Sumário

1. Finalidade, escopo e usuários

Esta política tem a finalidade de definir as diretrizes, os princípios e as regras básicas de gestão da segurança da informação.

As diretrizes de segurança da informação são formadas por metas e medidas específicas sobre este tema, definidas pela alta direção e gestores da Vports responsáveis pela sua definição e implementação. Essas metas e medidas, que representam os objetivos a serem alcançados e as ações necessárias para atingi-los, podem estar alinhadas a requisitos regulatórios, contratuais e operacionais, além de promoverem uma cultura sólida de segurança da informação em toda a organização.

Esta política aplica-se a todo o Sistema de gestão de segurança da informação (SGSI).

Os usuários deste documento são funcionários da Vports, assim como as partes externas relacionadas.

2. Documentos de referência

- Norma ISO/IEC 27001:2022, cláusulas 5.1, 5.2, 5.3 e A.5.1, A.5.2
- Manual do sistema de gestão de segurança da informação (SGSI-MNL-001)
- Metodologia de avaliação e tratamento de riscos de segurança da informação (SGSI-DOC-002)
- Declaração de aplicabilidade (SGSI-DOC-027)
- Lista de obrigações Legais, Regulamentares e Contratuais (Sistema CAL)
- Plano de Comunicação (SGI-DOC-004)

3. Terminologia básica de segurança da informação

Alta Direção - refere-se ao grupo de executivos e líderes seniores responsáveis pela tomada de decisões estratégicas e pela definição dos rumos e objetivos da organização. Esse grupo inclui os cargos de CEO, CFO, COO e outros membros do C-level.

Canal de Denúncias - é um meio formal e confidencial disponibilizado por uma organização para que colaboradores, clientes, fornecedores e outras partes interessadas possam relatar de forma segura e anônima (se desejado) qualquer comportamento inadequado, prática ilegal, conduta antiética ou violação de políticas internas, leis e regulamentos.

Comitê Gestor de Segurança da Informação (CGSI)- um grupo de pessoas designadas para discutir, analisar, avaliar e tomar decisões ou realizar ações específicas em nome de uma organização ou entidade.

Compliance - a conformidade com leis, regulamentos, políticas internas, normas e padrões éticos aplicáveis a uma organização.

Comunicação - o processo de troca de informações, ideias, pensamentos e sentimentos entre indivíduos ou grupos, por meio de métodos verbais, escritos ou não verbais.

Confidencialidade – características das informações que estão disponíveis somente para pessoas autorizadas ou sistemas.

Controles - são medidas, práticas, procedimentos ou mecanismos implementados para gerenciar riscos e garantir a proteção dos ativos de uma organização, como informações, sistemas e processos.

Data Protection Officer (DPO) - ou Encarregado de Proteção de Dados, é o profissional responsável por assegurar que uma organização esteja em conformidade com as leis e regulamentos de proteção de dados pessoais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na Europa. O DPO atua como ponto de contato entre a organização, os titulares de dados e as autoridades reguladoras, garantindo a proteção dos direitos dos indivíduos e a transparência no tratamento de dados pessoais.

Diretrizes - são orientações estratégicas e normas estabelecidas por uma organização para direcionar comportamentos, práticas e processos. As diretrizes incluem metas/objetivos e medidas/ações necessárias e suficientes para que as metas e objetivos sejam alcançados.

Disponibilidade - características das informações que somente podem ser acessadas por pessoas autorizadas quando for necessário.

Eficácia - é a capacidade de alcançar os resultados ou objetivos esperados com sucesso, independentemente dos recursos utilizados.

Integridade - características das informações que somente são alteradas somente por pessoas de forma permitida.

Medição - o processo de quantificação de características, desempenho ou resultados de um objeto, atividade ou processo, utilizando critérios e métodos definidos.

Não conformidade - é o descumprimento de um requisito estabelecido por normas, regulamentos, políticas, procedimentos ou especificações previamente definidos.

Norma - um conjunto de regras, requisitos, especificações ou diretrizes formalmente estabelecidos e reconhecidos para garantir que materiais, produtos, processos e serviços estejam em conformidade com critérios de qualidade, segurança, eficiência e desempenho específicos.

Objetivos - são resultados ou condições específicas que uma organização ou indivíduo pretende alcançar em um determinado período.

Padrão - um modelo ou referência estabelecida como base para comparação, medição ou desempenho em relação a produtos, processos, serviços ou comportamentos.

Penalidades - são sanções ou consequências impostas a indivíduos, grupos ou organizações em resposta ao não cumprimento de regras, normas, políticas ou obrigações legais estabelecidas.

Requisitos - são condições, critérios ou especificações que devem ser atendidos para alcançar um determinado objetivo ou para que um produto, serviço ou processo esteja em conformidade com normas, regulamentações, contratos ou expectativas.

