1. Introdução

No banQi, criamos soluções financeiras simples, acessíveis e seguras, para que você tenha total controle sobre seu dinheiro, diretamente da palma da sua mão e sem complicações.

Nosso compromisso vai além de fornecer serviços financeiros. Cuidamos de você e das suas finanças, e estamos sempre investindo em Segurança Cibernética para que você use nossa plataforma com confiança e tranquilidade.

O banQi implementou políticas e normas rigorosas de Segurança Cibernética para garantir o monitoramento, processamento, armazenamento, transmissão e a comunicação de informações de forma segura e protegida. Essa política busca resguardar a confidencialidade, integridade e disponibilidade dos dados, estabelecendo práticas que minimizam riscos e garantem a proteção contínua das informações de nossos clientes e parceiros.

2. Abrangência

Esta Política é amplamente disseminada e aplica-se a todos os clientes, colaboradores, terceiros, 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.

3. Diretrizes Gerais

A Política de Segurança Cibernética tem como objetivo principal assegurar a proteção das informações institucionais contra uma variedade de ameaças, com foco na redução de riscos e na maximização dos benefícios decorrentes das oportunidades de negócios. A segurança da informação é entendida pela preservação dos seguintes princípios:

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.

V. Integridade: Assegurar a precisão, completude e consistência da informação, bem como a integridade dos processos de armazenamento, transmissão e processamento de dados.

Esta política deve ser amplamente divulgada, estando disponível de forma acessível para consulta a qualquer momento, garantindo transparência e compreensão de seus objetivos.

Segurança da Informação

Consideramos como informação qualquer conjunto organizado de dados que possua valor e propósito, sendo de propriedade do banQi, que esteja sob sua custódia ou de terceiros. A Instituição deve implementar e manter a Política, fundamentada em princípios sólidos e diretrizes claras, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas de informação utilizados. A Política de Segurança Cibernética deve abranger, mas não se limitar a:

I. Proteção de Dados Sensíveis
Definimos e implementamos critérios claros para a classificação das informações com base no grau de sensibilidade, considerando o impacto potencial de seu uso indevido, divulgação não autorizada ou acesso por pessoas não autorizadas. Para garantir a proteção adequada, estabelecemos controles específicos para cada categoria de dados, com ênfase na restrição de acesso. Isso significa que apenas indivíduos com necessidade legítima terão acesso aos dados sensíveis, e com isso, as informações serão protegidas de forma rigorosa por meio de monitoramento contínuo de acessos. Além disso, a organização deve assegurar que todas as práticas estejam em conformidade com a legislação vigente e Lei Geral de Proteção de Dados (LGPD).

II. Gestão Integrada de Segurança
A gestão da Segurança Cibernética e da Segurança da Informação está alinhada diretamente aos objetivos de nossos negócios, garantindo a proteção de informações críticas ao longo de todas as operações.

III. Princípios
São princípios norteadores a preservação da confidencialidade, integridade e

disponibilidade das informações em todas as fases de seu ciclo de vida, garantindo que essas práticas sejam conduzidas de maneira ética e responsável.

IV. Controles

Preservamos que os controles e requisitos de Segurança da Informação e Cibernética sejam aplicados rigorosamente em desenvolvimentos tecnológicos, manutenções e na contratação de prestadores de serviços ou colaboradores, permanecendo vigentes durante todo o seu relacionamento.

V. Proteção de Ativos de Informação

Implementamos medidas de proteção aos ativos de informação, em conformidade com sua criticidade para as nossas atividades, abrangendo todos os processos, informatizados ou não, incluindo aqueles envolvendo o uso de computação em nuvem.

VI. Monitoramento, Detecção e Respostas de Ataques Cibernéticos

Continuamente, implementamos e monitoramos os ativos de informação e utilizamos controles, processos e tecnologias robustas para prevenção e resposta a ataques cibernéticos, bem como análise de comportamentos anômalos, minimizando riscos e danos potenciais.

VII. Classificação de Informações

Mantemos padrões e procedimentos pré-estabelecidos para a classificação das informações, considerando seus riscos e impactos, objetificando que todas as informações sejam tratadas em seu nível de relevância e sensibilidade.

VIII. Gestão de Acessos

Estabelecemos e cumprimos um processo formal de permissionamento, garantindo a gestão de acessos apenas aos usuários autorizados, conforme as melhores práticas do mercado.

IX. Tratamento de Informações

Analisamos as ocorrências de tratamento indevido de informações sob os aspectos legais e disciplinares. Nos casos devidamente comprovados de

infração, o responsável e aqueles que com ele colaborarem, terão aplicadas as sanções cabíveis.

X. Aculturamento de Segurança da Informação
Disseminamos e promovemos permanentemente a cultura de Segurança da Informação e Cibernética, por meio de programas e aptidão para sensibilização, conscientização e capacitação sobre o tema, com o objetivo de reduzir erros humanos e fortalecer a cultura de segurança dentro da organização.

XI. Gestão de Riscos
Por meio de avaliações periódicas e intervalos regulares, atuamos com um processo estruturado na Gestão de Riscos de Segurança Cibernética, que contempla a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoramento dos riscos, bem como, identificação, análise e correção de vulnerabilidades em sistemas e redes.

XII. Continuidade das Atividades
Adotamos medidas de segurança com o objetivo de garantir a continuidade das atividades do banQi, mesmo diante de possíveis incidentes de segurança cibernética, mitigando impactos.

XIII. Conformidade Regulatória e Governança
Asseguramos que a política de segurança cibernética esteja alinhada com as regulamentações pertinentes e demais Leis que possam abordar o tema.

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.