

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO	2
2. TERMOS E DEFINIÇÕES	2
3. ABRANGÊNCIA	3
4. PRINCÍPIOS E DIRETRIZES	3
5. DISPOSIÇÕES GERAIS	7
6. ANEXOS E CORRELAÇÕES	7
7. HISTÓRICO DE REVISÕES	8

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	1

1. INTRODUÇÃO

A Trio reconhece que a informação é um dos seus principais ativos e, portanto, deve ser protegida de forma adequada.

Esta Política de Segurança da Informação (PSI) foi elaborada em conformidade com a Resolução BCB nº 85, de 8 de abril de 2021, refletindo o compromisso da Trio com o cumprimento das normas legais e regulamentares aplicáveis e, estabelece os princípios, diretrizes e responsabilidades para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações tratadas pela organização.

O objetivo é minimizar riscos, prevenir, detectar e reduzir a exposição a incidentes de segurança, assegurando a continuidade das operações, a proteção das informações corporativas e a conformidade com as leis e regulamentações aplicáveis, além de promover a cultura de segurança da informação entre colaboradores, prestadores de serviço e parceiros.

Esta PSI é complementada por Políticas específicas (como Senhas, Classificação da Informação, Backup, Gestão de Identidade e Acessos, entre outras), que estabelecem diretrizes, responsabilidades e controles técnicos e operacionais relacionados à segurança da informação.

2. TERMOS E DEFINIÇÕES

2.1.Quando referenciado nesta Política, os termos a seguir terão os seguintes significados:

2.1.1.Área de TI/SI: Área de Tecnologia da Informação / Segurança da Informação.

2.1.2.Ativos: Todos os recursos que possuem valor para a organização e que devem ser protegidos. Podem incluir: informações, aplicações, equipamentos, pessoas, etc.

2.1.3.Backup: Processo de criar cópias de segurança de dados, sistemas ou arquivos para garantir que possam ser recuperados em caso de perda, falha ou incidente.

2.1.4.Computação em Nuvem: Modelo de prestação e consumo de serviços de tecnologia (como servidores, armazenamento, bancos de dados e redes) entregues sob demanda através da internet.

2.1.5.Criptografia: Processo de transformar informações legíveis em dados codificados para protegê-las contra acessos não autorizados.

2.1.6.Incidentes: Eventos que comprometem ou tem potencial de comprometer a integridade, confidencialidade ou disponibilidade de ativos, dados ou sistemas.

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	2

2.1.7.LGPD: Lei Geral de Proteção de Dados, que estabelece regras para o tratamento de dados pessoais.

2.1.8.Logs: Registros automáticos de atividades realizadas em aplicações. São fundamentais para monitoramento, auditoria, diagnóstico de problemas, etc.

2.1.9.OWASP Top 10: Documento de conscientização padrão para desenvolvedores que lista e explica os riscos de segurança mais críticos em aplicações web.

2.1.10.Patches: Atualizações de software que corrigem falhas, vulnerabilidades ou melhoram funcionalidades.

2.1.11.Plano de Contingência / Continuidade de Negócios: Conjunto de procedimentos documentados para garantir que os processos críticos da empresa possam continuar operando ou ser recuperados rapidamente em caso de falhas, interrupções ou desastres.

2.1.12.Princípio do menor privilégio: Usuário deve ter apenas os acessos e permissões estritamente necessários para realizar as suas funções

2.1.13.PSI: Política de Segurança da Informação.

2.1.14.Secure By Default (Segurança por Padrão): Princípio no qual um sistema ou software já é entregue configurado com os níveis mais rígidos de segurança possíveis.

2.1.15.Secure By Design (Segurança desde a Concepção): Abordagem de engenharia de software onde os requisitos e controles de segurança são incorporados desde a fase inicial de planejamento e arquitetura da solução.

3. ABRANGÊNCIA

3.1.Esta política se aplica à Trio, abrangendo todos os sistemas, processos, informações e ativos. Seu cumprimento é obrigatório para todos os sócios, acionistas, diretores, membros do Conselho de Administração, usuários, colaboradores, colaboradores temporários, terceiros, estagiários e aprendizes, doravante chamados de “colaboradores”.

4. PRINCÍPIOS E DIRETRIZES

4.1.A PSI tem como princípios fundamentais:

4.1.1.Confidencialidade: Acesso às informações restrito apenas a pessoas autorizadas.

4.1.2.Integridade: Assegurar que as informações sejam corretas, completas e não alteradas indevidamente.

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	3

4.1.3.Disponibilidade: Garantir acesso às informações e sistemas sempre que necessário para a operação.

4.2.Para apoiar estes princípios, a Trio adota os seguintes compromissos:

4.2.1.Gestão de Ativos: Estabelecer controles para identificação, registro, classificação, utilização, monitoramento e proteção dos ativos da organização durante todo o seu ciclo de vida, visando garantir a segurança, integridade, disponibilidade e rastreabilidade das informações corporativas.

