RESUMO DA **POLÍTICA DE SEGURANÇA CIBERNÉTICA**

FEVEREIRO 2024

VERSÃO 4.0

BNY MELLON

1. Introdução e Propósito

O BNY Mellon desenvolveu políticas e normas de segurança cibernética, para o controle, o processamento, o armazenamento, a transmissão e a comunicação de informação de forma segura.

Este documento fornece um resumo contendo as linhas gerais da Política de Segurança Cibernética para cumprir a exigência regulatória da Resolução 4.893/2021, divulgada pelo Banco Central do Brasil

2. Aplicabilidade e Escopo

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

3. Resumo da Política de Segurança Cibernética

1. A Política de Segurança Cibernética descreve o programa de segurança cibernética do BNY Mellon 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.
2. Adicionalmente, 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.
3. O programa desta Política é apoiado por um framework de governança, que incluem e não se limita, a diversas políticas, normas e procedimentos, cobrindo disciplinas-chave relacionadas, e também pelo programa de conscientização 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 Mellon.

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 Mellon.

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 Mellon 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 - Uso indevido de tecnologia,** o BNY Mellon possui um programa global com diretrizes e governança e conscientização na gestão de riscos relacionados a este assunto.

4. Governança e Responsabilidades

O BNY Mellon conta com equipes e indivíduos responsáveis pela manutenção, implementação, aderência e/ou responsabilidades da Política de Segurança Cibernética.

Dentre eles, destacamos o CIO, CISO, Gerenciamento de Controles de Tecnologia, Governança de Operações e Tecnologia e as áreas de negócios.

5. Aderência e Controles

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

6. 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.