P.P27.001.02

Política Segurança Cibernética

1. OBJETIVO

A Mirae Asset Wealth Management (Brazil) CCTVM Ltda. ("Mirae Asset") estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

• Proteger o valor e a reputação da empresa;

• Garantir a confidencialidade, integridade e disponibilidade das informações da Mirae Asset e de informações de terceiro por ela custodiada, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

• Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

• Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

• Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

• Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias; e

• Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

2. CONCEITOS

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos:

Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares:

- **Vírus:** software que causa danos a máquina, rede, softwares e banco de dados;

• **Cavalo de Troia:** aparece dentro de outro software e cria uma porta para a invasão do computador;

• **Spyware:** software malicioso para coletar e monitorar o uso de informações;

• **Ransomware:** software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia Social:

• Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

• **Phishing:** links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

• **Vishing:** simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

• **Smishing:** simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

• **Acesso pessoal:** pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

3. PRINCÍPIO

A proteção e privacidade de dados dos clientes refletem os valores da Mirae Asset e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados; e

- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

4. DIRETRIZES

O cumprimento da Política Corporativa de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

4.1 Controle de Segurança Cibernética

Os controles de segurança cibernética, devem estar alinhados e acordados entre a estrutura da organização, porém a sua execução deverá ser garantida pela área de Tecnologia da Informação:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada, com ferramenta segura de backup e criptografia, conforme a necessidade;

- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;

- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Mirae Asset;

- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;

- Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores dos sistemas/redes, filtros de spam, controle para uso de periféricos, soluções de prevenção e correções de vulnerabilidades e filtros de uso de internet;

- Garantir a continuidade do processamento das informações críticas de negócios;

- Atender às leis que regulamentam as atividades da Mirae Asset e seu mercado de atuação;

- Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acesso;

- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo; e

- Comunicar imediatamente à área de Segurança Cibernética, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

4.2 Teste de Controle

A efetividade da política de segurança cibernética deve ser verificada por meio de testes e revisões periódicas dos controles existentes. O plano de teste deve ser executado pela área de Tecnologia da Informação assegurando que:

- Os acessos dos colaboradores estão em conformidade com os acessos as áreas de atuação;

- Que os níveis de confidencialidade e acessos as informações confidenciais estão adequadas;

- Recursos computacionais de controle de acesso físico e lógico, estejam protegidos; e

- Que haja rastreabilidade de registros que permitam a realização de auditorias periódicas.

5. ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política Corporativa de Segurança.

5.1 Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

5.2 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

O acesso como administrador aos sistemas em nuvem de ambientes produtivos ou que possuam ativos críticos do qual fazem gestão de infraestruturas, plataformas e softwares/funções, como serviço, devem ser restritos aos administradores da Nuvem. Qualquer tipo de exceção deverá ser previamente autorizado pela equipe de Segurança da Informação.

5.2.1 Acesso Físico

O acesso físico às dependências da Mirae Asset é determinado por faixas de horários e dias da semana. É concedido conforme cargo e função do colaborador. Em algumas ocasiões, exceções são feitas pelos gestores e o acesso é concedido através do registro e aprovação pelas áreas de Compliance e Segurança da Informação.

5.3 Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros da Mirae Asset são treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa efetivo de conscientização realizada pela área de Segurança da Informação.

5.4 Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

5.5 Processamento, Armazenamento de dados e Computação em Nuvem

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a Mirae Asset deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar que:

• A adoção de serviços hospedados em nuvem privada, pública, híbrida ou em ambiente de parceiros e/ou fornecedores, respeitam sempre a premissa da confidencialidade, integridade e disponibilidades das informações;

• Os serviços devem respeitar a legislação e localidades, que estejam dentro dos acordos estabelecidos pelas autarquias responsáveis pela regulação e fiscalização de nosso mercado e atuação;

• O acesso pela Mirae Asset aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

• O acesso pela Mirae Asset aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

• A identificação e a segregação dos dados dos usuários finais da Mirae Asset por meio de controles físicos ou lógicos; e

• A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da Mirae Asset.

Na avaliação da relevância do serviço a ser contratado, a Mirae Asset também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

5.5.1 Contratação de prestação de serviços

A Mirae Asset deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem contemplem:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;

- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;

- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;

- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à Mirae Asset, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

- O acesso da Mirae Asset às informações fornecidas pela empresa contratada bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

- A obrigação da empresa contratada notificar a Mirae Asset sobre a subcontratação de serviços relevantes para a Mirae Asset;

- A permissão de acesso do Banco Central do Brasil aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;

- A adoção de medidas pela Mirae Asset, em decorrência de determinação do Banco Central do Brasil;

- A obrigação de a empresa contratada manter a Mirae Asset permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Em caso de decretação de regime de resolução da Mirae Asset pelo Banco central do Brasil, o contrato de prestação de serviços deve prever:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;

- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços.

A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:

• A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

• A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da Mirae Asset.

5.5.1.1 Comunicação ao Banco Central do Brasil

A comunicação ao Banco Central do Brasil deve conter as seguintes informações:

- A denominação da empresa a ser contratada;

- Os serviços relevantes a serem contratados;

- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é do mínimo 60 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Banco Central do Brasil, deverá ocorrer em até 60 dias contados da alteração contratual.

