Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

RESUMO DAS POLÍTICAS DE PROTEÇÃO DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

3 de maio de 2019

Versão 1.0

BNY MELLON

Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

1. INTRODUÇÃO/PROPÓSITO

BNY Mellon desenvolveu políticas, normas e diretrizes abrangentes de proteção da informação e cibernética, para o controle, o processamento, o armazenamento, a transmissão e a comunicação de sua informação de forma segura.

Este documento fornece um resumo das principais políticas e normas em vigor para cumprir a exigência regulatória da Resolução 4.658, divulgada pelo Banco Cnetral do Brasil, para divulgar ao público as diretrizes gerais sobre segurança cibernética.

2. APLICABILIDADE E ESCOPO

As políticas e normas neste resumo aplicam-se às empresas do The Bank of New York Mellon Corporation ("BNY Mellon") no Brasil ("BNY Mellon Brasil" ou "empresa "). 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 as políticas de Proteção da Informação e 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 & NORMAS

A POLÍTICA DE SEGURANÇA CIBERNÉTCIA descreve o programa se segurança cibernética do BNY Mellon e as políticas e normas de apoio relacionadas.

Segurança cibernétcia 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.

Adicionalmente, segurança cibernética abrange os controles projetados para se 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 é apoiado por um framework de governança, que inclui diversas políticas e normas, cobrindo disciplinas-chave relacionadas, e também pelo programa de conscientização de segurança cibernética. A seguir segue resumo das principais políticas e normas relacionadas.

A NORMA DE PROTEÇAÕ DA INFORMAÇÃO E CIBERNÉTICA é um índice para as políticas e normas corporativas de proteção da informação e cibernétcia com controles complementares ou substitutos requeridos por exigências regulatórias do Brasil.

A POLÍTICA DE PROTEÇÃO DA INFORMAÇÃO fornece a direção para a manutenção da confidencialidade, da integridade e da disponibilidade da informação corporativa.

A política define as responsabilidades de alto nível de usuários da informação, de unidades de negócios e de grupos de apoio ao negócio sob as políticas e normas de proteção da informação do BNY Mellon a nível corporativo. A política igualmente fornece um framework para proteger pro-ativamente contra violações da segurança, destruição involuntária ou não autorizada, perda acidental, divulgação não autorizada, e alteração não autorizada intencional ou acidental de informação da empresa.

Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

Qualquer empregado do BNY Mellon que negligenciar cumprir com as disposições das políticas e normas de proteção da informação e cibernética estará sujeito à ação corretiva, podendo incluir até o término do emprego, e, quando apropriado, processo criminal, ou civil sob as leis aplicáveis. Todos os empregados são responsáveis por proteger toda a informação não-pública de maneira apropriada. A informação de cliente pessoa física e de cliente institucional deve ser usada somente para as finalidades autorizadas pela administração. Qualquer pessoa acessando informações de cliente é proibida de fazer uso pessoal de tal informação ou de fornecê-la a terceiros não autorizados.

A política da proteção de informação é apoiada por um número de políticas, normas e diretrizies - emitidas a nível corporativo, assim como de unidade de negócios ou geopolítico - que detalha as exigências para proteger informação corporativa do BNY Mellon e de seus clientes.

Qualquer exceção às políticas e normas de proteção da informação e cibernética deve ser aprovada por um nível de gerência considerada apropriada pela alta administração da unidade de negócio que solicita a exceção. As exceções que representam o risco significativo para a empresa devem ser apresentadas ao Comitê de Risco de Informação e Tecnologia ou a membros apropriados desse comitê. A aceitação do risco deve ser apropriadamente documentada e as aprovações exigidas devem ser obtidas antes da implementação do processo para o qual a exceção foi solicitada.

A POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO exige que toda a informação sob a custódia do BNY Mellon, incluindo dados de fornecedor e de cliente, receba classificações específicas que são usadas para determinar as exigências para controle de acesso, criptografia, processos de negócios e de manuseio de dados.

A política exige a classificação da informação como Altamente Confidencial, Confidencial, Para Uso Interno Apenas e Pública.

A política da classificação da informação é apoiada pelas seguintes normas que especificam controles do BNY Mellon para informação custodiada pela empresa:

– **Classificação e Manuseio da Informação**, que estabelece os controles mínimos para corretamente classificar e manusear a informação possuída ou custodiada pelo BNY Mellon.

