços de Cloud e PROC019-TI Gestão de Disponibilidade de Dados

4.16. Gestão de Incidentes (Controles A.5.24, 5.25, 5.26, 5.27. 5.28, 6.8)

Promover um ambiente onde todos se comprometem com segurança da informação na empresa é extremamente importante e exige um processo contínuo de conscientização. É responsabilidade de todos informar possíveis violações das Diretrizes de Segurança da Informação seguindo o descrito nas sistemáticas PROC018-TI Gestão de incidentes, NOR001-GP CCD - Canal Direto de Denuncias, ou até mesmo utilizando os canais controlador.lgpd@psmcompany.com.br, ouvidoria.interna@psmcompany.com.br, PSM Conecta

Qualquer colaborador ou terceiro pode emitir um relato relacionado à Segurança da Informação ou Proteção de Dados através utilizando como referência o descrito no documento PROC018-TI Gestão de incidentes. O relato será analisado e, de acordo com cada caso, levará o assunto ao responsável pela àrea de Tecnologia da Informação para a tomada de providências necessárias.
Todo incidente será investigado e as ações corretivas devidamente implementadas. Além disso é realizado todo o acompanhamento e coletada todas as evidências necessárias. Todo o processo é registrado e acompanhado através do formulário FOR003-TI - Incidente

4.17. Segurança da informação durante a disrupção (Controles A. 5.29, 5.30)

A PSM Company possui PCN001-TI PCN TI relativo à segurança de informações para a manutenção ou recuperação das operações e para garantir a disponibilidade das informações no tempo necessário após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

- PROC019-TI Gestão de disponibilidade de dados
- NOR 002-SESMT-PAE-Procedimento de Emergencia
- PROC018-TI Gestão de incidentes
- PCN001-TI PCN TI
- NOR 002-SESMT-PAE-Procedimento de Emergencia

4.18. Requisitos legais e Direitos de propriedade intelectual (Controles A.5.31, 5.32)

Todos os requisitos legais aplicáveis ao negócio da PSM Company estão identificados na planilha de controle de requisites e podem sedr evidenciados em contratos.

- PROC-SGSI-003 Requisitos Legais e Outros Requisitos
- REG-SGSI-003 - REQUISITOS LEGAIS E OUTROS REQUISITOS
- Requisitos legais, estatutários, regulamentares e contratuais

Procedimentos para proteção da propriedade intelectual e privacidade são aplicados de forma constante para assegurar de forma eficaz o atendimento das legislações pertinentes.

- PROC001 ADMPESSOAL - ADMISSÃO E INTEGRAÇÃO
- MAN001-TI USO DOS RECURSOS DE TI PSM

4.19. Proteção de registros e Backup (Controle A.5.33, 8.13)

A PSM Company armazena todos os seus registros em rede ou banco de dados, e protege através de controle de acesso e backup conforme sistemáticas.

- PROC005-TI Backup Restore Sharepoint Exchange
- PROC002-TI Backup Restore Banco de Dados
- PROC014-TI Controle Acesso Lógico

4.20. Privacidade e proteção dados de DP (Controle A.5.34)

Para garantir a confidencialidade das informações, todos os colaboradores/partes externas assinam o termo de privacidade de proteção de dados.

- PROC001 ADMPESSOAL - ADMISSÃO E INTEGRAÇÃO, TER025-SI CONFICENCIALIDADE E SEGURANÇA DA INFORAMAÇÃO

4.21. Conformidade com políticas, regras e normas para segurança da informação (Controle A.5.36)

As auditorias de sistema são realizadas conforme PROC-SGSI-004 - Auditorias Internas
As não conformidades identificadas são registradas e tratadas no PROC-SGSI-005 - Gestão de Não Conformidades e Ações de Melhoria
Além das auditorias, é realizado a verificação e o monitoramento de forma constante através da PROC-SGSI-008 - Análise Crítica pela Direção

4.22. Seleção, Termos e condições de contratação e Processo disciplinar (Controles A.6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 7.8, 8.1, 8.2.3)

Está estruturado um processo para contratação de colaboradores, conforme diretrizes definidas nos documentos POL001-RS ver.00 - Politíca de R&S e PROC001 - Procedimento R&S
Profissionais designados (exemplos: representantes da qualidade, TI e comitê de segurança da informação) recebem capacitação em Sistema de Gestão da Segurança da Informação e atualização regular nas políticas de segurança da informação.

