

PrivSecOpsIT

Política do Sistema de Gestão Integrado

Versão Português

Sumário

1. OBJETIVO	3
2. ABRANGÊNCIA	3
3. DEFINIÇÕES	3
4. DIRETRIZES	4
4.1. Sistema de Gestão de Segurança Integrado	4
4.2. Política do Sistema de Gestão Integrado	5
5. DISPOSIÇÕES FINAIS	5
6. HISTÓRICO DE REVISÃO	6
7. ENGLISH VERSION OF THE POLICY	7
1. OBJECTIVE	8
2. APPLICABILITY	8
3. ROLES AND RESPONSIBILITIES	8
4. GUIDELINES	8
4.1. THEME	8
5. FINAL DISPOSITIONS	8
6. REVISION HISTORY	9

1. OBJETIVO

Como um dos objetivos da área de Segurança da Informação da Pipefy, a certificação de seu Sistema de Gestão de Segurança da Informação na ISO 27001 tem uma série de requisitos e registros que devem garantir a manutenção e eficácia de todo o sistema em seu ciclo PDCA.

O objetivo deste Manual do Sistema de Gerenciamento de Segurança da Informação é manter um repositório unificado onde vários destes pontos são descritos e detalhados.

Este conjunto de informações relativas ao SGSI servirá como um guia para a Equipe de Segurança da Informação da Pipefy.

A correta manutenção e atualização deste Manual trará uma série de benefícios ao Sistema de Gerenciamento de Segurança da Informação e apoiará a Organização em seu processo de tomada de decisões.

O objetivo deste Manual é fornecer uma visão do Sistema de Gestão de Segurança da Informação - SGSI da Pipefy, a fim de orientar a conduta da Alta Administração, do Comitê de Segurança da Informação, de seus funcionários e de outras partes interessadas da Pipefy, a qualquer momento, nível hierárquico, sobre questões relacionadas à segurança das informações geradas ou mantidas pela Organização e dos ativos que suportam essas informações.

2. ABRANGÊNCIA

Este Manual é aplicável a todos os locais da Pipefy, indivíduos, prestadores de serviços e outras partes interessadas que interagem ou são parte do escopo de nosso SGSI.

3. DEFINIÇÕES

ISMS: Information Security Management System - Sistema de Gestão de Segurança da Informação

SGSI: Sistema de Gestão de Segurança da Informação.

Risco: combinação da probabilidade da concretização de uma ameaça e suas consequências.

PrivSecOps: é um time dedicado de Segurança, Privacidade e IT Operations do Pipefy. O time é responsável pelas demandas de privacidade e proteção de dados, segurança do ambiente e produto pipefy, bem como por sua governança de tecnologia, sendo complementado pelo time de IT Operations, que é responsável por gerir acessos, administrar hardware e prestar suporte para os times internos da Pipefy.

4. DIRETRIZES

4.1. Sistema de Gestão de Segurança Integrado

A proteção das informações corporativas e dados pessoais não consiste apenas em estabelecer regras de segurança e zelar para que as pessoas as sigam. A preocupação primordial é estabelecer um processo em que, com base em indicadores e objetivos definidos, onde sejam estabelecidas ações que busquem implementar o que foi planejado, haja o acompanhamento e validação dos resultados através de métricas pré-definidas e que estas sejam avaliadas, e lições aprendidas e correções são feitas no final do ciclo para melhorá-lo.

Esse processo, denominado Sistema de Gestão Integrado, está baseados nas normas:

- ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos
- ISO/IEC 27701:2019 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
- ISO/IEC 27018:2021 - Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP

A segurança da informação, segurança cibernética e proteção à privacidade protege as informações de diversos tipos de ameaças, a fim de minimizar os danos aos negócios e maximizar o retorno dos investimentos e caracteriza-se pela preservação de três fatores:

- a)** Confidencialidade: garantir que a informação seja acessível apenas por pessoas autorizadas a ter acesso;
- b)** Integridade: zelar pela exatidão e integridade das informações e métodos de processamento;
- c)** Disponibilidade: garantir que os usuários autorizados tenham acesso às informações e aos respectivos ativos sempre que necessário.

A participação e contribuição de todos os colaboradores é essencial para o sucesso do SGI. Toda a força de trabalho do Pipefy é responsável pela segurança da informação, segurança cibernética e proteção à

privacidade. A equipe de PrivSecOpsIT, Gerentes e Executivos têm o protagonismo no desenvolvimento das ações exigidas pelo SGI

4.2. Política do Sistema de Gestão Integrado

A Pipefy tem como premissa estratégica a segurança da Informação, segurança cibernética e proteção à privacidade, portanto todos os colaboradores devem conhecer e praticar a nossa Política do Sistema de Gestão Integrado, que consiste em:

- Promover o cumprimento das leis, normas e regulamentos relacionados aos negócios em seus aspectos relacionados à Segurança e Privacidade da Informação;
- Melhorar continuamente a segurança da informação, segurança cibernética, proteção à privacidade e maturidade na Plataforma Pipefy para mitigar riscos.
- Aumentar o conhecimento interno e a conscientização sobre a necessidade de Segurança da Informação e privacidade de dados pessoais para o negócio.