4.2.2.Proteção e Classificação da Informação: Estabelecer controles para classificação, tratamento, armazenamento, compartilhamento e proteção das informações corporativas, de acordo com seu nível de sensibilidade (pública, interna, confidencial ou restrita), conforme definido na Política de Classificação da Informação, visando garantir a confidencialidade, integridade e disponibilidade das informações da organização.

4.2.3.Gestão de Identidades e Acessos: Estabelecer controles para concessão, alteração, revisão e revogação de acessos aos ativos e sistemas corporativos, seguindo o princípio do menor privilégio e a segregação de funções, com revisões periódicas e monitoramento dos acessos, conforme definido na Política de Gestão de Identidade e Acessos.

4.2.4.Privacidade de Dados Pessoais: Estabelecer processo para tratamento de dados pessoais em conformidade com a LGPD e demais regulamentações aplicáveis.

4.2.5.Senhas e Autenticação: Utilizar credenciais seguras, vedado o compartilhamento, conforme Política de Senhas.

4.2.6.Dispositivos e Rede: Assegurar que os equipamentos, sistemas e demais ativos de tecnologia sejam utilizados e gerenciados em conformidade com os padrões de Segurança da Informação e Tecnologia da Informação, por meio da definição, implementação e manutenção de configurações seguras, bem como da aplicação contínua de mecanismos de proteção, monitoramento e controle da infraestrutura e da rede corporativa, garantindo a confidencialidade, integridade, disponibilidade e confiabilidade do ambiente tecnológico da organização.

4.2.7.Backups e Retenção: Estabelecer cópias de segurança de dados críticos, criptografadas e com períodos de retenção definidos na Política de Backup e Retenção.

4.2.8.Gestão de Incidentes: Estabelecer processos para identificação, registro, análise, tratamento e resposta a incidentes de segurança da informação, incluindo avaliação do impacto, comunicação aos reguladores, instituições autorizadas a funcionar pelo Banco Central do Brasil e titulares de dados, quando aplicável, visando reduzir impactos e assegurar a continuidade das operações da organização.

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	4

4.2.9.Gestão de Certificados Digitais: Estabelecer controles para a gestão do ciclo de vida dos certificados digitais, abrangendo emissão, renovação, armazenamento, revogação e monitoramento, com o objetivo de garantir a autenticidade, integridade e segurança das comunicações, transações e sistemas corporativos.

4.2.10.Plano de Contingência e Continuidade: Manter planos de contingência e continuidade de negócios voltados à rápida recuperação dos processos, sistemas e serviços críticos da organização. Os planos devem assegurar a capacidade de resposta a incidentes, indisponibilidades e situações de crise, estabelecendo as diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios, a fim de minimizar impactos operacionais e garantir a segurança das informações.

4.2.11.Criptografia: Assegurar a proteção de informações sensíveis por meio de mecanismos de criptografia adequados, tanto em repouso quanto em trânsito, utilizando algoritmos e protocolos reconhecidos pelo mercado. A gestão de chaves criptográficas deve ser controlada, com acesso restrito e ciclos de vida definidos.

4.2.12. Desenvolvimento Seguro:

- I. Adoção de práticas de desenvolvimento seguro ao longo de todo o ciclo de vida de sistemas, incluindo análise de requisitos de segurança e revisão de código.
- II. Devem ser seguidas diretrizes reconhecidas de mercado, como o OWASP Top 10, bem como princípios de secure by design e secure by default, assegurando que controles de segurança sejam incorporados desde a concepção das soluções.
- III. Os testes de segurança nos sistemas críticos devem ser realizados periodicamente, no mínimo anualmente. As vulnerabilidades identificadas devem ser registradas, classificadas quanto ao risco e tratadas por meio de plano de ação com prazos definidos e acompanhamento até sua resolução.

4.2.13.Prevenção e Detecção de Intrusão: Implementar mecanismos de prevenção, detecção e monitoramento contínuo de ameaças e eventos de segurança, com o objetivo de identificar, bloquear e responder rapidamente a tentativas de acesso não autorizado, comportamentos suspeitos e atividades anômalas que possam comprometer os ativos e informações da organização.

4.2.14.Prevenção de Vazamentos de Informações: Implementar mecanismos de prevenção de vazamento de informações, por meio de controles técnicos e procedimentais voltados à proteção de dados sensíveis e confidenciais, visando reduzir riscos de extração, compartilhamento, cópia, exposição indevida, perda ou acesso não autorizado às informações corporativas, de forma intencional ou acidental.

4.2.15.Proteção Contra Softwares Maliciosos: Garantir a utilização de mecanismos de proteção contra softwares maliciosos nos ativos de tecnologia da organização, com o

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	5

objetivo de reduzir riscos relacionados ao comprometimento de ativos, indisponibilidade de serviços e exposição indevida de informações corporativas.

4.2.15. Inteligência Cibernética: Realizar monitoramento contínuo de ameaças cibernéticas, com coleta e análise de informações relevantes para antecipação de riscos, identificação de tendências e apoio à tomada de decisão em segurança da informação. Devem ser utilizadas fontes confiáveis.

