

# MSK GESTÃO DE RECURSOS LTDA.

## Política de *Compliance*, Controles Internos e Segregação de Atividades

Versão	Data de Atualização
1ª	Julho/2020

## SUMÁRIO

1. Introdução .....	3
2. Abrangência.....	3
3. Estrutura de Compliance.....	3
3.1. Departamento de Risco e Compliance .....	3
4. Controles Internos.....	4
4.1. Procedimentos da MSK Asset.....	5
4.2. Reportes Regulatórios.....	6
5. Incidentes de Segurança .....	6
6. Segregação de Atividades .....	6
6.1. Segregação de Atividades entre a MSK Asset e MSK Invest .....	7
7. Treinamento.....	8
8. Política de Certificação .....	8
9. Plano de Continuidade de Negócios .....	8
10. Política Cibernética.....	10
11. Revisão da Política.....	12

## 1. Introdução

A presente Política de *Compliance*, Controles Internos e Segregação de Atividades (“Política”) tem como objetivo estabelecer os conceitos, regras e procedimentos dos controles internos da **MSK Gestão de Recursos LTDA** (“MSK Asset”) na condução de suas atividades inerentes à administração de carteiras de valores mobiliários, conforme estabelecido pela Instrução da Comissão de Valores Mobiliários (“CVM”) nº 558, de 26 de março de 2015 (“Instrução CVM 558”), pelo Código de Melhores Práticas para Administração de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais (“ANBIMA”) (“Código ANBIMA”), e demais regulamentações aplicáveis. A MSK Asset busca, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, bem como a elevados padrões éticos e profissionais.

A Política apresentada poderá ser atualizada e complementada, e é de responsabilidade de todos os Colaboradores (conforme abaixo definido) conhecer e cumprir todas as obrigações legais e regulatórias em suas atividades, prezando por altos padrões de conduta profissional. Também é obrigação de todos os Colaboradores notificar o Departamento de Risco e Compliance em casos de condutas indevidas sob o ponto de vista legal, ético ou regulatório.

## 2. Abrangência

Esta Política aplica-se a todos os colaboradores da MSK Asset, incluindo sócios, administradores, diretores, funcionários, estagiários, consultores e colaboradores temporários (“Colaboradores”) que deverão compreender o seu conteúdo e aderir formalmente à presente Política por meio da assinatura do “Termo de Compromisso” anexo ao Código de Ética e Conduta da MSK Asset.

## 3. Estrutura de Compliance

A MSK Asset possui estrutura capaz de garantir (i) o controle de informações confidenciais; (ii) a execução de testes periódicos de sistema de informações e; (iii) a implantação de treinamentos a todos os seu Colaboradores que possuem acesso a informações sigilosas, que participam no processo de decisão de investimentos.

### 3.1. Departamento de Risco e Compliance

O Departamento de Risco e Compliance é independente e não está subordinado a nenhum outro departamento da MSK Asset. O referido departamento é liderado pelo Diretor responsável, perante a CVM, designado no contrato social possuindo comunicação direta para a divulgação dos resultados decorrentes das atividades de *compliance* incluindo irregularidades ou falhas identificadas.

Entre as atividades aplicáveis ao Departamento de Risco e Compliance da MSK Asset, estão as seguintes:

- (i) administração da presente Política;

- (ii) verificação da correta aderência dos Colaboradores às políticas e códigos;
- (iii) atualização em relação às legislações em vigor e realização de testes periódicos dos processos e controles internos, efetuando as correções de quaisquer falhas detectadas; e
- (iv) oferecimento de suporte às outras áreas da MSK Asset para esclarecer eventuais dúvidas sobre as políticas, manuais e regulamentos internos.

O Departamento de Risco e Compliance possui autonomia e autoridade para questionar os riscos assumidos nas operações realizadas pela mesa de operações.

Além disso, em atendimento ao artigo 22 da Instrução CVM 558, caberá ao Departamento de Risco e *Compliance* elaborar o “Relatório de Compliance e Controles Internos”, até o último dia útil de abril, mantendo-o à disposição da CVM, arquivado na sede da MSK Asset. O Relatório de Compliance e Controles Internos faz referência às operações do ano anterior ao de sua elaboração e contém: (a) os resultados dos testes periódicos de controle e aderência executados; (b) recomendações para solucionar quaisquer deficiências e cronograma de plano relevante para solucioná-las; e (c) comentários do responsável pelas atividades de gestão de ativos perante a CVM com relação a essas deficiências ou quaisquer deficiências encontradas em verificações anteriores, se houver, bem como o plano de solução do problema ou as atuais medidas tomadas para resolver tais deficiências de acordo com o cronograma de plano estabelecido para tal propósito.

