# Política de Segurança Cibernética

**Versão Pública para Fornecedores e Prestadores de Serviços**

## 1. Introdução

No banQi, criamos soluções financeiras acessíveis e seguras, para que você tenha total controle do seu dinheiro, diretamente da palma da mão e sem burocracia.

Nosso compromisso e objetivo vai além de oferecer serviços financeiros. Cuidamos de você e das suas finanças todos os dias, investindo constantemente em Segurança Cibernética para que você possa usar nossa plataforma com tranquilidade e confiança.

A segurança dos dados e informações dos nossos clientes é uma prioridade fundamental para o banQi. Por isso, adotamos rigorosas políticas de proteção de dados para garantir a máxima segurança em todos os processos. Conheça mais sobre a Política de Segurança Cibernética, que abrange fornecedores e prestadores de serviços, além das diretrizes que seguimos para proteger suas informações em cada transação.

Este documento estabelece os princípios, valores e práticas essenciais para assegurar a confidencialidade, integridade e a disponibilidade dos dados, garantindo que todos os dados da instituição sejam tratados com o mais alto nível de segurança.

## 2. Abrangência

Esta Política Corporativa é amplamente divulgada e se aplica a todos os colaboradores, fornecedores e prestadores de serviços do banQi, em conformidade com a Resolução BCB nº 85 de 2021 e a Resolução CMN nº 4.893 de 2021 do Banco Central do Brasil. Nosso objetivo é garantir que todos os envolvidos estejam plenamente cientes das diretrizes e princípios estabelecidos, promovendo uma cultura de responsabilidade e compromisso com a segurança da informação.

## 3. Diretrizes Gerais

Todo fornecedor e prestador de serviços do banQi deve ter pleno conhecimento desta política e zelar pelo cumprimento de suas diretrizes, com o objetivo de garantir a confidencialidade, integridade e disponibilidade das informações.

Além das cláusulas contratuais e das melhores práticas esperadas, ficam estabelecidas as seguintes obrigações para fornecedores e prestadores de serviços:

I. Notificação de Suspeitas e Violações
Notificar imediatamente a área de Segurança Cibernética do banQi, de forma exclusiva, em caso de suspeita ou violação de segurança relacionada aos ativos que acessam, armazenam, processam ou transmitem informações, conforme as diretrizes desta política.

II. Processo de Due Diligence e Qualificação em Segurança
Participar do processo de due diligence e avaliação de fornecedores em segurança cibernética, respondendo aos questionários de mapeamento de Riscos e atendendo aos critérios e requisitos estabelecidos pelo banQi para garantir a conformidade com as melhores práticas de segurança.

III. Políticas e Procedimentos de Segurança
Apresentar, sempre que solicitado, as políticas, normas e procedimentos implementados para a adoção das melhores práticas de segurança cibernética, demonstrando compromisso com a proteção das informações.

IV. Plano de Gerenciamento de Incidentes de Segurança
Submeter, sempre que solicitado, os planos para gerenciamento de incidentes de segurança, que contemple técnicas para detecção, prevenção e correção dos incidentes, bem como a definição clara dos responsáveis pela gestão e mitigação dos impactos decorrentes.

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

Adicionalmente aos requisitos já mencionados, solicitamos que o fornecedor ou prestador de serviço banQi:

I. Políticas e Controles de Segurança Cibernética
Possua políticas, normativos, procedimentos e controles tecnológicos robustos, visando assegurar a aplicação dos princípios fundamentais da Segurança Cibernética em todas as suas operações.

**II.** Conscientização e Treinamento
Implemente programas eficazes de conscientização e treinamento contínuo, buscando disseminar e engajar todos os colaboradores na cultura de Segurança Cibernética, promovendo práticas seguras no uso da tecnologia.

**III.** Gestão de Acessos
Implemente um processo formal e utilize mecanismos automatizados para a gestão de acessos, incluindo a segregação de funções, determinando o mínimo necessário para o desempenho de funções , em conformidade com as melhores práticas do mercado.

**IV.** Comunicação de Dúvidas
Em caso de dúvidas sobre a implementação de controles de segurança cibernética, o fornecedor ou prestador de serviço deve comunicar imediatamente aos gestores do banQi, responsáveis pela contratação dos serviços, visando esclarecimentos.