4.2.16. Gestão de Riscos:

- I. Estabelecer processos contínuos para identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos relacionados à segurança da informação e à tecnologia, considerando impactos operacionais, financeiros, reputacionais, regulatórios e de continuidade do negócio.
- II. Identificação, análise, avaliação e tratamento contínuo dos riscos relacionados à segurança da informação e tecnologia, considerando impactos ao negócio, financeiro, reputacional, operacional e conformidade regulatória.
- III. Os riscos identificados devem ser documentados, classificados e acompanhados por meio de planos de tratamento, definição de responsáveis e revisões periódicas, visando reduzir a exposição da organização a ameaças e vulnerabilidades que possam comprometer seus ativos e informações corporativas.

4.2.17. Avaliação e Monitoramento de Fornecedores de Tecnologia: Avaliar e monitorar fornecedores que tenham acesso a informações ou sistemas da organização, garantindo que atendam aos requisitos de segurança da informação e privacidade. Devem ser estabelecidos contratos com cláusulas específicas de segurança, confidencialidade e proteção de dados.

4.2.18. Computação em Nuvem: Adotar controles de segurança adequados no uso de serviços em nuvem, incluindo gestão de acessos, proteção de dados, monitoramento de atividades e conformidade com requisitos legais e regulatórios. Deve ser considerado o modelo de responsabilidade compartilhada entre a organização e o provedor de serviços.

4.2.19. Integração Segura de Sistemas: Assegurar que as integrações entre sistemas e serviços corporativos sejam realizadas utilizando controles de segurança adequados, visando proteger as informações trafegadas entre ambientes internos e externos.

4.2.20. Logs e Auditoria: Gerar, proteger e analisar registros de eventos relevantes, conforme Política de Gestão de Logs.

4.2.21. Cultura e Conscientização:

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	6

- I. Estabelecer ações contínuas de conscientização em segurança da informação, assegurando que colaboradores compreendam e apliquem boas práticas e suas responsabilidades na proteção das informações.
- II. Implementar programas de capacitação e de avaliação periódica de pessoal.
- III. Assegurar o comprometimento da alta administração com a promoção da cultura de segurança, gestão de riscos e melhoria contínua dos processos, controles e procedimentos relacionados à segurança da informação e à segurança cibernética.

5. DISPOSIÇÕES GERAIS

- 5.1.O descumprimento desta PSI poderá resultar em medidas disciplinares, conforme legislação e normas internas.
- 5.2.Gestores devem garantir que suas equipes estejam cientes e em conformidade com esta PSI.
- 5.3.A área de Segurança da Informação é responsável por revisar esta Política e propor atualizações.
- 5.4.A alta administração é responsável por sua aprovação.
- 5.5.Esta Política será revisada periodicamente, no mínimo uma vez ao ano, ou sempre que ocorrerem alterações significativas nos processos de TI, riscos, estrutura organizacional, mudanças legais, regulatórias ou de caráter operacional relevantes.

6. ANEXOS E CORRELAÇÕES

- 6.1. Política de Backup e Retenção
- 6.2.Política de Classificação da Informação
- 6.3.Política de Continuidade de Negócios
- 6.4.Política de Criptografia
- 6.5.Política de Desenvolvimento Seguro
- 6.6.Política de Equipamentos
- 6.7.Política de Gestão de Ativos de Informação
- 6.8.Política de Gestão de Identidade e Acessos
- 6.9. Política de Gestão de Incidentes
- 6.10.Política de Gestão de Logs e Auditoria
- 6.11.Política de Gestão de Riscos
- 6.12. Política de Gestão de Risco de Fornecedores de Tecnologia
- 6.13.Política de Gestão de Vulnerabilidades
- 6.14.Política de Governança de TI
- 6.15.Política de Inteligência Cibernética

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	7

- 6.16.Política de Privacidade
- 6.17.Política de Segurança de Redes
- 6.18.Política de Senhas
- 6.19.Política de Hardening

7. HISTÓRICO DE REVISÕES

DATA	VERSÃO	RESPONSÁVEL	DESCRIÇÃO
23/10/2025	01	Géssica Ribeiro	Elaboração do documento.
29/04/2026	02	Géssica Ribeiro	Revisão de conteúdo, adequação do padrão documental, inclusão de item regulatório, alteração dos itens referentes ao tópico de anexo e correlações.
09/06/2026	03	Géssica Ribeiro	Revisão geral do documento.

8. APROVAÇÕES

ELABORADOR	REVISOR	APROVADOR
<i>Géssica Ribeiro</i> Géssica Ribeiro Governança de TI	<i>Eurico Nicacio</i> Eurico Nicácio Cloud Ops e Segurança de TI	<i>Manoel Souza</i> Manoel Souza Tecnologia

Título	Referência	Versão	Data	Página
Política de Segurança da Informação	BRA-TEC-POL-001	03	09/06/2026	8