– **Transporte e Armazenamento de Mídia Física**, que estabelece os controles mínimos para armazenar e transportar mídias físicas de forma segura a fim proteger a informação armazenada nas mesmas.

– **Eliminação e Destruição de Informação**, que estabelece controles para assegurar que, no fim do período de retenção atribuído, a informação possuída ou custodiada pelo BNY Mellon que seja classificada como Altamente Confidencial, Confidencial ou Para Uso Interno Apenas seja devidamente apagada e/ou que o equipamento/mídia associado seja destruído.

POLÍTICA DE PRIVACIDADE DA INFORMAÇÃO, que estabelece os princípios chave que devem ser seguidos para proteger a privacidade de clientes, empregados e outros indivíduos de acordo com exigências legais e regulatórias de privacidade.

POLÍTICA DE GERENCIAMENTO DE IDENTIDADE E ACESSO, que define as exigências para a concessão de acesso aos ativos de informação da empresa.

A política cobre a identificação, a autenticação, a autorização e a re-certificação periódica de usuários da informação. A política também estabelece exigências mínimas para níveis elevados de privilégios para acessar ativos de informação do BNY Mellon. A política aplica-se a acesso às redes, aplicações (que incluem aquelas hospedadas por provedores de serviços de aplicativo), sistemas operacionais, bancos de dados, dispositivos

Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

de computação portáteis e tecnologias desenvolvidas por usuário (User Developed Technologies - UDTs) da empresa. A seguir, resumo dos requerimentos da política:

– O acesso aos ativos de informação deve ser restringido a usuários autorizados e/ou aos processos de sistema que tenha uma necessidade de usar os ativos. Os usuários devem acessar somente dados aos quais tiveram acesso explicitamente concedidos.
– Os direitos de acesso devem ser periodicamente revistos com base no nível de risco relacionado e devem ser revogados e/ou desabilitados quando são forem mais necessários.
– Intencionalmente acessar, ver, alterar ou apagar recursos sem autorização é proibido.
– A concessão de privilégios de acesso deve assegurar a segregação básica de funções.
– Os pedidos do acesso não devem ser submetidos e aprovados pelo mesmo indivíduo para o seu próprio identificador de usuário nem para nenhum identificador de sistema para o qual o indivíduo é o responsável.

Controles operacionais relativos à Política de Gerencimanento de Identidade e Acesso podem ser encontrados nas seguintes normas corporativas de apoio:

– **Controle de Acesso**, que define os controles mínimos para a identificação e a autenticação dos usuários nos sistemas informáticos que guardam informação que pertence ao BNY Mellon ou seus clientes. Esta norma exige que senhas de usuário cumpram com exigências mínimas da composição.

– **Autorização e Certificação**, que requer gerenciamento de direitos de acesso através de um processo formal ao longo de seu ciclo de vida desde a solicitação original até a sua revogação. O uso dos direitos de acesso deve ser revisto e certificado periodicamente de acordo com sua criticidade para o negócio. A frequência da recertificação é baseada no nível de risco do ativo para o qual o acesso foi concedido.

– A**dministração de Usuário com Privilégios**, que descreve os controles exigidos pelo BNY Mellon para conceder, alterar, revogar e certificar acesso aos ativos de informação da empresa para usuários com níveis elevados de privilégios ou acesso de sistema para controlar eficazmente o alto risco de uso indevido de tais privilégios ou acesso.

– **Norma de Definição de Acesso Privilegiado**, que fornece a definição de acesso privilegiado.

– **Norma de Controle e Administração de Acesso Privilegiado**, que descreve os controles necessários para o BNY Mellon endereçar o risco associado com a criação, a emissão e o uso das credenciais com permissões de acesso privilegiado.

A POLÍTICA DE COMUNICAÇÃO ELETRÔNICA, que estabelece as exigências da empresa para manter a segurança, a privacidade e a confidencialidade de informação do BNY Mellon quando comunicada eletronicamente.