**V.** Proteção da Informação
Assegurar a implementação de procedimentos, práticas e controles para preservação a confidencialidade, integridade e disponibilidade das informações, quaisquer seja o formato (impressa, digitais, áudio, vídeo etc).

**VI.** Separação Física de Departamentos
Quando em locais compartilhados com outras áreas ou empresas, deve garantir a separação física dos departamentos que atendam ao banQi, para proteger as informações e operações sensíveis.

**VII.** Prevenção e Respostas a Incidentes
Adotar mecanismos para prevenção de ameaças no ambiente cibernético, e em caso de incidente, aplicar o plano de resposta de forma imediata, realizando as ações necessárias para mitigar os impactos, garantindo a comunicação imediata à equipe de Segurança Cibernética do banQi.

## Conformidade Regulatória

Visando atender as regulamentações vigentes, especialmente a Resolução nº 85 de 2021 e Resolução CMN nº 4.893 de 2021 do Banco Central do Brasil, relacionadas ao processo de contratação de Serviços de processamento, armazenamento de dados e computação em nuvem, os fornecedores e prestadores de serviços devem:

**I.** Garantir o cumprimento das legislações e regulamentações vigentes, aplicáveis à segurança cibernética, proteção de dados e privacidade.

**II.** Assegurar a aderência as certificações exigidas para o mercado em que atuam, garantindo a conformidade com as normas de segurança cibernética e os requisitos de proteção de dados.

**III.** Apresentar, sempre que solicitado, os dados processados e armazenados, bem como, relatórios elaborados por auditorias externas relativas à prestação do serviço, e informações para monitoramento do serviço prestado.

**IV.** Implementar controles de acesso, visando a proteção dos dados dos usuários finais, prevenindo acessos não autorizados e garantindo a segurança das informações em todas as etapas do processo.

**V.** Segregar os dados dos usuários finais, por meio de controles físicos e lógicos, assegurando que informações sensíveis sejam protegidas adequadamente de acordo com sua criticidade.

**VI.** Implementar controles voltados à confidencialidade, integridade, disponibilidade e a recuperação de dados e informações processadas ou armazenadas.

**VII.** Para serviços prestados no exterior, garantir que exista um convênio formalizado entre o Banco Central do Brasil e as autoridades reguladoras dos demais países em que os serviços estão sendo prestados.

**VIII.** Comunicar imediatamente o banQi sobre qualquer limitação que possa impactar a prestação dos serviços ou o cumprimento das regulamentações e legislações vigentes.

## Princípios da Segurança da Informação

São princípios da Segurança da Informação:

I. Confidencialidade: Assegurar que as informações sejam acessíveis ou divulgadas exclusivamente a indivíduos, entidades ou processos autorizados, prevenindo acessos não autorizados.

II. Disponibilidade: Assegurar que as informações estejam sempre acessíveis e utilizáveis, conforme a necessidade, por indivíduos, entidades ou processos autorizados, sem interrupções ou limitações indevidas.

III. Autenticidade: Garantir que a informação seja originada de sua fonte legítima, sem alterações ou manipulações indevidas, assegurando sua origem e veracidade.

IV. Conformidade: Garantir que todos os processos da Instituição estejam em total conformidade com as regulamentações, normativas e legislações vigentes, cumprindo rigorosamente todos os protocolos e requisitos exigidos para o setor em que a organização atua.

## 4. Avaliação e Revisão da Política

Esta Política será avaliada e revisada anualmente pelas instâncias competentes do banQi, com a participação ativa das partes interessadas. O processo de revisão é fundamental para assegurar que a política continue relevante e eficaz, alinhada às melhores práticas e às necessidades em constante evolução da organização e da sociedade. A inclusão de diversas perspectivas na avaliação contribui para o aprimoramento contínuo das diretrizes, fortalecendo nosso compromisso com a transparência e a responsabilidade.

## 5. Regulamentação

- Resolução BACEN nº 85, de 8 de abril de 2021 (“Resolução BCB 85/21”)
- Resolução CMN nº 4.893, de 26 de fevereiro de 2021.