RESUMO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Janeiro, 2025

Versão 4.0 – Documento Público

BNY

1. Introdução

O BNY desenvolveu políticas e normas de segurança cibernética, para o controle, o processamento, o armazenamento, a transferência e a comunicação de informação de forma segura.
Este documento fornece as linhas gerais da Política de Segurança Cibernética do BNY para cumprir a exigência regulatória da Resolução 4.893/2021, divulgada pelo Banco Central do Brasil

2. Objetivo

As descrições e procedimentos descritos neste resumo aplicam-se às empresas do The Bank of New York Mellon Corporation ("BNY") e suas afiliadas. Para manter a confidencialidade, a integridade e a disponibilidade das informações da empresa, todos os funcionários permanentes e temporários do BNY, e das empresas por ele controladas e os terceiros contratados (doravante referidos como "usuários") devem respeitar a Política de Segurança Cibernética e quaisquer normas e diretrizes relacionadas, bem como as diretrizes e os procedimentos desenvolvidos pela unidade de negócio na qual o usuário está alocado.

3. Políticas e Normas

A Política de Segurança Cibernética descreve o programa de segurança cibernética do BNY e as políticas e normas de apoio relacionadas. Neste âmbito, a segurança cibernética inclui as práticas e os processos para proteger a informação corporativa, incluindo a confidencialidade, a integridade e a disponibilidade dessa informação, de dano causado através de meios eletrônicos. A segurança cibernética abrange os controles que visam manter a acessibilidade e a resiliência das aplicações, dos sistemas, das redes e dos outros elementos de infraestrutura que suportam a manutenção de informação corporativa.
O programa desta Política é apoiado por um framework de governança, que inclui e não se limita, a diversas políticas e normas, cobrindo disciplinas-chave relacionadas, e também pelo programa de conscientização de segurança cibernética.

4. Resumo da Política de Segurança Cibernética

Este documento apresenta um resumo dos principais diretrizes de segurança que abordamos em nossa Política de Segurança Cibernética.

A **Governança da Segurança Cibernética** visa estabelecer os controles e processos para cumprir com a segurança cibernética, proteção de informações, privacidade, exigências regulatórias e legais, a fim de responder à cenários que envolvem ameaças cibernéticas. Os programas educacionais e de conscientização fazem parte do processo de governança do BNY .

O **Gerenciamento de Vulnerabilidades** é definido e operado para identificar, quantificar, classificar, priorizar e tratar das vulnerabilidades nos sistemas, redes ou aplicações com acesso aos dados da empresa, tanto em trânsito ou em repouso.

O **Monitoramento de Segurança e Logs** é definido e operado para identificar e responder a atividades suspeitas ou maliciosas e incidentes suspeitos ou reais no ambiente de tecnologia da empresa, as atividades atípicas detectadas são direcionadas para análise da equipe de resposta à incidentes.

A **Segurança Física e de Ambientes**, consiste em processos e controles de segurança física definidos e operados para garantir que ativos de tecnologia sejam protegidos contra acesso não autorizado, perda, dano ou roubo.

A **Proteção da Informação e Criptografia**, consiste em processos e controles de proteção de informação definidos e operados para preservar a confidencialidade, integridade, disponibilidade, e proteger contra acesso, uso, divulgação, interrupção, modificação, coleta, vazamento ou destruição de informações não autorizado.

O **Gerenciamento de Identidade e Acesso** visa garantir que os acessos sejam provisionados, aprovados, mantidos, revisados periodicamente e desativados ou removidos, em conformidade com os princípios de menor privilégio e segregação de funções. Os parâmetros de autenticação e proteção de senhas são definidos e operados para proteger contra o uso não autorizado ou acesso aos ativos de tecnologia ou informações da organização

O processo de **Resposta a Incidentes Cibernéticos** é definido e operado para identificar, analisar, gerenciar e investigar atividades suspeitas ou maliciosas e incidentes e eventos cibernéticos suspeitos ou reais. Os incidentes são gerenciados e tratados em conformidade com o programa de resposta a incidentes cibernéticos do BNY .

O **Gerenciamento de Prestadores de Serviços Terceirizados e Fornecedores** é definido e operado para garantir e verificar se prestadores e ou parcerias externas

implementem processos e controles que, no mínimo, são iguais em eficácia aos controles e processos do BNY na proteção das informações da organização, resiliência e conformidade com quaisquer exigências regulatórias.

No processo de **Segurança em Containers**, todos os riscos da arquitetura são identificados, avaliados e tratados.

O suporte ao programa de aderência ao **Segurança na Indústria de Pagamentos com Cartões (PCI-DSS)** visa garantir que os padrões de criptografia e ferramentas apropriadas sejam implementadas para proteger a confidencialidade, autenticidade e integridade dos dados em trânsito ou em repouso, assim como processos preventivos e detectivos são implementados para gerenciar o vazamento ou perda de dados.

A **Segurança em Dispositivos Móveis ou Portáteis** seguem diretrizes de configurações e proteção de dados e equipamentos, conforme determinado em políticas e procedimentos específicos para estes recursos.

Para **Ameaças Internas (Insider Threat) - Uso Indevido de Tecnologia da Informação**, o BNY possui um programa global com diretrizes e governança e conscientização na gestão de riscos relacionados a este tema.

Para **Preparação de Segurança Cibernética Centrado em Pessoas**, o BNY possui um programa global que visa garantir que treinamentos e campanhas de conscientização de segurança cibernética seja promovido a todos os colaboradores.

Para **Prevenção de Vazamento de Dados**, o BNY possui um programa dedicado ao monitoramento e proteção das informações e dados.

5. Governança e Responsabilidades

Abaixo encontram-se os indivíduos ou equipes responsáveis pela manutenção, implementação, aderência e/ou responsabilidades da Política de Segurança Cibernética no BNY.

Chief Information Officer (CIO) and Technology - responsável por desenvolver e implementar um Programa de Segurança Cibernética para as áreas que representam.

Chief Information Security Officer (CISO) – responsável pelo Programa de Segurança Cibernética em toda a empresa.

Information Security Division (Defend Platform) - área responsável pelas políticas e procedimentos e consultoria de segurança da informação do BNY, assim como auxiliar as áreas de negócios, tecnologia e parceiros no cumprimento das melhores práticas do mercado.

Áreas de Negócio – são responsáveis pelo gerenciamento de riscos associados ao uso de tecnologia e quaisquer desvios dos serviços e soluções de tecnologia e por cumprirem com os requisitos do Programa de Segurança Cibernética.

Serviços de Controles de Engenharia – responsáveis por fornecer serviços de supervisão, governança e consultoria, suporte ao gerenciamento e monitoramento de controles para Engenharia.

Controle de Políticas e Gerenciamento de Processos para Engenharia, Operações e Primeira Linha de Negócios (1LOD) - responsáveis pelas melhores práticas da indústria, tendências e consciência regulatória. Revisão, aprovações e publicações de políticas e procedimentos.

Business Information Security Officer (BISO) - É responsável por fazer uma conexão entre Segurança da Informação e as Linhas de Negócios (Não Engenharia) do BNY.

6. Aderência e Controles

O não cumprimento a Política de Segurança Cibernética poderá resultar em ações disciplinares e as exceções podem ser analisadas e concedidas conforme políticas e procedimentos internos.

7. Observações Gerais da Política de Segurança Cibernética

A Política de Segurança Cibernética poderá ser alterada sempre que necessário pelos indivíduos, equipes responsáveis ou qualquer indivíduo que identificar algum risco ou ameaça que não estejam contemplados neste documento.