O programa de conscientização em segurança da informação, proteção de dados, utilização de dispositivos endpoint e trabalho remoto são realizados forma sistêmica através dos Onboarding de novos colaboradores e reciclagens (MAN001-TI Uso dos Recursos de TI PSM, TER001-TI Termo de Responsabilidade, MAN001-TI Uso dos Recursos de TI PSM)

Acordos de confidencialidade que incluem a não divulgação de dados mesmo após o encerramento de contrato ou mudança de contratação são assinados e documentados no TER025 -SI - CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO;
Convém que as responsabilidades e funções de segurança da informação que permaneçam válidos após o encerramento ou mudança da contratação sejam definidos, aplicados e comunicados ao pessoal e outras partes interessadas pertinentes.

Casos de violações de segurança da informação por parte dos colaboradores serão investigados e estarão sujeitos à processos disciplinares.

4.23. Perímetros segurança física (Controles A.7.1,7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9,)

A PSM Company definiu os controles de prevenção acesso físico não autorizado a todos os seus ambientes de forma a evitar danos e interferências nos seus processos conforme definido do documento PROC-011-DIR-Acesso Fisico a PSM.

O acesso ao escritório ou outro local da empresa que contenha informação sensível é restrito fisicamente (MAN001-TI Uso dos Recursos de TI PSM, TER001-TI Termo de Responsabilidade, POL003-TI rede internet email)

Os documentos que contém informações sensíveis são mantidos em local seguro e de acesso monitorado conforme PROC012-TI Cameras

Para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente os usuários adotam a política de "mesa limpa / tela limpa" NOR008 SI Política Mesa Limpa e Tela Limpa de tal forma que, pessoas sem autorização não tenham acesso a informação sensível que seja eventualmente exibida na tela e/ou estação de trabalho

São realizados simulados de possíveis ocorrências possíveis e e considerado ações para mitigar os efeitos e riscos quanto a ameaças a segurança da informação e outros aspectos.

- NOR001-SESMT
- PAE
- PCN001-TI PCN TI

4.24. Serviços de Infraestrutura e Segurança de cabeamento (Controles A.7.11,7.12)

Na PSM Company, a infraestrutura crítica, hospedada na AWS para servidores Cloud e na Microsoft 365 (Azure) para arquivos de rede, é protegida contra perdas, danos, roubo ou comprometimento.
Para evitar falhas de energia e outras disrupções, implementamos medidas de redundância em ambientes cloud.
Todo o cabeamento é mapeado e o acesso ao cabeamento, fica em piso elevado, facilitando a manutenção, em caso de algum problema.

- NOR006-TI Serviços de Cloud
- NOR002-SESMT-PAE - Procedimento Atendimento de Emergencia
- PCN001 - TI - PCN TI
- CONT004-TI
- MAPA_DA_REDEPSM

4.25. Mídia de armazenamento e Manutenção de equipamentos (Controles A.7.10, 7.13, 7.14)

As mídias de armazenamento são bloqueadas para acesso nos equipamentos da PSM.
Em caso de descarte e envio para manutenção, a mídia de armazenamento principal (HDs, SSDs) é removida, evitando o acesso de arquivos em mãos de terceiros.

- CHK001-TI Checklist TI
- NOR007-SI Politica de Utilização Dispositivos Moveis
- PROC006-TI PSM-Procedimento de Descarte Seguro
- PROC010-TI Procedimento Checklist

Para casos de maior gravidade, criticidade A PSM possui um procedimento PROC001-manutencao de equipamentos, que orienta esse tipo de assistência e manutenção

4.26. Serviços de Rede (Controles A.7.10, 7.14)

A PSM Company utiliza o Sharepoint como ferramenta para armazenar seus arquivos e realiza o controle de acessos através de uma planilha e gestão de contratos.
CONT001-TI ACESSOS SHAREPOINT

PROC014-TI Controle Acesso Lógico

4.27. Criptografia (Controles A.8.24, 8.4)

Para manter e proteger a integridade, identidade e confidencialidade das informações utilizadas pelo PSM Company é utilizado a ferramenta Bitlocker para criptografia de discos e nos dispositivos móveis é utilizado o nativo do Android.
Para armazenamento de códigos fonte é utilizado o repósitorio GitHub.com. Todos são criptografados e privados, protegendo contra o acesso indevido.

