

Política de Segurança da Informação

SII/ITP

ÍNDICE

1. Introdução.....	3
1.1. Âmbito e Objetivo.....	3
1.2. Referências	3
2. Política de Segurança da Informação	4
3. Princípios Orientadores da Segurança da Informação.....	4
4. O Modelo de Governo de Segurança da Informação da SILVIP	5

1. INTRODUÇÃO

1.1. ÂMBITO E OBJETIVO

Esta Política estabelece os objetivos de Segurança de Informação na *SILVIP*, servindo a mesma como linha orientadora de todas as Políticas de Segurança da Informação existentes no Modelo de Governo de Segurança da Informação da *SILVIP*.

O presente documento aplica-se a:

- todas as Unidades Orgânicas da *SILVIP*;
- todos os procedimentos e atividades da *SILVIP*;
- todos os procedimentos e atividades desenvolvidas pela *SILVIP*.

Todos os colaboradores, têm de cumprir com as regras estipuladas que lhes são aplicáveis.

1.2. REFERÊNCIAS

ISO 27000:2018 - Sistemas de gestão de segurança da informação – Visão geral e vocabulário.

ISO 27001:2013 - Sistemas de gestão de segurança da informação – Requisitos. A.5 Políticas de Segurança da Informação.

ISO 27002:2013 - Tecnologia de informação - Técnicas de segurança. Código de práticas para controlos de segurança da informação. Cap. 5.

ISO/IEC 27001:2022 – Requisitos e Controlos - Sistemas de gestão de segurança da informação – Requisitos.

ISO 27002:2022 – Tecnologia de informação – Técnicas de segurança. Código de práticas para controlos de segurança da informação.

Código de Conduta da *SILVIP*.

Manual de Estrutura Organizacional da *SILVIP*.

Manual de Procedimentos da *SILVIP*.

Lei n.º 7/2009, de 12 de fevereiro, conforme alterado – Código do Trabalho.

ISO 27000:2018 – Sistemas de gestão de segurança da informação – Visão geral e vocabulário.

ISO/IEC 27005 – Information Technology – Security techniques – Information security risk management.

NP ISO/IEC 31000 – Gestão do Risco – Linhas de orientação.

Quadro Nacional de Referência para a Cibersegurança.

Enterprise Risk Management | Compliance Risk Management: Applying the COSO ERM Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), Nov. 2020.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação da *SILVIP* é aplicável a todos os colaboradores, tendo os mesmos a obrigação de atuar em conformidade com as Políticas e restante documentação do Modelo de Governo da Segurança da Informação.

A Política de Segurança da Informação aplica-se a todos os ativos informacionais da organização, independentemente do seu suporte. Inclui informação em papel, armazenada digitalmente ou em outros suportes, informação transmitida por correio, por canais digitais e por comunicação oral, incluindo telefone e correio de voz. Inclui texto, imagens, áudio e vídeo. Por inerência, aplica-se também a todos os ativos relacionados com o tratamento de informação.

Aplica-se ao longo de todo o ciclo de vida da informação, desde a criação, passando pelo armazenamento e utilização, até à sua eliminação.

3. PRINCÍPIOS ORIENTADORES DA SEGURANÇA DA INFORMAÇÃO

A *SILVIP* está comprometida com o zelo pelos ativos dos quais é responsável, tendo como princípios:

- Garantir a segurança de toda a informação da *SILVIP*, protegendo os seus sistemas de informação com base nos pilares de Confidencialidade, Integridade e Disponibilidade;
- Assegurar a conformidade das práticas com requisitos externos relativos à informação (como leis, regulamentos, requisitos de clientes ou parceiros);
- Desenvolver e manter políticas, procedimentos e diretrizes apropriados para manter um alto padrão de segurança da tecnologia da informação, refletindo as melhores práticas do setor;
- Garantir a melhoria contínua de políticas e práticas de segurança, com o objetivo de elevar o estado de maturidade da organização face às suas tecnologias de informação;
- Realizar uma adequada gestão de incidentes de segurança, através de adequados processos de prevenção, deteção, registo, comunicação e tratamento;
- Promover a consciencialização e formação dos Colaboradores no domínio da segurança da informação;
- Incorporar a segurança de informação em todos os processos de negócio da organização, incluindo a definição de requisitos de segurança para qualquer projeto ou relação contratual;
- Manter um processo de gestão de risco robusto, capaz de guiar a gestão da segurança de informação na *SILVIP*;
- Realizar auditorias internas e externas aos seus sistemas e procedimentos, de forma a avaliar a sua conformidade com os requisitos de segurança da informação, estabelecidos e atuar no sentido de elevar a maturidade da organização .

4. O MODELO DE GOVERNO DE SEGURANÇA DA INFORMAÇÃO DA SILVIP

O Modelo de Governo de Segurança da Informação da SILVIP tem por objetivo assegurar que as suas atividades estão de acordo com todas as disposições legislativas, regulamentares e normativos relevantes, ao nível da segurança da informação.

O atual Modelo de Governo da SILVIP aborda a segurança da informação de forma holística, nas suas diferentes vertentes – pessoas, processos e tecnologia, no sentido de melhorar continuamente a eficácia do seu sistema de gestão da informação, seguindo as boas práticas da norma ISO/IEC 2700, e assenta nos três pilares fundamentais da segurança da informação:

- Confidencialidade: garantia de que a informação está acessível apenas a utilizadores e entidades externas devidamente autorizados para o efeito;
- Integridade: salvaguarda da exatidão da informação e dos métodos de processamento;
- Disponibilidade: garantia de que utilizadores autorizados têm acesso à informação sempre que necessário.

Com efeito, foi elaborado e implementado um conjunto de Políticas que suportam e operacionalizam a Política de Segurança da Informação e que no seu conjunto constituem o Modelo de Governo de Segurança da Informação da SILVIP, através da adoção de uma estratégia assente na melhoria contínua e por uma gestão de risco robusta, que permita identificar oportunidades e prevenir eventos indesejáveis.

As Políticas específicas que constituem o Modelo de Governo de Segurança da Informação da SILVIP, são:

- PSI -01_Política de Segurança da Informação;
- PSI -02_Política de Gestão De Recursos Humanos;
- PSI -03_Política de Trabalho Remoto E Dispositivos Móveis;
- PSI -04_Política de Gestão De Ativos;
- PSI -05_Política de Classificação Da Informação;
- PSI -06_Política de Transferência De Informação;
- PSI -07_Política de Utilização Aceitável De Ativos;
- PSI -08_Política de Gestão De Acessos;
- PSI -09_Política de Gestão Da Mudança;
- PSI -10_Política de Segurança Física;
- PSI -11_Política de Segurança De Operações E Comunicações;
- PSI -12_Política de *Backup*;
- PSI -13_Política de Palavras-Passe;
- PSI -14_Política de Gestão De Fornecedores;
- PSI -15_Política de Gestão De Incidentes.

A SILVIP tomará todas as medidas consideradas necessárias para responder a qualquer violação destas políticas, incluindo o uso de processo disciplinar quando apropriado.

Lisboa, agosto de 2024.