Responsabilidades - são as obrigações e deveres atribuídos a indivíduos ou grupos dentro de uma organização para realizar determinadas tarefas, tomar decisões e garantir o cumprimento de políticas, normas e objetivos estabelecidos.

Segurança da informação - preservação da confidencialidade, integridade e disponibilidade da informação.

Sistema de gestão da segurança da informação (SGSI) - um conjunto de políticas, procedimentos e tecnologias utilizadas para gerenciar e proteger as informações de uma organização.

Usuários - são indivíduos ou entidades que utilizam sistemas, serviços, produtos ou recursos para alcançar um determinado objetivo ou realizar atividades específicas.

4. Gerenciando a segurança da informação

4.1. Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação são:

- Atender as exigências da Alta Direção relacionadas às demandas de mercado para a área de segurança da informação;
- Conscientizar os colaboradores sobre a importância da segurança da informação;
- Garantir a eficácia dos controles de segurança da informação para assegurar a confidencialidade, integridade e disponibilidade dos ativos.

Para alcançar os objetivos definidos para o SGSI, é determinado o Planejamento Anual dos Objetivos do SGSI (SGSI-DOC-005), este é acompanhado periodicamente nas reuniões de análises críticas do SGSI e do Comitê Gestor de Segurança da Informação, onde são verificados os índices de atendimento conforme indicadores definidos.

4.2. Requisitos de segurança da informação

A Alta Direção e Comitê Gestor de Segurança da Informação - CGSI estão comprometidos com uma gestão efetiva da Segurança da Informação na Vports. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da Vports.

Esta Política e todo o SGSI devem estar em conformidade com os requisitos legais e regulamentares vigentes e aplicáveis à organização na área de segurança da informação, bem como com as obrigações contratuais.

4.3. Controles da segurança da informação

Os critérios para avaliação e tratamento de riscos de segurança da informação são definidos na Metodologia de Avaliação de Riscos e de Tratamento do Risco de Segurança da Informação (SGSI-DOC-002).

Os controles do Anexo A da ISO/IEC 27001:2022 selecionados para tratamento de riscos de segurança da informação e seu status de implementação serão listados na Declaração de Aplicabilidade (SGSI-DOC-027).

4.4. Responsabilidades

As responsabilidades básicas para o SGSI são:

A Alta Direção deve:

- Atribuir responsabilidade e autoridade para assegurar que o sistema de gestão da segurança da informação esteja em conformidade com os requisitos da Norma ISO/IEC 27001;
- Atribuir responsabilidade e autoridade para relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção;
- Assegurar que os recursos necessários para o sistema de gestão da segurança da informação estão disponíveis;
- Comunicar a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;

O Gerente Tecnologia da Informação deve:

- Garantir que o SGSI seja implementado de acordo com esta Política e possua todos os recursos necessários.
- Coordenar e reportar sobre o desempenho do SGSI;

- Elaborar em conjunto com a equipe de segurança da informação e RH o programa de Treinamento e Conscientização sobre segurança da informação para os funcionários e todas as pessoas que possam impactar o Sistema de Gestão de Segurança da Informação - SGSI.
- Criar e implementar políticas de segurança da informação alinhadas aos objetivos e necessidades da organização.
- Identificar, avaliar e mitigar riscos relacionados à segurança da informação, garantindo que medidas adequadas estejam em vigor para proteger os ativos da empresa.
- Orientar a organização para que esteja em conformidade com todas as leis, regulamentações e normas de segurança da informação aplicáveis.
- Desenvolver estratégia de segurança cibernética de longo prazo.
- Desenvolver métricas para monitoramento dos objetivos de segurança da informação.
- Reportar regularmente sobre o estado da segurança da informação à alta administração, fornecendo análises e recomendações para melhorias.
- Apoiar na Coordenação e resposta a incidentes de segurança, incluindo a investigação de violações, mitigação de impactos e recuperação de sistemas afetados.
- Apoiar na avaliação de segurança da informação dos fornecedores e parceiros, garantindo que estejam alinhados com os padrões de segurança da empresa.
- Desenvolver e manter plano de recuperação de desastres, assegurando que a empresa possa operar com o mínimo de interrupção em caso de incidentes.
- Manter-se atualizado com as últimas tendências e tecnologias em segurança da informação, promovendo a inovação e a melhoria contínua dos processos de segurança.

O Comitê Gestor de Segurança da Informação (CGSI) deve:

- Analisar o SGSI pelo menos uma vez por ano ou sempre que ocorrer uma mudança importante e elaborar registros sobre a reunião. A finalidade da revisão da gestão é definir a adequabilidade e a eficácia do SGSI;
- Sinalizar possíveis impactos dos controles na área operacional;
- Apoiar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da Vports;

A equipe de Segurança da Informação deve:

- Propor metodologias, processos e iniciativas que visem à segurança da informação;
- Promover a conscientização dos funcionários em relação à relevância da segurança da informação para a Vports, através de ações conjuntas com o RH;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;
- 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, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- Habilitar trilha de auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes em transações críticas. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

A equipe de Infraestrutura deve:

- Configurar os equipamentos, ferramentas e sistemas concedidos aos funcionários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta política e pelas normas de segurança da informação complementares.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Vports.