- PROC003-TI Criptografia de discos - Bitlocker
- NOR009 - TI CRIPTOGRAFIA EM DISPOSITIVOS MOVEIS
- NOR002-TI Repositório de código fonte

4.28. Desenvolvimento Seguro (Controles A.8.25,8.29, 8.33)

A PSM Company estabeleceu procedimentos que tem como objetivo especificar os princípios e boas práticas para identificar os requisitos relacionados à segurança da informação e eficiência do produto para novos projetos de desenvolvimento e/ou melhorias dos já existentes.

- POL001-TI PSM-DesenvolvimentoSeguro
- PROC007-TI Solicitacao de Desenvolvimento de Sistemas
- PROC016-TI Testes de Sistemas
- PROC001-GPRO-Gerenciamento de projetos
- NOR003-TI Tecnologias De Desenvolvimento De Software

4.29. Gestão de Acessos (Controles A.8.2, 8.3, 8.5, 8.9)

A PSM Company A PSM gerencia os acessos e autenticação a rede e os Owners de sistemas através de controle em planilhas e auditorias nos equipamentos

- CONT003-TI Owner vs Sistemas
- CONT001-TI ACESSOS SHAREPOINT
- PROC014-TI Controle Acesso Lógico
- CHK001-TI Checklist TI
- PROC010-TI Procedimento Checklist

4.30. Segurança de redes e redundância (Controles A.8.14, 8.20)

A rede corporative (Sharepoint) da PSM Company possui implementações de segurança que impedem que pessoas externas à organização acessem seus recursos.
Para acessar a rede é necessário login e senha pessoal.
A rede também é monitorada por sistema de TI que verifica os principais serviços e servidores de infraestrutura de rede, emitindo alertas caso algum deles apresente problemas de desempenho ou inatividade.

- CONT001-TI ACESSOS SHAREPOINT
- CONT005-TI - Inventário
- PROC005-TI Backup Restore Sharepoint Exchange
- PROC002-TI Backup e restore banco de dados
- PROC015-TI Gestão de Vulnerabilidades

Os arquivos são armazenados no Sharepoint (Azure) e os sistemas/banco de dados na AWS com redundancia.

- NOR005-TI- Serviços de Cloud
- PROC019-TI Gestão de disponibilidade de dados

4.31. Separação dos ambientes de desenvolvimento, teste e produção (Controle A.8.31)

A PSM realiza a separação de ambientes conforme sistemáticas POL001-TI DesenvolvimentoSeguro e NOR004-TI-Ambiente de desenvolvimento a fim de garantir a integridade das informações. São 3 ambiente distintos:

- Ambiente de Desenvolvimento (equipamento do desenvolvedor),
- Ambiente de Homologação: AWS
- Ambiente de Produção: AWS

4.32. Gestão de Mudanças (Controle A.8.32)

O Departamento de Tecnologia da Informação controla as alterações no ambiente computacional. Como alteração se entende mudança em hardware, sistema operacional, substituição ou atualização de sistemas aplicativos. Tais mudanças são executadas e controladas através de uma solicitação de mudança GMUD.

- PROC017-TI Gestão de mudanças
- FOR002-TI GMUD

4.33. Gestão de Vulnerabilidade (Controle A.8.8, 8.16)

As questões de vulnerabilidade técnica da PSM Company são fortemente identificadas e controladas através de ferramentas que auxiliam na detecção conforme descrito no document PROC015-TI Gestão de Vulnerabilidades.

4.34. Gestão da Capacidade (Controle A.8.6)

O Departamento de Tecnologia da Informação monitora a capacidade de processamento dos equipamentos e sistemas através do levantamento da capacidade fluxo de dados, processamento, armazenamento em nuvem.

Também realiza, sempre que requerido o report dessas informações para análise da Direção.

