

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

A **MIROMA** é constituída por uma equipa unida e flexível, onde o potencial individual dos colaboradores é maximizado por uma liderança transparente, forte e acessível, sempre orientada para melhor servir o cliente.

Na **MIROMA** antecipamos e transformamos as necessidades dos nossos clientes em resultados e estabelecemos, com os mesmos, relações de confiança.

Investimos na melhoria contínua das nossas competências e na qualidade dos nossos produtos e serviços, cumprindo as normas e procedimentos de segurança da informação, assim como a legislação aplicável.

Apostamos na criação de um ambiente de satisfação e valorização pessoal dos colaboradores.

Procuramos ser uma referência na nossa área de atuação e retribuir valor aos acionistas.

A importância que damos à Informação, associada a uma utilização adequada e segura da mesma, é a razão do nosso investimento na implementação de uma prática regular e quotidiana, onde a informação (e a sua gestão) é considerada uma componente vital para o nosso êxito.

As políticas e as normas corporativas definidas para gerir a segurança da informação estão alinhadas com a missão e os objetivos da **MIROMA**, nomeadamente no que respeita à promoção do nosso negócio e à garantia dos requisitos da segurança da informação.

O nosso **SGSI** – Sistema de Gestão da Segurança da Informação está orientado para os seguintes objetivos:

1. É adequado ao propósito e ao contexto da **MIROMA**;
2. Inclui o comprometimento da gestão de topo para satisfazer os requisitos da segurança da informação;
3. Preservar a confidencialidade, integridade e disponibilidade da informação de suporte aos processos de negócio e da empresa;
4. Proteger a informação de acessos ilícitos e de tratamentos incorretos ou indesejados (voluntários ou involuntários, internos ou externos), através da implementação de controlos de segurança criados para esse efeito;
5. Promover a melhoria contínua de todos os processos organizacionais, potenciando a sua otimização, eficácia e eficiência, nomeadamente os que suportam o SGSI – Sistema de Gestão da Segurança da Informação;
6. Gerir a informação de acordo com os pressupostos e objetivos da Política da Segurança da Informação, reduzindo e vigiando as vulnerabilidades dos ativos através de uma análise e gestão adequada dos riscos e potenciais impactos;
7. Garantir que os recursos necessários para o SGSI – Sistema de Gestão da Segurança da Informação estão disponíveis;
8. Assegurar que o SGSI – Sistema de Gestão da Segurança da Informação atinge os KPI's a que se propõe.

A Presidente da **MIROMA** assume a liderança dos objetivos de segurança e o compromisso de dar suporte à Política de Segurança da Informação. A estratégia da Presidente tem como vetor orientador o alinhamento de todos os processos da organização, disponibilizando os recursos necessários para garantir o uso; mas também a segurança da informação, por forma a atingir os objetivos pretendidos.

A nossa Política de Segurança da Informação assenta nos seguintes princípios:

- Cumprir e assegurar todos os níveis de serviço/SLA – *Service Level Agreement* assumidos com entidades terceiras (fornecedores, clientes e outras entidades interessadas);
- Assegurar a integração dos requisitos de informação e objetivos de segurança da informação nos processos de negócio da **MIROMA**;
- Comunicar, formar e sensibilizar continuamente todos os colaboradores da **MIROMA** por forma a garantir uma cultura interna e uma prática diária em conformidade com as normas legais e organizacionais em matéria de segurança da informação;
- Assegurar o cumprimento de todas as normas legais em vigor em matéria de segurança da informação, nomeadamente a Norma 27001;
- Realizar uma análise da informação recebida pelas partes interessadas;
- Assegurar que é realizada a análise de tendências sobre o desempenho face a períodos anteriores;
- Definir e implementar um sistema de gestão e monitorização de todas as operações, garantindo a capacidade para detetar, reportar, analisar e corrigir vulnerabilidades do SGSI – Sistema de Gestão da Segurança da Informação;
- Prever a capacidade de resposta a incidentes de segurança e garantir a continuidade de negócio. Para assegurar este pressuposto, os planos de recuperação de desastre e de continuidade do negócio são testados, revistos e atualizados periodicamente;
- Definir e implementar procedimentos adequados ao reporte de incidentes de segurança e implementar processos de responsabilização e punição para as transgressões às normas internas e regras do SGSI.