O *Data Protection Officer* (DPO) deve:

- Garantir que a gestão de privacidade seja realizada em conformidade com esta Política e possua todos os recursos necessários.
- Gerenciar e reportar sobre o desempenho de privacidade;
- Reportar sobre quaisquer preocupações relacionadas à segurança da informação e cibernética;
- Criar e implementar políticas de privacidade e proteção de dados pessoais alinhadas aos objetivos e necessidades da organização.
- Identificar, avaliar e mitigar riscos relacionados à privacidade e proteção de dados pessoais, garantindo que medidas adequadas estejam em vigor para proteger os ativos da empresa.
- Orientar a organização para que esteja em conformidade com todas as leis, regulamentações e normas de privacidade e proteção de dados aplicáveis.
- Reportar regularmente sobre o estado da privacidade e proteção de dados pessoais à alta administração, fornecendo análises e recomendações para melhorias.
- Apoiar na coordenação e resposta a incidentes de privacidade, incluindo a investigação de violações e mitigação de impactos.
- Implementar programas de treinamento e conscientização sobre privacidade e proteção de dados pessoais para funcionários e partes interessadas, em colaboração com os departamentos de TI e RH.
- Avaliação de Fornecedores: Avaliar a segurança da informação dos fornecedores e parceiros, garantindo que estejam alinhados com os padrões de segurança da empresa.

- Manter-se atualizado com as últimas tendências e tecnologias, promovendo a inovação e a melhoria contínua dos processos de privacidade e proteção de dados pessoais.

Gestores de Pessoas e/ou Processos devem:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os funcionários sob a sua gestão;
- Verificar se os funcionários sob sua gestão, na fase de contratação e de formalização dos contratos individuais de trabalho e de prestação de serviços foram informados desta política e se foi coletado o aceite.
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política de segurança da informação.

A Comissão de Compliance deve:

- Analisar a aplicação de sanções e punições desta política, bem como demais normas e procedimentos de segurança.

Os usuários da Informação devem:

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança do SGSI;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, e das normas e procedimentos de Segurança da Informação ou, quando pertinente, a Comissão de Segurança da Informação;
- Comunicar a área de Tecnologia e Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Vports;
- Assinar o Termo de Aceite formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
- Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.
- A proteção da integridade, disponibilidade e confidencialidade é responsabilidade do proprietário e do custodiante de cada ativo.
- Todos os incidentes e as fragilidades de segurança devem ser reportados a área de Tecnologia e Segurança da Informação que definirá quais informações relativas à segurança da informação serão comunicadas para qual parte interessada internamente e externamente, por quem e quando.

4.5. Comunicação da política

Esta política deve ser comunicada para todos os funcionários da Vports, bem como para todas as partes externas apropriadas.

5. Canal de denúncias

A VPORTS disponibiliza um canal especializado e independente para que todos os Colaboradores e Terceiros, anonimamente ou não, possam reportar suspeitas ou violação às diretrizes estabelecidas nesta Política ou em qualquer outro normativo relacionado, através do site ou telefone:

- Site: www.canaldedenuncia.com.br/vports
- Telefone: 0800 721 0729

É vedada qualquer forma de retaliação contra aqueles que, de boa-fé, comuniquem as violações ou suspeitas de violações a esta Política ou à legislação vigente.

6. Penalidades

O não cumprimento das regras estabelecidas nesta Política sujeitará o Colaborador envolvido à aplicação das medidas disciplinares, de acordo com as normas internas da VPORTS, sem prejuízo das sanções administrativas, cíveis, penais ou outras medidas cabíveis.

Em relação a Terceiros, o descumprimento desta Política ou da legislação aplicável poderá ensejar a imediata rescisão contratual, com aplicação das penalidades decorrentes da rescisão, sem prejuízo de ação indenizatória e outras providências legais.

7. Suporte para o SGSI

Deste modo, a Alta Direção da Vports declara que a implementação do SGSI e seu contínuo aprimoramento serão suportados pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como para atender todos os requisitos identificados.

8. Validade e gestão de documentos

Este documento é válido a partir de sua aprovação.

O proprietário deste documento é o Gerente de Tecnologia da Informação, que deve verificar e, se necessário, atualizar o documento anualmente.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- Quantidade de funcionários e terceiros que têm um papel no SGSI, mas não conhecem este documento;
- Não conformidade do SGSI com as leis e as regulamentações, as obrigações contratuais e outros documentos internos da organização;
- Ineficácia da manutenção e da implementação do SGSI;
- Responsabilidades confusas na implementação do SGSI.