

Política de Segurança Cibernética

(Resumo Público)

24.04.2026



realize

SUMÁRIO

INTRODUÇÃO.....	3
DIRETRIZES.....	3
DISPOSIÇÕES FINAIS	4
DOCUMENTOS RELACIONADOS.....	5
REGULAMENTAÇÃO ASSOCIADA	5

INTRODUÇÃO

Define-se Segurança Cibernética como um conjunto de atividades para prevenção, detecção e redução das vulnerabilidades que possam materializar o risco cibernético. Tais riscos estão ligados ao vazamento de informações confidenciais, fraude interna e externa, indisponibilidade de sistemas críticos, sequestro de dados, falhas de segurança e da preservação da confidencialidade, da integridade e da indisponibilidade da informação.

A Realize SCFI reconhece por esta política que a segurança, a proteção dos dados e das informações sob sua responsabilidade são essenciais para a continuidade dos negócios, e esta empenhada em garantir todas as ações necessárias para tal.

O presente documento é um resumo da Política de Segurança Cibernética interna da Realize SCFI, em conformidade com o Artigo 5º da Resolução CMN nº 4.893 de 26/02/2021, alterada pela Resolução CMN nº 5.274 de 18/12/2025.

DIRETRIZES

As diretrizes de **Segurança Cibernética** da **Realize SCFI**, alinham-se integralmente ao comprometimento da Alta Administração e das estratégias corporativas, e às melhores práticas de mercado, regulamentações e leis vigentes. Os critérios, requisitos e demais detalhamentos relativos aos assuntos decorrentes desta política são contemplados em documentos de políticas e normas internas.

Em linhas gerais, aplicam-se as seguintes diretrizes e princípios orientadores para segurança cibernética para áreas, colaboradores, parceiros, clientes e demais partes interessadas:

- a. Deve-se preservar a Segurança Cibernética da Realize SCFI com base nos princípios de **confidencialidade**, de **integridade** e de **disponibilidade** dos dados e informações sob responsabilidade da Instituição Financeira;
- b. Manter procedimentos, tais quais, análises e testes regulares de segurança, conforme calendário interno (varreduras, testes de intrusão, simulação de incidente etc.) e controles compatíveis com o porte da Instituição para **prevenir, detectar, mitigar e monitorar** incidentes de segurança, vulnerabilidades e riscos cibernéticos;
- c. **Classificar adequadamente os dados e informações** relevantes para a operação da Instituição, conforme critérios, tais quais grau de sigilo do conteúdo, valor para o negócio, requisitos legais, sensibilidade e confidencialidade;
- d. Implementar e manter **controles de acesso lógico**, incluindo revisões periódicas dos acessos, entre outras ações, garantindo a adequação dos acessos às informações da Realize SCFI;

- e. Implementar e sustentar controles aderentes às exigências legais e regulamentares, que permitam identificar a **rastreabilidade das informações relevantes** ao longo de todo seu ciclo de vida (geração, armazenamento, processamento, transmissão e descarte);
- f. Prover mecanismos de **prevenção ao vazamento de dados e informações**, visando a detecção de violações que infrinjam os regulamentos da Realize SCFI, e assegurar o comprometimento com a proteção de dados pessoais tratados;
- g. Confeccionar o **plano de ação e de resposta a incidentes**, contemplando cenários de incidentes cibernéticos, bem como testá-lo e atualizá-lo periodicamente;
- h. Fortalecer a postura de segurança cibernética, suportando o aprimoramento da resiliência operacional e as estratégias de continuidade de negócios;
- i. Registrar e analisar **a causa e o impacto de incidentes relevantes**, aplicando correção e controles necessários, inclusive de procedimentos que envolvam informações recebidas de empresas terceiras;
- j. **Compartilhar informações sobre incidentes relevantes** com partes interessadas, como órgãos reguladores, parceiros de inteligência, áreas internas e entidades externas;
- k. Disseminar a **cultura de segurança cibernética** por meio de programa permanente de conscientização e capacitação dos profissionais envolvidos com os negócios da Realize SCFI.
- l. Prestar, via canais oficiais da Realize SCFI, informações a clientes sobre a temática de segurança cibernética e as precauções gerais relacionadas à utilização de produtos e serviços financeiros;
- m. Manter processo e metodologia de **análise crítica e avaliação de fornecedores e parceiros**, especialmente sobre os serviços relevantes ao contexto da Realize SCFI;
- n. Manter **procedimentos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem** visando a identificação de riscos cibernéticos que comprometam os princípios de segurança;
- o. Assegurar o desenvolvimento e utilização segura de sistemas de informação; e
- p. Zelar pela melhoria contínua dos procedimentos e processos de segurança cibernética.

DISPOSIÇÕES FINAIS

As violações das determinações da Política de Segurança Cibernética da Realize SCFI e seus respectivos controles associados constitui infração, passível aos responsáveis, de aplicações de medidas administrativas e judiciais/legais cabíveis. Incidentes de segurança ou desvios de conduta são registrados e avaliados, podendo resultar em sanções após análise pela áreas internas competentes.

Este documento deve ser revisado anualmente ou a cada mudança significativa em processo, tecnologia ou legislação, garantindo a melhoria contínua das práticas de segurança cibernética.

DOCUMENTOS RELACIONADOS

A Política de Segurança Cibernética da Realize SCFI é complementada por procedimentos e documentações internas específicas de segurança da informação em conformidade com aspectos legais e regulamentares.

REGULAMENTAÇÃO ASSOCIADA

- Resolução CMN 4.893/2021
- Resolução CMN 5.274/2025

REALIZE SOCIEDADE DE CRÉDITO, FINANCIAMENTO E INVESTIMENTO S.A.