# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

| | |
|---|---|
| **CÓDIGO:** | **PO SGSI 01** |
| **VERSÃO:** | 1.0 |
| **DATA DA VERSÃO:** | 25/07/2022 |
| **CRIADO POR:** | RMSAfe |
| **APROVADO POR:** | |
| **NÍVEL DE CONFIDENCIALIDADE:** | **EXTERNO** |

## HISTÓRICO DE ALTERAÇÕES

| DATA | VERSÃO | CRIADO POR | DESCRIÇÃO DA ALTERAÇÃO |
|---|---|---|---|
| 13/04/2022 | 1.0 | RMSAfe | DOCUMENTAÇÃO DA POLÍTICA |
| 25/07/2022 | 1.0 | RMSAfe | REVISÃO |
| | | | |
| | | | |
| | | | |

# SUMÁRIO

## 1. INTRODUÇÃO

Os primeiros passos para a implementação do **Sistema de Gestão de Segurança da Informação** é a adoção de uma **Política de Segurança da Informação**, definida e aprovada pelo Comitê de Privacidade. A eficácia deste documento depende da combinação de requisitos do negócio, de estrutura de processos, do uso de tecnologias e mecanismos de proteção e, o mais importante, depende do comportamento de seus colaboradores e prestadores de serviço, independentemente do nível hierárquico ou da atividade desenvolvida para a TRINUS.

Para ampliar a cultura de segurança da informação e privacidade, a TRINUS alinhada às boas práticas e normas internacionalmente aceitas, criou sua **Política de Segurança da Informação**, a fim de adequá-la à legislação nacional vigente e garantir a proteção de todos os seus ativos tangíveis e intangíveis.

## 2. OBJETIVOS

Declarar formalmente, por meio do Comitê de Privacidade, as diretrizes da TRINUS que visam à proteção de dados pessoais e informações com eficiência, eficácia e competitividade, de modo seguro, garantnindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade, assim como dos ativos de TI que as sustentam, de forma alinhada aos requisitos legais.

Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da TRINUS como resultado de falhas de segurança ou violação de dados pessoais.

Esta Política se aplica a todos os colaboradores da TRINUS, estagiários, parceiros, fornecedores, terceiros, prestadores de serviços e visitantes.

## 3. DIRETRIZES GERAIS

A TRINUS por meio dessa Política, busca:

- ✓ Assegurar o cumprimento de todas as suas obrigações legais, para atender aos requisitos regulamentares e contratuais pertinentes às suas atividades, a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD), 13.709 de agosto de 2018.

- ✓ Empregar medidas técnicas e organizacionais adequadas no tratamento e envidar esforços para proteção dos dados pessoais dos titulares contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses.
- ✓ Garantir a confidencialidade, integridade e disponibilidade das informações de seus clientes e da própria TRINUS, protegendo os sistemas de informação contra acessos indevidos e modificações não autorizadas;
- ✓ Assegurar que somente pessoas autorizadas tenham acesso às instalações da TRINUS, às informações e aos sistemas de informação;
- ✓ Conscientizar as pessoas das possíveis consequências para a TRINUS e para os seus colaboradores, sobre incidentes de segurança da informação ou violação as políticas de segurança e privacidade;
- ✓ Garantir a continuidade de seus negócios, protegendo os processos críticos contra falhas ou desastres significativos;
- ✓ Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos de segurança da informação e privacidade, enfatizando as obrigações das pessoas pela proteção de dados;
- ✓ Garantir que todas as responsabilidades pela segurança da informação e privacidade, estão claramente definidas e que as pessoas indicadas são competentes e capazes de cumprir com as atribuições;
- ✓ Melhorar continuamente o Programa de Segurança e Privacidade.

## 4. RISCOS

A não observância dos princípios e diretrizes constantes nesta Política e seus documentos complementares, podem impactar seriamente os clientes da TRINUS, possibilitar a violação de leis e regulamentos, e afetar negativamente a reputação e a estabilidade financeira da TRINUS.

Desvios e exceções devem ser tratados pelo Comitê de Privacidade.

## 5. ORIENTAÇÕES E RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO

## 5.1 Procedimento de composição, guarda, troca de senha e login

✓ Crie senhas complexas e as memorize;

✓ Não utilize datas comemorativas como senhas;

✓ Não anote senhas no bloco de notas, papeis ou em análogos;

✓ Não compartilhe login e senha com terceiros;

✓ A Trinus Investimentos em nenhuma hipótese solicitará sua senha.

## 5.2 Riscos envolvidos no uso da internet, métodos de prevenção e links de Internet

✓ Ao acessar sua conta Trinus Investimentos certifique-se de utilizar uma conexão segura;

✓ Não utilize wi-fi públicos, pois existe a possibilidade de pessoas má intencionadas acessarem seus dados;

✓ Não abra e-mail de remetentes desconhecidos, nem clique em links de origem duvidosa, visto que há risco de subtração de seus dados e instalação de vírus em seus dispositivos eletrônicos. Atualização de Segurança nos computadores

✓ Constantemente atualize os firewall e antivírus;

✓ Sempre atualize o software, assim como o computador, garantindo estar em consonância com a última versão do sistema operacional e dos aplicativos;

## 5.3 Segurança em computadores e dispositivos móveis

✓ Sempre bloquei sua tela, use códigos de bloqueio para evitar que outras pessoas utilizem seus aparelhos;

✓ Não baixe aplicativos, arquivos e documentos em sites de procedência duvidosa. Opte, sempre, por utilizar lojas oficiais;

✓ Utilize firewalls e antivírus em seus dispositivos eletrônicos, tais como celulares e computadores, para evitar a infecção do equipamento com programas (“vírus”) capazes de danificar e roubar dados pessoais.

Questões relacionadas a dispositivos informáticos e segurança da informação como um todo são reguladas pela presente política.