Política Pública de Segurança da Informação e Cibernética

Novo Banco Continental

Última Modificação: 24/11/2020

Versão: 1

segunda-feira, 5 de abril de 2021

Sumário

1. Objetivo

Estabelecer diretrizes e objetivos de segurança da informação e cibernética apropriadas ao contexto dos negócios e seus riscos, visando assegurar a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação, e em acordo com Os Princípios, Visão e Valores do Novo Banco Continental S.A. – Banco Múltiplo.

2. Público-alvo

Este documento é dirigido a todos os administradores, colaboradores, funcionários e terceiros e clientes.

3. Divulgação

Este documento pode ser encontrado em:

www.nbcbank.com.br

4. Diretrizes de Segurança da Informação

4.1. Classificação da informação

Todos os colaboradores devem seguir as diretrizes e procedimentos de classificação e proteção das informações de propriedade do NBCBank, manipuladas e armazenadas no ambiente físico e lógico existente a fim de preservar a integridade, confidencialidade e disponibilidade das informações.

4.2. Segurança de dados

As informações da instituição, dos clientes devem ser tratadas de forma ética e sigilosa, os dados devem ser utilizados de forma transparente e apenas para as finalidades para quais foram coletadas, evitando-se o mal uso e exposição indevida.

4.3. Eventos de segurança

Devem ser reportados a área de segurança da informação os riscos às informações e eventuais fatos ou ocorrências que possam colocar em risco o NBCBank, seguindo as instruções fornecidas no treinamento de Cibersegurança.

Todos os funcionários e terceiros podem registrar a suspeita de um evento de segurança da informação e cibernética através do e-mail segurançati@nbcbank.com.br. Clientes podem registrar a suspeita de um evento de segurança da Informação e cibernética através do e-mail ouvidoria@nbcbank.com.br .

4.4. Controles de segurança física

O NBCBank mantém um conjunto de políticas e boas práticas para controlar o acesso físico não autorizado, e zelar pela segurança física de suas agências, escritórios e data centers.

4.5. Uso de dispositivos móveis

Não é permitido o uso de tablets e smartphones que não forem cedidos pelo NBCBank para apoio às atividades de trabalho. O NBCBank orienta os funcionários e terceiros a utilização correta dos dispositivos móveis que devem cumprir os requisitos de segurança para seu uso dentro e fora da organização.

4.6. Segurança Lógica

A fim de coibir o uso e modificações não autorizadas em ativos digitais, recursos, aplicações nos computadores, redes e servidores a área de segurança TI mantém um conjunto de controles e práticas baseadas na confidencialidade, integridade e disponibilidade das informações.

4.7. Gestão com as áreas de negócio e tecnologia

Os projetos das áreas de negócio e tecnologia devem estar alinhados com as diretrizes e arquiteturas de segurança da informação e cibernética, garantindo a confidencialidade, integridade e disponibilidade das informações.

4.8. Controles de backup

É mantido um conjunto de diretrizes, controles e práticas para armazenagem, retenção, recuperação e eliminação de dados visando garantir a funcionalidade dos ambientes de TI, atendimento a exigências legais e de contingência.

4.9. Controles de acesso

A senha é pessoal, intransferível e deve ser mantida secreta, sendo proibido seu compartilhamento. O NBCBank mantém um conjunto de diretrizes e práticas para controle de acessos de dispositivos, tokens, sistemas internos e sistemas externos.

4.10. Utilização de Internet, rede sem fio e e-mail

O NBCBank mantém controles que visam minimizar a exposição desnecessária aos riscos e possíveis danos (perda de informação confidencial, dano à imagem da empresa, danos aos sistemas internos e externos) que possam ser causados pelo uso inadequado dos recursos de e-mail, internet e rede sem fio.

4.11. Segurança no desenvolvimento de sistemas de aplicação

O NBCBank mantém um conjunto de normas e diretrizes para garantir as boas práticas de segurança.

4.12. Computação em nuvem

O NBCBank mantém um conjunto de práticas e requisitos para a aquisição de infraestrutura, software e processamento de dados em nuvem.

4.13. Continuidade dos negócios

O NBCBank mantém diretrizes e controles que visam minimizar os impactos negativos causados por quaisquer eventos que ofereçam riscos à continuidade de negócios, bem como definição dos papéis e responsabilidades necessários à sua execução

4.14. Auditoria

O NBCBank planeja, implementa e mantém um programa de auditoria interna e externa, incluindo frequência semestral e relatórios.

4.15. Controles de riscos

Os riscos devem ser identificados pela análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação do NBCBank, considerando a implantação e a manutenção do ambiente com controles e proteções necessárias para apoiar o cumprimento dos objetivos do NBCBank.

4.16. Controles de incidentes

Medidas adotadas para reduzir os efeitos dos incidentes, bem como sua prevenção adotando clausula de sigilo e confidencialidade, proteção contra software malicioso. Políticas, procedimentos e tecnologias para minimizar riscos são constantemente implementados.

4.17. Cuidados com descarte

O NBCBank mantém diretrizes, normas e controles para o correto descarte de informações e dispositivos.

4.18. Disseminação da Cultura de Segurança da informação e cibernética.

O NBCBank promove a disseminação dos princípios e informações da segurança da informação e cibernética por meio de programas de conscientização e capacitação.