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 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 nossa Política de Segurança Cibernética ("Política") e as diretrizes.

2. Abrangência

Esta Política tem aplicação aos parceiros e prestadores de serviços que tenha acesso a informações, equipamentos, sistemas, processos e ambientes do Conglomerado banQi ("banQi"), em conformidade com a Resolução 4.893/21 e a Circular 85/21 do Banco Central do Brasil.

3. Processos de Segurança

Adotados processos internos que buscam proteger o banQi contra Riscos Cibernéticos e capacitamos nossos colaboradores para monitorar, identificar e responder a qualquer evento adverso em nossos ativos.

4. Princípios

São princípios norteadores da nossa Política a preservação da *confidencialidade, integridade, disponibilidade, e conformidade* da informação durante todo o seu ciclo de vida e dos sistemas banQi, bem como a melhoria contínua dos procedimentos relacionados à segurança cibernética.

Confidencialidade: garantir que as informações são disponibilizadas ou divulgadas apenas a indivíduos, entidades ou processos autorizados;

Integridade: garantir que as informações são precisas, completas e protegidas de alterações indevidas, intencionais ou acidentais;

Disponibilidade: garantir que as informações são acessíveis e utilizáveis sob demanda por indivíduos, entidades ou processos autorizados.

Conformidade: garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

5. Avaliação do Parceiro e do Prestador de Serviço

Na avaliação da relevância do serviço a ser contratado, o banQi considera a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

6. Plano de Resposta a Incidentes

Todos os parceiros e prestadores de serviços do banQi devem implementar plano estruturado de gestão de incidentes de segurança. O plano deve incluir, no mínimo, medidas para identificar, monitorar, comunicar e tratar incidentes, de forma a mitigar riscos e evitar a interrupção das atividades, danos ao seu funcionamento ou afetação da confidencialidade, integridade, disponibilidade e conformidade dos ativos do banQi.

7. Requisitos Gerais Para Todos Parceiros e Fornecedores

Todos os parceiros e prestadores de serviços do banQi, independentemente da criticidade da contratação, devem zelar pelo cumprimento desta Política, visando assegurar a confidencialidade, integridade e disponibilidade das informações. Portanto, os parceiros e prestadores de serviços devem implementar um programa de segurança adequado às complexidades do contrato, incluindo os procedimentos e salvaguardas abaixo:

I. Notificar, de forma imediata, a área de Segurança da Informação 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 de parceiro ou prestador de serviço, 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 da Informação, sempre que solicitado.

IV. Apresentar os planos para gerenciamento de incidentes de segurança da Informação, que contemple técnicas para detecção, prevenção e correção dos incidentes, bem como a definição dos responsáveis pelos impactos ocasionados, sempre que solicitado.

V. Apresentar 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 realizados, sempre que solicitado.

VI. Estabelecer políticas, normativos, procedimentos e controles tecnológicos, visando assegurar os princípios da Segurança da Informação.

VII. Implementar programas de conscientização e treinamento, disseminando e engajando a cultura de Segurança da Informação.

VIII. Implementar processo formal e mecanismos automatizados para gestão de acessos, seguindo as melhores práticas do mercado.

IX. Comunicar quaisquer dúvidas sobre a implementação dos controles de Segurança Cibernética, aos gestores banQi responsáveis pela contratação dos serviços.

X. Assegurar procedimentos, práticas e controles para preservação da confidencialidade, integridade, disponibilidade e conformidade da informação, seja de forma impressa, falada, por imagens, vídeos e qualquer outro.

XI. Manter a separação física de departamentos que atendam ao banQi, quando em locais compartilhados com diferentes áreas e/ou empresas.

XII. Adotar 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 da Informação do banQi.

XIII. Permitir que o banQi realize análise no seu ambiente com foco em segurança da Informação, com objetivo de confirmar se todos os requisitos de segurança previstos nesta Política e/ou no contrato estão implantados e atualizados.

8. Prestadores de Serviços de Processamento, Armazenamento de Dados e de Computação em Nuvem

Sem prejuízo das disposições gerais previstas no capítulo 7 acima, os prestadores de serviços de processamento, armazenamento de dados e de computação em nuvem devem:

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

II. Garantir a aderência a certificações exigidas para o mercado que atua.

III. 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.

IV. Implementar controles de acesso voltados à proteção dos dados dos usuários finais.

V. Segregar os dados dos usuários finais por meio de controles físicos e lógicos.

VI. Sempre que exigido na legislação em vigor, possuir convênio com o Banco Central do Brasil e/ou autoridades supervisoras dos demais países onde os serviços são prestados.

VII. Comunicar imediatamente o banQi sobre qualquer limitação que afete a prestação dos serviços ou cumprimento das regulamentações e legislações vigentes.