

**BOAS PRÁTICAS PARA SEGURANÇA DA
INFORMAÇÃO DA EMPRESA MUNICIPAL
DE INFORMÁTICA - Emprel**

PSI
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Diretrizes Gerais
Versão 1.0

Palavras-chave: Política, Segurança, Informação, Diretrizes, Sanções, Normas, Risco, Continuidade, Incidente, ativo, Confidencialidade, Disponibilidade, Integridade, EMPREL..

Direitos autorais exclusivos da Emprel, sendo permitida reprodução parcial ou total, desde que citada a fonte (Emprel), mantido o texto original e não acrescentado nenhum tipo de propaganda comercial.

Esse Documento é classificado como público

Política de Segurança da Informação da EMPREL	3
Princípios	3
Disponibilidade e Comunicação	4
Violações e Sanções Aplicáveis	4

BOAS PRÁTICAS PARA SEGURANÇA DA INFORMAÇÃO DA EMPRESA MUNICIPAL DE INFORMÁTICA – EMPREL

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Palavras-chave: Política, Segurança, Informação, Diretrizes, Sanções, Normas, Risco, Continuidade, Incidente, ativo, Confidencialidade, Disponibilidade, Integridade, EMPREL.

Direitos autorais exclusivos da Emprel, sendo permitida reprodução parcial ou total, desde que citada a fonte (Emprel), mantido o texto original e não acrescentado nenhum tipo de propaganda comercial.

Este documento é classificado como público.

Política de Segurança da Informação da EMPREL

Esta política aplica-se e deve ser seguida por todos os empregados, servidores postos à disposição por órgãos ou entidades da administração centralizada ou descentralizada, federal, estadual ou municipal, não importando o regime jurídico a que estejam submetidos, prestadores de serviço alocados na prestação de serviços por força de contrato, e colaboradores em geral que, direta ou indiretamente, utilizem os sistemas da EMPREL para o desenvolvimento de suas atividades profissionais no escopo do Sistema de Gestão da Segurança da Informação e demais partes interessadas atuando sob a gestão da organização.

É dever de todos, de acordo com seus papéis, autoridades e responsabilidades atribuídas:

- Atuar de forma transparente e responsável para evitar a perda da Confidencialidade, Integridade e Disponibilidade das informações tratadas pela organização, bem como dos recursos (ativos de informação) utilizados para este fim.
- Identificar, analisar, avaliar e tratar os riscos e oportunidades relacionadas à Segurança da Informação.
- Proteger os dados pessoais identificáveis, bem como identificar, analisar, avaliar e tratar os riscos e oportunidades para os titulares desses dados.
- Definir, a partir da análise do contexto e dos riscos, os objetivos de segurança da informação e gerenciar os processos visando atingir tais objetivos.
- Cumprir e comprometer-se com as diretrizes, políticas e procedimentos do RISI (Regulamento Interno de Segurança da Informação) e do SGSI da organização, incluindo os processos organizacionais.
- Comprometer-se com os requisitos aplicáveis, incluindo requisitos legais, regulamentares, estatutários, contratuais e dos processos e práticas adotadas pela organização.
- Buscar continuamente a melhoria da Segurança da Informação e do SGSI.

Princípios

A Política de Segurança de Informações da EMPREL adotará os seguintes princípios:

I - Salvaguarda dos dados, informações, documentos e materiais sigilosos de interesse e responsabilidade da EMPREL, bem como dos sistemas computacionais e das áreas e instalações onde tramitam, respeitando os critérios de:

- a) Garantia dos direitos individuais e coletivos.
- b) Garantia da privacidade e segurança das pessoas físicas e jurídicas.
- c) Garantia de acesso às informações disseminadas pela Prefeitura através de seus serviços de rede.

II - Promoção de medidas para evitar:

- a) Destruição, modificação ou divulgação indevida de informações, documentos e materiais sigilosos, sejam eles acidentais ou intencionais, e para impedir fraudes.
- b) Danos a dados ou programas de computador.
- c) Acessos indevidos ou não autorizados às informações disponíveis.
- d) Alteração indevida de senhas ou mecanismos de acesso a programas de computador ou dados.

III - Elaboração de planos de contingência e continuidade dos serviços informatizados, de forma a garantir a continuidade em casos de sinistros, panes elétricas ou mecânicas, ou outras causas de descontinuidade.c

Disponibilidade e Comunicação

A Política de Segurança da Informação deve ser disponibilizada:

- No website da organização.
- Por e-mail, quando solicitado pela parte interessada.
- Via intranet.

Esta política deve ser comunicada aos colaboradores:

- Durante o processo de admissão e integração.
- Por meio da intranet.
- Durante o programa de conscientização sobre Segurança da Informação.
- Em caso de alterações no seu conteúdo.

Violações e Sanções Aplicáveis

O colaborador que praticar ou tentar ações contrárias ao estabelecido nesta Política de Segurança da Informação, colocando em risco a Segurança da Informação, ou quaisquer incidentes que violem esta Política, deve ser comunicado imediatamente à Gerência de Segurança da Informação, ao suporte ou a qualquer usuário ciente do ocorrido.

Esses casos serão avaliados pelo Comitê de Segurança da Informação, que recomendará as medidas necessárias. Dependendo da gravidade do ato, o colaborador estará sujeito às penalidades previstas em lei e no processo disciplinar da organização.

O Comitê de Segurança da Informação submeterá à Gestão da EMPREL os resultados de seu trabalho, destacando os pontos mais relevantes e que requeiram maior atenção para deliberação final. Este documento será publicado na intranet para publicidade e conhecimento geral dos usuários da EMPREL.

Este documento entrará em vigor a partir da data de sua publicação.

Bernardo Juarez D´Almeida
Diretor Presidente

Alyson Carvalho Pereira de Matos
Diretor de Infraestrutura de Informática

Jorge Luiz Pinto de Souza
CISO

Versão 2.6 - 2024