A política delinea o uso apropriado e responsável dos recursos de comunicação eletrônica da empresa os quais incluem correio eletrônico, mensagens instantâneas, Internet e rede. Segue resumo da política:

Os recursos de uma comunicação eletrônica de BNY Mellon devem ser usados prioritariamente para fins de negócios. As mensagens transmitidas através destes recursos são de propriedade do BNY Mellon independetemente de sua forma. Os usuários não devem ter nenhuma expectativa da privacidade no que diz respeito a suas atividades na Internet ou em nenhum recurso de comunicação eletrônica do BNY Mellon.

A empresa se reserva o direito de monitorar o uso de facilidades de comunicação eletrônica. A informação associada com o uso não autorizado ou atividades ilegais coletada em consequência de monitoramento pode ser fornecida a autoridades compententes, e informação associada com conduta inapprioriada, incluindo

Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

comunicações incompatíveis com as políticas,normas e proceidmentos da empresa, pode formar a base de ação disciplinar, que pode incluir até a recisão do emprego.

Coletar, ou tentar coletar, informações pessoais a respeito de terceiros sem seu conhecimento é proibido.

Todos dados armazenados em dispositivos de computação pessoal e o equipamento da empresa (que inclui estações de trabalho, computadores pessoais, dispositivos sem fios e dispositivos portáteis de armazenamento de dados) são de propriedade da empresa.

A informação Altamente Confidencial não deve ser transmitida em texto claro através da Internet ou de outra rede aberta não confiável a partir de um dispositivo da computação pessoal.

A política inclui uma lista de usos proibidos de ativos de informação do BNY Mellon. Tais usos incluem a postagem de conteúdo ofensivo, violações de leis de direitos autorais e de licenciamento de software e “spam”.

A Política de Comunicação Eletrônica é apoiada pelas seguintes normas que documentam os relacionados controles da empresa:

– **Uso da Internet**, que especifica os controles mínimos exigidos para o acesso e o uso da Internet através da infraestrutura de rede do BNY Mellon e dos recursos eletrônicos disponibilizados pela empresa.

– **Dispositivos Portáteis de Computação**, que estabelce os controles mínimos para o uso e a proteção da informação do BNY Mellon em dispositivos de computação portáteis conforme definido na norma.

A POLÍTICA DE OPERAÇÕES DE USUÁRIO FINAL define requerimentos para proteger a informação do BNY Mellon manuseadas pelos prestadores de serviços da empresa, por Tecnologia Desenvolvida por Usuário e acessível nas mesas e nos espaços de trabalho dos usuários na condução do negócio.

A política de Operações de Usuário Final é apoiada pelas seguintes normas que listam os controles exigidos sob a política:

– Tecnologia Desenvolvida por Usuário, que define tecnologias desenvolvidas usuário (UDTs), fornece os critérios para determinar as UDTs cobertas por esta norma e prescreve os controles de processo de desenvolvimento e de tecnologia exigidos.

– **Mesa Limpa**, que exige usuários de informação do BNY Mellon protejam informação sensível, formatos físico e eletrônico, a todo momento.

– **Reporte de Incidente da Segurança da Informação**, que estebelece controles mínimos para o reporte oportuno de incidentes da segurança da informação conforme definido na norma.

A POLÍTICA DE OPERAÇÕES DE TECNOLOGIA DA INFORMAÇÃO documenta os requerimentos da empresa para a proteção de ativos de informação de BNY Mellon contra ameaças internas e externas, intencionais ou acidentais, com os objetivos de assegurar a continuidade do negócio e de minimizar o impacto de violações de segurança. Essa política é apoiada pelas seguintes normas que documentam os controles mínimos exigidos pela política:

– **Segurança de Rede**, que define as exigências mínimas do controle para serviços e dispositivos de rede, incluindo firewalls , roteadores, servidores proxy e serviços de comunicação de dados, visando proteger adequadamente os sistemas informáticos e canais de comunicação do BNY Mellon.

Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

– **Firewall de Rede**, que define os requerimentos mínimos de controle de segurança para implementar e manter firewalls de rede do BNY Mellon.

– **Anti-vírus**, que descreve os controles da empresa para prevenir, conter a introdução de, e mitigar o impacto de software malicioso na rede do BNY Mellon, em aplicações e em outros sistemas que poderiam impactar a confidencialidade, a integridade ou a disponibilidade da informação.

– **Monitoramento e Registro de Proteção da Informação**, que descreve os controles para o registro e a o monitoramento eficazes de eventos e de circunstâncias relativos à segurança para fins de atividades investigativas e de audotoria.