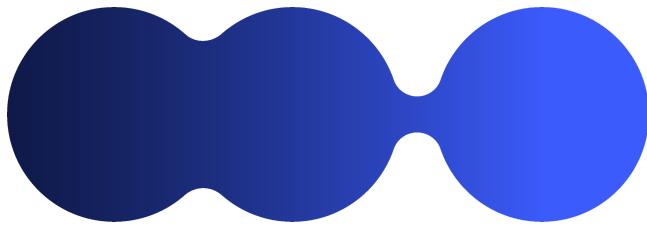
5. DISPOSIÇÕES FINAIS

Esse documento foi criado para formalizar e manter o processo de gestão de Segurança da Informação na Organização. Esse documento será gerido e atualizado anualmente ou após mudanças significativas, atendendo às melhores práticas de SI.

6. HISTÓRICO DE REVISÃO

#	Data	Descrição
1.0	10 de Abril 2023	Criação do Documento

7. ENGLISH VERSION OF THE POLICY



PrivSecOps

Integrated Management System Policy

English Version

1. OBJECTIVE

As one of the goals of Pipefy's Information Security area, the certification of its Information Security Management System in ISO 27001 has a series of requirements and records that should ensure the maintenance and effectiveness of the entire system in its PDCA cycle.

The purpose of this Information Security Management System Manual is to maintain a unified repository where a number of these points are described and detailed.

This set of ISMS-related information will serve as a guide for Pipefy's Information Security Team.

Proper maintenance and updating of this Manual will bring a number of benefits to the Information Security Management System and support the Organization in its decision making process.

The purpose of this Manual is to provide a vision of Pipefy's Information Security Management System - ISMS, in order to guide the conduct of Senior Management, the Information Security Committee, its employees and other Pipefy stakeholders, at any time. hierarchical level, on issues related to the security of information generated or maintained by the Organization and the assets supporting that information.

2. APPLICABILITY

This Manual is applicable to all Pipefy locations, individuals, service providers and other stakeholders who interact with or are part of the scope of our ISMS.

3. ROLES AND RESPONSIBILITIES

ISMS: Information Security Management System

ISMS: Information Security Management System.

Risk: combination of the probability of a threat materializing and its consequences.

PrivSecOps: is Pipefy's dedicated Security, Privacy and IT Operations team. The team is responsible for the demands of privacy and data protection, security of the Pipefy environment and product, as well as its technology governance, and is complemented by the IT Operations team, which is responsible for managing access, administering hardware and providing support to Pipefy's internal teams.

4. GUIDELINES

4.1. Integrated Security Management System

The protection of corporate information and personal data is not only about establishing security rules and making sure that people follow them. The overriding concern is to establish a process in which, based on defined indicators and objectives, where actions are established that seek to implement what was planned, there is the monitoring and validation of results through predefined metrics and that these are evaluated, and lessons learned and corrections are made at the end of the cycle to improve it.

This process, called Integrated Management System, is based on the standards:

- ISO/IEC 27001:2022 - Information security, cyber security and privacy protection - Information security management systems - Requirements
- ISO/IEC 27701:2019 - Security techniques - Extension of ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 to information privacy management - Requirements and guidelines
- ISO/IEC 27018:2021 - Information technology - Security techniques - Code of practice for personal data (PD) protection in public clouds acting as PD operators

Information security, cybersecurity and privacy protection protects information from various types of threats in order to minimize business damage and maximize return on investment and is characterized by preserving three factors:

- Confidentiality: ensuring that information is accessible only by persons authorized to have access;
- Integrity: ensure the accuracy and integrity of information and processing methods;
- Availability: ensure that authorized users have access to the information and respective assets whenever necessary.

The participation and contribution of all employees is essential for the SGI success. Pipefy's entire workforce is responsible for information security, cybersecurity, and privacy protection. The PrivSecOpsIT team, Managers and Executives have the leading role in the development of the actions required by the IMS

4.2. Integrated Management System Policy

Pipefy has as strategic premise the Information security cyber security and privacy protection, so all employees should know and practice our Integrated Management System Policy, which consists of:

- Promote compliance with business-related laws, rules and regulations in their aspects related to Information Security and Privacy;
- Continuously improve information security, cyber security, privacy protection and maturity in Pipefy Platform to mitigate risks.
- Increase internal knowledge and awareness about the need for Information Security and privacy of personal data for the business.

5. FINAL DISPOSITIONS

This document was created to formalize and maintain the Information Security management process in the Organization. This document will be managed and updated annually or after significant changes, meeting IS best practices.

6. REVISION HISTORY

#	Date	Description
1.0	April 10, 2023	Document Creation