O objetivo desse monitoramento é evitar que o sistema seja sobrecarregado e cause prejuízos e/ou perda de lucratividade.

- PROC020-TI Gestão de capacidade

4.35. Sincronização do Relógio (Controle A.8.17)

Nos softwares desenvolvidos na PSM é utilizado o padrão UTC-3 (America/São_SaoPaulo) e para os equipamentos Windows está configurado a hora atualizada da internet.

4.36. Log (Controle A.8.15)

Os usuários com acesso privilegiado não conseguem excluir as evidências do seu próprio log, somente consulta.

O monitoramento dos logs é realizado através das ferramentas AWS CloudWatch e MicrosoftEntra, que mantém o registro de logs, o que permite a rastreabilidade de qualquer log de usuário privilegiado.

4.37. Exclusão de informações, Mascaramento e Prevenção de vazamento de dados (Controle A.8.10, 8.11 e 8.12)

A PSM Company Analisa informações, e quando identifica que essa não é mais necessária realiza a exclusão dos dados armazenados de forma Segura conforome sistemáticas PROC006-TI PSM-

Procedimento de Descarte Seguro, CHK003-DP - Check List Demissional, PROC009-TI Procedimento de Solicitação e devolução de equipamentos

Para utilização de dados pessoais de colaboradores na operação dos negócios, solicita autorização. Esses são coletados e armazenados para a finalidade proposta e são tratados nos sistemas de acordo com as necessidades de finalidades de cada departamento, tendo em vista as politicas de segurança de dados já realizada pelos fornecedores de serviços em nuvem, onde são armazenados os nossos bancos de dados e informações gerais da PSM Company. Senhas são mascaradas nos sistemas internos com a técnica MD5.

- PROC001 ADMPESSOAL - ADMISSÃO E INTEGRAÇÃO,
- PROC001-RS - PROCEDIMENTO
- POL001 - TI - Desenvolvimento seguro/(MD5).
- POL001-SI Politica Seguranca da informacao
- PROC015-TI Gestão de Vulnerabilidades

4.38. Proteção contra Malware (Controle A.8.7)

As estações de trabalho da PSM Company possuem solução de antivírus instalada e gerenciada através de uma plataforma que integra todos os logs de atividades suspeitas e de ameaças de softwares maliciosos, impedindo a ação demalwares.

- Microsoft Defender
- NOR027-SI Normas Antispam
- NOR004-SI Antivírus PSM
- AWS Guard

4.39. Instalação Padrão (A.8.18 / 8.19)

A instalação inicial dos sistemas é orientada através do uso do CHK001-TI Checklist TI
Um conjunto padrão de instalação de software é preparado e mantido em local seguro. Estas cópias padrão são usadas para a recuperação de infecções de vírus, falhas do disco rígido e outros problemas do equipamento.
O check list também contempla a configuração (formatação de máquina ou disponibilização de nova máquina) no perfil do usuário (configuração do outlook e onedrive)

O uso ou instalação de software ou hardware só é permitido quando devidamente homologado e licenciado.

Todos os usuários recebem na Integração a orientação sobre a proibição de instalação e uso de software e hardware não homologados.

- CHK001-TI Checklist TI
- PROC010-TI Procedimento Checklist

4.40. Auditorias de sistemas de informação (A.8.34)

As auditorias de sistema são realizadas e registradas conforme procedimento PROC010 - PROCEDIMENTO CHECKLIST
Além das auditorias é realizado a verificação e o monitoramento de forma constante através dos alertas de segurança sistêmicos.

5. ANEXOS

Análise do Contexto Organizacional;
Declaração de Aplicabilidade;
Análise de Riscos.

Revisão	Data da Emissão	Emitente	Aprovador	Descrição da revisão
0	29/12/2023	Vítor Marques	Flavio Borges	Emissão inicial
1	22/01/2024	Vítor Marques	Flavio Borges	Ajustes conforme auditoria interna 2024
2	26/01/2024	Vitor Marques	Flavio Borges	Alterado o termo de “Alta Administração” para “Direção”.
3	12/02/2024	Vitor Marques	Flavio Borges	Inclusão do item 4 – Controles do Anexo A e todos os subitens (Políticas por tema).