6. CLASSIFICAÇÃO DOS DADOS E DAS INFORMAÇÕES

A Mirae Asset estabelece o compromisso com o tratamento adequado das informações de seus clientes, visando:

- **Confidencialidade:** garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;

- **Disponibilidade**: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário; e

• **Integridade:** garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

6.1 Níveis de Confidencialidade

Os dados e as informações devem ser classificados de acordo com a sua criticidade, com três níveis de confidencialidade: confidencial, uso interno e pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, compartilhamento ou restrição de acessos, bem como os impactos no caso de utilização indevida dos dados e das informações.

• **Confidencial:** informação sigilosa, de caráter estratégica, restrita a diretoria ou a quem for designado por esta;

• **Uso interno**: informação destinada para uso exclusivo da Mirae Asset; e

• **Pública**: informação destinada para o público em geral.

6.2 Avaliação de relevância do incidente

Os incidentes são classificados da seguinte forma:

Crítica: Todo e qualquer incidente que possa comprometer a imagem da instituição e dados confidenciais dos seus clientes.

Alta: Todo e qualquer incidente que possa comprometer a disponibilidade de serviços e sistemas relevantes da organização, ou seja, aqueles que afetam o processamento de Custódia, Liquidações e Ordem.

Média: Todo e qualquer incidente relacionado a tentativas de acessos não autorizados e qualquer incidente que possa comprometer a disponibilidade de serviços e sistemas da organização não relevantes.

Baixa: Incidentes relacionados ao compartilhamento de informações não relevantes.

7. PLANO DE RESPOSTA A INCIDENTE

A Mirae Asset deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios ("Plano"), considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave).

Os colaboradores poderão reportar incidentes diretamente ao Responsável pela Segurança Cibernética ou por meio do canal de reporte de incidentes:

it.ctvm@miraeinvest.com.br

Os incidentes reportados serão classificados segundo o risco que representam para a Mirae Asset e o impacto na continuidade dos negócios da Mirae Asset. Além disso, devem ser devidamente registrados, tratados e comunicados.

A Mirae Asset adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

Para efeito desta política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação de uma ameaça que

explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação.

7.1. Procedimento em Caso de Incidente

Toda ocorrência, bem como as informações recebidas de terceiros, deverá ser avaliada pela equipe de tecnologia da informação para a determinação da criticidade e impacto causados nas operações.

Uma vez que a equipe de tecnologia da informação tenha sido acionada devido a um potencial incidente, este deverá convocar Comitê de Segurança Cibernética.

7.1.1 Avaliação Inicial

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

7.1.2 Incidente Caracterizado

Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à órgãos reguladores e autorreguladores (ii) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial a Investidor que tenha sido afetado; e (iv) houve prejuízo para a Mirae Asset, algum veículo de investimento ou investidor específico. Além disso, o Comitê, em conjunto com eventual

consultor, deverá definir os passos a serem tomados sob o aspecto de cibe segurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telefonia a desviar linhas de dados/e-mail.

7.1.3 Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a Mirae Asset adota iniciativas para o compartilhamento de informações sobre incidentes relevantes com os integrantes do sistema financeiro nacional por meio dos canais adotados por elas.

A Mirae Asset efetuará também comunicação tempestiva aos órgãos reguladores das ocorrências de incidentes classificados com relevância crítica e alta e de interrupções de serviços relevantes que configurem uma situação de crise, bem como as providências adotadas para o reinício dessas atividades.

7.1.4. Plano de ação e resposta a incidentes

A Mirae Asset irá estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;

- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

Além disso, são elaborados cenários de incidentes considerados nos testes de continuidade de negócios. Adicionalmente, será requerida a

classificação dos dados e as informações quanto à relevância, conforme critérios estabelecidos.

O Plano de Ação ainda deverá prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.

7.1.5 Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um call diário ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pelo Comitê, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos.

Também deverá avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, enquanto o Diretor responsável verificará se todas as informações necessárias da Mirae Asset estão seguras. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Corretora, devem ser comunicados ao Comitê. Colaboradores externos relevantes deverão ser mantidos atualizados.

O serviço será considerado como reestabelecido após o incidente tenha sido tratado de forma definitiva.

7.1.6 Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de Compliance deverá registrar o histórico em local adequado, como o sistema de gerenciamento.

7.1.7 Plano de ação e resposta a incidentes

A Mirae Asset deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política; e

- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

7.1.8 Relatório Anual

A área de Segurança da Informação deverá elaborar relatório anual sobre os processos realizados conforme a Resolução 4.658/18, considerando os seguintes itens:

- A efetividade da implementação das ações desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

- O resumo dos resultados obtido na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes, em

conformidade com as diretrizes da política de segurança cibernética;

• Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

• Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O Relatório deverá ser submetido aos diretores da instituição até 31 de Março do ano seguinte ao da data-base.

8. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

A Mirae Asset promove a disseminação dos princípios e diretrizes de segurança cibernética através de programas de conscientização e treinamentos específicos, visando o fortalecimento da cultura interna de gestão de segurança da informação.

A Mirae Asset promoverá também a ampla divulgação desta Política ao público em geral, bem como às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

9. RESPONSABILIDADE

A Alta Administração da Mirae Asset se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os

quais devem ser objetos de pautas recorrentes em reuniões internas da empresa.

10. COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail it.ctvm@miraeinvest.com.br

11. HISTÓRICO DE VERSÕES

Versão	Motivo	Data	Autor	Departamento
P.P27.001.01	Elaboração Política	27/02/2019	Ricardo Aizawa	Compliance
P.P27.001.02	Revisão periódica	01/12/2020	Ricardo Aizawa	Compliance