

Política de Segurança da Informação - Pública

1. Objetivo

A presente Política de Segurança da Informação, visa estabelecer o Sistema de Gestão da Segurança da Informação e consolidar as diretrizes a serem adotadas pela Ipiranga (incluindo fornecedores de produtos e/ou serviços), para tratar de Segurança da Informação. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

Este documento deve ser considerado em conjunto com a [Política Corporativa - Código de Ética](#) e as demais políticas e normas da Ipiranga.

2. Público-Alvo

Esta Política é aplicável a todas as partes interessadas.

3. Papéis e Responsabilidades

- **Diretoria Executiva:** Aprovar a Política e garantir recursos e apoio para sua implementação.
- **Comitê de Segurança da Informação:** Estruturar e definir o planejamento estratégico de Segurança da Informação.
- **Segurança da Informação:** mantém e monitora o cumprimento da Política e dos controles de segurança.
- **Gestores:** Assegurar que suas equipes sigam as diretrizes e proteger as informações sob sua responsabilidade.
- **Colaboradores e Terceiros:** Cumprir a Política, utilizar os recursos de forma segura e comunicar incidentes.
- **Tecnologia da Informação:** Implementar e manter controles técnicos que suportam a proteção das informações.

4. Termos e Definições

- **Confidencialidade:** As informações devem estar disponíveis apenas para indivíduos, entidades e/ou processos autorizados pela Ipiranga.
- **Integridade:** O processamento de informações na Ipiranga deve garantir a sua exatidão e a sua completude.
- **Disponibilidade:** as informações e os ambientes de tecnologia da Ipiranga devem estar acessíveis e disponíveis aos usuários de maneira permanente.

- **Autenticidade:** é fundamental que as informações sejam verdadeiras e seguras. Isto é, elas precisam ser decorrentes de fontes confiáveis.
- **Privacidade:** a privacidade se pode definir como o direito que tem o indivíduo de manter indevidados dados e informações que lhe digam respeito.

5. Descrição das Regras Gerais

5.1. Política de Segurança da Informação

- Garantir a satisfação dos nossos clientes e prover a melhoria contínua dos processos e serviços de tecnologia considerando: Confidencialidade, integridade e disponibilidade das informações das partes interessada.

5.2. Gestão de Segurança da Informação

- De forma geral, a organização baseia sua estratégia de segurança da informação nas exigências e boas práticas de mercado e em requisitos definidos na Norma Internacional de Gestão de Segurança da Informação – ISO 27001/2022.
- A implementação de mecanismos e controles de segurança deve ser justificada com base no valor associado às informações envolvidas e ao impacto oriundo da eventual perda dessas informações.
- Os registros de auditoria dos acessos e alterações das informações críticas devem ser devidamente mantidos e tais registros devem possibilitar a identificação de qualquer operação ou alteração não autorizada.
- Devem ser priorizadas medidas preventivas ao contrário de controles reativos e, sempre que possível, as medidas de segurança devem ser atendidas através de soluções técnicas que não dependam de processos manuais ou que não estejam sujeitas a erros humanos.

Atualizado pela última vez em 13 de novembro de 2025.