

POLÍTICA DE SEGURANÇA CIBERNÉTICA

POLÍTICA DE SEGURANÇA CIBERNÉTICA
USO EXTERNO
Aprovação: Diretoria
Data: versão - maio/2025
Elaboração: TI



SUMÁRIO

1.	NOSSA ABORDAGEM DE SEGURANÇA.....	3
2.	COMO PROTEGEMOS AS INFORMAÇÕES AQUI NA TRINUS?	3
3.	DICAS DE SEGURANÇA PARA VOCÊ	4
4.	REVISÃO	4



1. NOSSA ABORDAGEM DE SEGURANÇA

A Trinus adota medidas rigorosas para proteger suas informações, garantindo que elas sejam tratadas com cuidado e segurança. A política de segurança da informação da empresa é pautada em práticas avançadas que visam preservar a integridade, confidencialidade e disponibilidade dos dados, com uma estrutura robusta e monitoramento contínuo para proteção contra ameaças.

2. COMO PROTEGEMOS AS INFORMAÇÕES AQUI NA TRINUS?

A Trinus Co implementa um conjunto de controles para manter suas informações seguras em todas as etapas do processo:

- **Autenticação e Controle de Acesso:** Para garantir que apenas pessoas autorizadas tenham acesso aos dados, adotamos um processo de autenticação seguro e controle de acessos rigoroso em sistemas e ambientes físicos. Isso inclui senhas, biometria e autenticação multifatorial.
- **Criptografia:** Utilizamos criptografia avançada para proteger a confidencialidade dos dados armazenados e transmitidos, impedindo que informações sejam acessadas por pessoas não autorizadas.
- **Prevenção Contra Ameaças:** Protegemos nossos sistemas contra ameaças cibernéticas, como malwares e ataques de *phishing*, com ferramentas de segurança de última geração que detectam e bloqueiam códigos maliciosos.
- **Plano de Continuidade de Negócios (PCN):** Para garantir a continuidade das operações, contamos com um Plano de Continuidade de Negócios (PCN), que é revisado e testado regularmente. Esse plano assegura que a empresa possa responder a incidentes de maneira rápida e eficiente, minimizando qualquer impacto para os clientes.
- **Backup e Recuperação de Dados:** Mantemos um sistema robusto de backup, com cópias regulares das informações, o que garante a recuperação de dados em caso de incidentes.
- **Monitoramento e Testes de Vulnerabilidade:** Realizamos testes de segurança periódicos, como simulações de *phishing* e varreduras para identificar vulnerabilidades, além de monitoramento 24 horas, que nos permite responder rapidamente a ameaças emergentes.



- **Treinamentos e Conscientização:** Acreditamos que a segurança é uma responsabilidade compartilhada. Por isso, realizamos treinamentos regulares e programas de conscientização para que todos nossos colaboradores estejam preparados para identificar e evitar potenciais riscos.

3. DICAS DE SEGURANÇA PARA VOCÊ

Para aumentar a proteção de sua conta e prevenir fraudes, siga essas dicas simples:

- **Use senhas fortes e exclusivas:** Evite senhas óbvias e nunca compartilhe sua senha com ninguém. Habilite a autenticação em duas etapas sempre que disponível.
- **Cuidado com mensagens suspeitas:** Não clique em links nem forneça dados pessoais em mensagens de origem desconhecida ou não solicitada. Bancos não pedem informações confidenciais por e-mail ou SMS.
- **Prefira redes seguras:** Evite acessar o aplicativo do banco em redes Wi-Fi públicas ou desconhecidas. Use apenas conexões confiáveis para transações financeiras.
- **Habilite notificações de conta:** Ative notificações para monitorar movimentações em sua conta. Isso ajuda a identificar transações suspeitas em tempo real.
- **Desconfie de ofertas e promoções:** Verifique a autenticidade de mensagens com ofertas ou benefícios inesperados. Golpes podem ocorrer através de promessas muito vantajosas.

Na Trinus Co, a segurança de suas informações é prioridade. Nosso compromisso é manter seus dados protegidos e garantir a continuidade de nossos serviços com transparência e confiança.

4. REVISÃO

Esta Política será revisada, no mínimo, a cada dois anos ou sempre que houver alterações significativas na estrutura organizacional, regulatória ou estratégica da Trinus.

