1. FINALIDADE, ESCOPO E DESTINATÁRIOS

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação. 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 relevantes.

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)

3. CRIAÇÃO E ATUALIZAÇÃO

A área de Tecnologia da Informação é a área proponente e responsável pela criação, revisão e atualização desta Política, garantindo sua adequação às necessidades da organização e conformidade com os requisitos normativos e regulatórios aplicáveis.

4. TERMOS E DEFINIÇÕES

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

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

Disponibilidade - características das informações que somente pode ser acessada por pessoas autorizadas quando for necessário.

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

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

5. DIRETRIZES GERAIS

5.1 Gerenciando a segurança da informação

5.1.1 Objetivo e Medição

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

- 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 de segurança da informação, onde são verificados os índices de atendimento conforme indicadores definidos.

5.1.2 Requisitos de segurança da informação

A Alta Direção e o Comitê Gestor de Segurança da Informação 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 deve 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.

Os requisitos contratuais e legais são registrados e controlados através do sistema CAL.

5.1.3 Controles da segurança da informação

Os processos para selecionar os controles (salvaguardas) serão definidos na Metodologia de Avaliação de Riscos e de Tratamento do Risco de Segurança da Informação (SGSI-DOC-002).

Os controles selecionados e seu status de implementação serão listados na Declaração de Aplicabilidade (SGSI-DOC-027).

5.1.4 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 está 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.

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.

O Chief Information Security Officer as a Service (CISOaaS) deve:

- 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.

- Implementar programas de treinamento e conscientização sobre segurança da informação para funcionários e partes interessadas, em colaboração com os departamentos de TI e RH.

- 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.

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 as a Service (DPOaaS) 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.

O Comitê 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, ao Comitê Gestor 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.

Comunicação da política

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

5.1.5 Sanções e Punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições será realizada conforme a análise do Comitê de Compliance, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Comitê de Compliance, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

No caso de terceiros contratados ou prestadores de serviço, o Comitê de Compliance deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano à Vports, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nesta política.

5.2 Suporte para 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.

6. ATRIBUIÇÕES E RESPONSABILIDADES

RESPONSÁVEIS	DESCRIÇÃO
Tecnologia da Informação	Garantir o cumprimento, comunicação e atualização dessa Política
Trabalhadores	Cumprir com o que está estabelecido nesta Política

7. ANEXOS

N/A

8. DISPOSIÇÕES FINAIS

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.