Política de Segurança da Informação e Cibernética - Brasil

Conselho Monetário Nacional - Resolução nº 4.658/2018
Instrução CVM Nº 612 de 21 de agosto de 2019

Este é um resumo das diretrizes da Política de Segurança da Informação e Cibernética - Brasil, em cumprimento à Resolução n° 4.658 / 2018 do Conselho Monetário Nacional e à Instrução CVM Nº 612 de 21 de agosto de 2019.

Versão Agosto 2020

I. Declaração da Política

O Bank of America e suas subsidiárias (doravante, "Bank of America" ou "Companhia") têm o compromisso de salvaguardar a confidencialidade, autenticidade, integridade e disponibilidade dos sistemas do Bank of America e informações, incluindo dados de clientes, funcionários, informações pessoais e de terceiros[2].

Este documento tem como objetivo informar as principais diretrizes da Política de Segurança da Informação e Cibernética do Conglomerado Prudencial Bank of America[1] ("Política"). Esta Política suporta a metodologia de riscos do Bank of America, estabelecendo os fundamentos para um programa de segurança da informação e cibernética proativo e ágil para proteger a Companhia, permitindo a implementação de medidas preventivas e detectivas para combater os riscos de segurança das informações e cibernética. A Política estabelece os requisitos para a conformidade com regulamentações e padrões da indústria, suportando as áreas de negócio, áreas de controle e auditoria corporativa para atingir objetivos estratégicos. A Política é suportada pelas normas e fundamentos que estabelecem requisitos para a realização do programa de Segurança da Informação e Cibernética do Bank of America.

A alta administração do Conglomerado Prudencial Bank of America está comprometida com a Política e com a melhoria contínua dos processos associados, tendo designado um diretor estatutário responsável pela Política e pela execução do plano de ação e respostas a incidentes cibernéticos.

[1] Conforme definido na política de governança, nos termos da resolução CMN 4.280/13, Circular CMN 3.701/14 e Carta-Circular 3.651/14 e para efeitos desta política, o Conglomerado Prudencial Bank of America ("BofA" ou a "Entidade" ou "Conglomerado Prudencial") é composto por Bank of America Merrill Lynch Banco Múltiplo S.A. ("BofAMLISA") e Merrill Lynch S.A. Corretora de Títulos e Valores Mobiliários ("MLCTVM").

[2] Como definido na política de terceiros - "Terceiro" é qualquer pessoa externa que não sejam clientes, que o Conglomerado Prudencial Bank of America se engaja no curso da realização de negócios. As partes externas que têm relacionamentos com clientes do Bank of America são tratadas como terceiros, exceto quando eles estão agindo exclusivamente no seu papel de cliente.

II. Fundamentos e Escopo

A Política define os requisitos necessários para permitir que o Conglomerado Prudencial Bank of America se prepare, previna, detecte, responda às crescentes ameaças e se recupere de eventuais crises. O programa de segurança contempla soluções e técnicas avançadas para prevenir que ameaças de segurança da informação interrompam as operações de negócios e abalem a confiança do cliente.

Como parte da infraestrutura crítica global, o Conglomerado Prudencial Bank of America atualiza sistematicamente sua Política, controles e processos operacionais em toda a Companhia. A equipe é treinada continuamente e participa dos principais fóruns de compartilhamento de informação da indústria e de organizações profissionais, buscando sempre manter um programa de segurança da informação forte e estável.

A Política abrange:

- Os objetivos de segurança da informação e cibernética da Entidade;
- Os procedimentos e controles para mitigar incidentes e atender aos demais objetivos de segurança da informação e cibernética, incluindo autenticação, criptografia, prevenção e detecção de intrusão, prevenção a vazamento de dados, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos, controle de acesso, rede de computadores segmentadas e manutenção de cópias de segurança dos dados e informações;
- Controles para garantir a rastreabilidade dos dados, a fim de proteger informações sensíveis;
- Gerenciamento de incidentes, incluindo procedimentos aplicáveis a fornecedores e comunicação tempestiva de incidentes relevantes ao BACEN e à CVM, incluindo aqueles reportados por fornecedores relevantes;
- Cenários de incidentes cibernéticos a serem considerados nos Testes e Planos de Continuidade de Negócios;
- Mecanismos de divulgação da cultura e das disposições da Política dentro da Entidade;
- Compartilhamento de informações com outras instituições financeiras;
- Diretrizes para classificação de dados/informações; e
- Os requisitos específicos para a contratação de serviços relevantes de processamento, armazenamento e computação em nuvem.

Esta Política se aplica aos sistemas de informação e ativos gerenciados internamente ou como parte de relações de terceiros. Aplica-se a todos os seus empregados, terceiros[1] e estagiários (“Usuários”) com acesso aos sistemas/dados do Bank of America e aos seus prestadores de serviços relevantes que processam/armazenam seus dados.

[1] O Terceiro é definido como qualquer pessoa física que não seja empregada do Conglomerado Prudencial Bank of America, mas foi contratada para lhe prestar serviços dentro de suas instalações, como parte do processo de execução de negócios e/ou operações bancárias.

III. Normas da Política

As normas são agrupadas em diferentes domínios que são agrupamentos lógicos dos requisitos de segurança da informação e cibernética. Os requisitos abrangem medidas preventivas, detectivas/de rastreabilidade e corretivas, voltadas à gestão do ambiente cibernético, para mitigação de potenciais ameaças/incidentes de segurança cibernética e redução de vulnerabilidades. Os principais agrupamentos são:

- Segurança da Aplicação;
- Criptografia;
- Proteção dos Dados;
- Segurança do Usuário Final;
- Gestão de Identidades e Acessos;
- Infraestrutura;
- Monitoramento, Resposta e Forense;
- Segurança de Terceiros; e
- Gerenciamento de Ameaças e Vulnerabilidades.

Os principais controles para mitigar incidentes e atender os objetivos da Política são:

- Autenticação, criptografia, controles de acesso e de segmentação da rede de computadores, segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;
- Classificação da informação;
- Prevenção e detecção de invasão e vazamento de informações;
- Realização periódica de testes e varreduras para detecção de vulnerabilidades;
- Proteção contra *softwares* maliciosos;
- Mecanismos de rastreabilidade da informação;
- Manutenção de cópias de segurança (*back-up*);
- Desenvolvimento seguro de sistemas e de implementação de tecnologias *(Secure by Design)*;
- Gestão de incidentes, plano de ação e de respostas a incidentes cibernéticos;
- Conscientização de usuários, clientes e fornecedores, contemplando iniciativas de disseminação da cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica da capacitação de colaboradores;
- Iniciativas para compartilhamento de informações sobre os incidentes relevantes com outras instituições financeiras autorizadas pelo Banco Central do Brasil ocorridos no Conglomerado Prudencial Bank of America e/ou comunicados por terceiros que prestam serviços relevantes de processamento de dados ao Conglomerado Prudencial Bank of America; e
- Elaboração de cenários de incidentes cibernéticos para a realização de testes de continuidade de negócio.

IV. Contato

O Conglomerado Prudencial Bank of America valoriza o relacionamento com os seus clientes e busca continuamente a proteção máxima de suas informações, prevenindo contra ameaças cibernéticas.

Para reportar um incidente cibernético (confirmado/materializado ou não), incluindo, mas não se limitando àqueles relacionados a um produto, aplicação, serviço ou *website*, por favor, entre em contato pelo e-mail: segurancacibernetica@bofa.com