– **Resposta a Incidente da Segurança da Informação**, que estebelece a abordagem do BNY Mellon apra responder aos incidentes cibernéticos e de segurança da informação, e descreve os papéis das partes interessadas do BNY Mellon na resposta a tais incidentes.

– **Computação em Nuvem**, que requer que ambientes de Computação em Nuvem estejam em conformidade com às políticas, normas e proceidmentos de proteção da informação do BNY Mellon, para o desenvolvimento e implementação da infraestrutura, da plataforma e dos serviços criados para dar suporte à arquitetura, ao software, e aos dispositivos de computação distribuídos em tais ambientes.

– **Acesso Remoto**, que descreve os controles de proteção da informação exigidos para prover acesso remoto seguro, quando autorizado, a empregados e prestadores de serviço, a ativos de informação do BNY Mellon.

POLÍTICA DE RISCO DE TENCOLOGIA DE PRESTADOR DE SERVIÇO determina requerimentos para o gerenciamento dos riscos de informação e tencologia associados com a contratação de prestadores de serviço para o BNY Mellon durante todo seu ciclo de vida.

POLÍTICA DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO, define os controles da proteção de informação projetados para assegurar a disponibilidade do ambiente da tecnologia da informação do BNY Mellon, mantendo a confidencialidade da informação sensível da empresa. Esta política também documenta os requerimentos da empresa para a proteção de ativos de informação do BNY Mellon contra ameaças, intencionais ou acidentais, com os objetivos de assegurar a continuidade do negócio e de minimizar o impacto das violações da segurança. Ela é apoiada pelas seguintes normas:

– **Criptografia**, que determina os requerimentos para o uso de criptografia para proteger os ativos de informação que contêm, processam ou transmitem informação Altamente Confidencial. A informação classificada de outra forma que não Altamente Confidencial pode requerer criptografia quando em repouso ou em trânsito se o proprietário dos dados determinar nível reforçado de proteção contra risco de exposição.

– **Gestão de Vulnerabilidade**, que estabelece os controles mínimos para o programa do BNY Mellon de gerenciamento de vulnerabilidade. Os controles abrandam riscos resultantes de vulnerabilidades de configuração de aplicações, nas redes e sistemas operacionais. BNY Mellon segue uma aboardagem baseada em risco para aplicação de patches e remediação de vulnerabilidades.

– **Ciclo de vida de Desenvolvimento de Sistema & Ciclo de Vida de Infraestrutura**, que estabelece as exigências mínimas de controle para aqusição de software ou hardware, e o desenvolvimento e a manutenção de ativos de informação, para assegurar-se de que eles operam de um modo que protege a confidencialidade, a integridade e a disponibilidade dos ambientes técnicos da empresa.

Avenida Presidente Wilson, 231
11° andar
20030-905 Rio de janeiro- RJ

A POLÍTICA DE GERENCIAMENTO DE MUDANÇAS estabelece as exigências para os domínios associados com a gestão de mudanças da empresa e assegura-se de que eles operam de um modo que protege a confidencialidade e a integridade da informação do BNY Mellon e a resiliência dos ambientes técnicos da empresa. É apoiada pelos seguintes padrões:

– **Gerenciamento de Configuração**, que estabelece os controles mínimos para o processo de gerenciamento de configuração do BNY Mellon para definir, documentar e manter especificações sobre como os ativos de informação são instalados, configurados, conectados e operados.

– **Gerenciamento de Mudanças de Tecnologia da Informação (TI)**, que estabelece os controles mínimos para mudanças da tecnologia da informação, o que inclui a definição de exigências para a revisão, a aprovação e a liberação de mudanças de TI em produção.

NORMA DE SUPERVISÃO DE QUALIDADE E CONSULTIVA define os critérios a serem usados para identificar as aplicações e a infraestrutura do BNY Mellon que são escopo para a avaliação de riscos de tecnologia e da informação, e delinea o procesos padronizado de avaliação de risco da segunda linha de defesa e de supervisão de mitigação de risco baseada na avaliação e na resposta aos resultados de avaliação de risco.

NORMA DE PROCESSO DE EXCEÇÃO DE RISCO DE TECNOLOGIA documenta os processos para solicitar, revisar e aprovar/rejeitar exceções às políticas e normas de proteção da informação e cibernética.