

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão Pública para Fornecedores e Prestadores de Serviços

1. Introdução

No banQi, desenvolvemos soluções financeiras simples e seguras, para que você possa ter o controle do seu dinheiro direto da palma da mão e sem burocracia.

Cuidamos de você e das suas finanças e investimos todos os dias em Segurança Cibernética para que você use nossa plataforma com tranquilidade.

A segurança dos dados e informações dos nossos clientes é nossa prioridade. Conheça um pouco mais sobre a Política de Segurança Cibernética para fornecedores e prestadores de serviços, e nossas diretrizes para a sua proteção!

2. Abrangência

Esta Política aplica-se a todos os fornecedores e prestadores de serviços do banQi.

3. Enunciados

Todo fornecedor e/ou prestador de serviços do banQi deve conhecer esta política, e zelar pelo cumprimento de suas diretrizes, visando assegurar a confidencialidade, integridade e disponibilidade das informações.

Não obstante das cláusulas contratuais e das melhores práticas esperadas, fica estabelecido que o fornecedor ou prestador de serviço deve:

- I.** Notificar de forma exclusiva e imediata a área de Segurança Cibernética do banQi, em caso de suspeita ou violações aos ativos que acessem, armazenem, processem ou transmitam informações conforme diretrizes desta política.
- II.** Aderir ao processo de due diligence e avaliação e qualificação de Fornecedores em Segurança, respondendo aos questionários para mapeamento de Riscos e atendimento aos critérios e requisitos estabelecidos pelo banQi.
- III.** Apresentar as políticas, normas e procedimentos utilizados para implementação das melhores práticas de Segurança Cibernética, sempre que solicitado.
- IV.** Apresentar os planos para gerenciamento de incidentes de segurança, que contemple técnicas para detecção, prevenção e correção dos incidentes, bem como a definição dos responsáveis pelos impactos ocasionados, sempre que solicitado.

Área responsável Segurança Digital	Data da última aprovação: Nov/2023	Aprovação Diretoria Executiva	Próxima revisão: Nov/24	Versão: 2.0	Página: 1 de 3
---------------------------------------	---------------------------------------	----------------------------------	----------------------------	----------------	-------------------

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão Pública para Fornecedores e Prestadores de Serviços

- V.** Apresentar O PCN (Plano de Continuidade de Negócios), contemplando as atividades para continuidade das operações, incluindo o plano de recuperação de desastres e o resultado dos testes realizados, sempre que solicitado.

Adicionalmente aos enunciados acima, solicitamos que o fornecedor ou prestador de serviço:

- VI.** Possua políticas, normativos, procedimentos e controles tecnológicos, visando assegurar os princípios da Segurança Cibernética.
- VII.** Implemente programas de conscientização e treinamento, disseminando e engajando a cultura de Segurança Cibernética.
- VIII.** Implemente um processo formal e mecanismos automatizados para gestão de acessos, seguindo as melhores práticas do mercado.
- IX.** Comunique quaisquer dúvidas sobre a implementação dos controles de Segurança Cibernética, aos gestores banQi responsáveis pela contratação dos serviços.
- X.** Assegure procedimentos, práticas e controles para preservação da confidencialidade, integridade e disponibilidade da informação, seja de forma impressa, falada, por imagens, vídeos e qualquer outro.
- XI.** Mantenha a separação física de departamentos que atendam ao banQi, quando em locais compartilhados com diferentes áreas e/ou empresas.
- XII.** Adote mecanismos para prevenção de ameaças no ambiente cibernético, e em situação real, aplicar o plano para resposta ao incidente, realizando as ações necessárias e garantindo a comunicação imediata à equipe de Segurança Cibernética do banQi.

Visando atender as regulamentações vigentes, sendo (i) Resolução BACEN nº 85, de 8 de abril de 2021 (“Resolução BCB 85/21”), e (ii) Resolução CMN nº 4.893, de 26 de fevereiro de 2021, referente ao processo de contratação de Serviços de processamento, armazenamento de dados e de computação em nuvem, os fornecedores e prestadores de serviços devem:

- XIII.** Cumprir a legislação e regulamentação vigentes.
- XIV.** Garantir a aderência a certificações exigidas para o mercado que o Fornecedor ou Prestador de Serviço atua.

Área responsável Segurança Digital	Data da última aprovação: Nov/2023	Aprovação Diretoria Executiva	Próxima revisão: Nov/24	Versão: 2.0	Página: 2 de 3
---------------------------------------	---------------------------------------	----------------------------------	----------------------------	----------------	-------------------

POLÍTICA DE SEGURANÇA CIBERNÉTICA
Versão Pública para Fornecedores e Prestadores de Serviços

- XV.** Apresentar os dados processados e armazenados, relatórios elaborados por auditorias externas relativas à prestação do serviço, e informações para monitoramento do serviço prestado, sempre que solicitado.
- XVI.** Implementar controles de acesso voltados à proteção dos dados dos usuários finais.
- XVII.** Segregar os dados dos usuários finais por meio de controles físicos e lógicos.
- XVIII.** Implementar Controles voltados à confidencialidade, integridade, disponibilidade e a recuperação de dados e informações processadas ou armazenadas;
- XIX.** Para serviços prestados no exterior, possuir convênio firmado entre Banco Central do Brasil com as autoridades supervisoras dos demais países onde os serviços são prestados.
- XX.** Comunicar imediatamente o banQi sobre qualquer limitação que afete a prestação dos serviços ou cumprimento das regulamentações e legislações vigentes.

Área responsável Segurança Digital	Data da última aprovação: Nov/2023	Aprovação Diretoria Executiva	Próxima revisão: Nov/24	Versão: 2.0	Página: 3 de 3
---------------------------------------	---------------------------------------	----------------------------------	----------------------------	----------------	-------------------