#### **4. Controles Internos**

O Departamento de Risco e Compliance é responsável pela execução dos testes de procedimentos relativos a controles internos a fim de garantir o cumprimento das regras, procedimentos e controles internos a que se refere esta Política e, conseqüentemente, deverá elaborar, em conjunto com as demais áreas aplicáveis, os planos de ação necessários a falhas de execução identificadas nos processos ou controles. Ao mesmo tempo, o Departamento de Risco e Compliance deve mitigar as ocorrências de ilícitos ou atividades contrárias à regulação.

A MSK Asset possui controles internos adequados para garantir o permanente atendimento às normas e regulamentações vigentes aplicáveis às atividades por ela desempenhadas, de forma a:

- (i) Estabelecer o conceito de controles internos através do estabelecimento de cultura de Compliance, visando melhoria nos controles;
- (ii) Realizar os reportes regulatórios periódicos exigidos pela Instrução CVM 558 e demais regulamentações aplicáveis;
- (iii) Assegurar que todos os Colaboradores atuem com imparcialidade e conheçam as Políticas Locais, Políticas Globais e normas aplicáveis às atividades desempenhadas;
- (iv) Apoiar as áreas de 1ª linha de defesa no processo de gestão dos riscos operacionais com o desenvolvimento de processos, métodos, ferramentas e Políticas Locais;
- (v) Efetuar testes de aderência às Políticas Locais e Políticas Globais e mapeamento dos processos relevantes com foco na eficiência operacional, identificando vulnerabilidade nas normas e processos de controle, para atualização da matriz de riscos e controles; e

(vi) Identificar, administrar e eliminar eventuais conflitos de interesses que possam afetar a imparcialidade dos Colaboradores que desempenhem funções ligadas à administração de carteiras de valores mobiliários.

#### 4.1. Procedimentos da MSK Asset

A supervisão dos Colaboradores que desempenham funções relacionadas à administração de carteiras de valores mobiliários ainda inclui a observância de que atuem com imparcialidade evitando qualquer potencial conflito de interesse. O Diretor de Risco e Compliance pode a qualquer momento requisitar a estação de trabalho de um Colaborador com o propósito de efetuar exames e análises quando houver suspeitas de descumprimento dos regulamentos internos ou atividades ilegais. A solicitação do computador é válida apenas com a finalidade de averiguar a correta observância das normas internas e utilização adequada dos recursos disponibilizados pela MSK Asset, devendo o Diretor de Risco e Compliance evitar qualquer exame que fira as regras e leis trabalhistas. Cada colaborador possui acesso eletrônico ao servidor apenas no que se referem às pastas e aos arquivos relacionados à sua atividade.

Apenas o Departamento de Risco e Compliance e o Diretor Presidente possuem acesso irrestrito aos arquivos do servidor. O Departamento de Risco e Compliance também deve apurar se os acessos estão adequados e sendo respeitados pelos Colaboradores. Prudência maior é dada para informações confidenciais de clientes cujos dados pessoais não podem ser copiados e devem ser utilizados apenas nas dependências da MSK Asset. O Departamento de Risco e Compliance deve observar acessos não autorizados e investigar os motivos. O Departamento de Risco e Compliance gerencia uma ficha com a lista de pastas eletrônicas a que cada Colaborador tem acesso. Os Colaboradores recebem e-mails e fazem parte de grupos de distribuição relativos à suas tarefas desempenhadas na MSK Asset. Apenas Colaboradores do departamento comercial, Departamento de Risco e Compliance e principais executivos recebem e-mails enviados pelos clientes com solicitações de movimentações.

Os Colaboradores são responsáveis pelas suas estações de trabalho, devendo protegê-las corretamente. As senhas, os acessos pessoais e as informações confidenciais devem ser guardadas e utilizadas adequadamente e podem ser requisitados pelo Departamento de Risco e Compliance quando da necessidade de alguma inspeção.

Toda rede computacional da MSK Asset está protegida por firewalls, antivírus e filtros de spans. Testes periódicos são feitos com propósito de avaliar possíveis vulnerabilidades e falhas nos sistemas operacionais, softwares e rede. São feitas avaliações de aplicativos e programas instalados, teste de “Ethical Hacking” (conjunto de técnicas de teste que utiliza os mesmos conhecimentos, ferramentas e metodologias utilizadas por um hacker para identificar pontos fracos dos controles existentes) e teste de penetração de rede (teste realizado por especialistas em segurança para procurar falhas no ambiente tecnológico). O Departamento de Risco e Compliance tem acesso a todas as mensagens trocadas via e-mail e deve ficar atento quanto aqueles contendo anexos de arquivos de grandes tamanhos. Todas as ligações telefônicas são gravadas e podem ser acessadas pelo Departamento de Risco e Compliance para esclarecer dúvidas ou quando houver suspeitas de descumprimento das políticas internas. Diariamente é feito *backup* dos arquivos salvos em nuvem em um local diferente do escritório da MSK Asset.

Anualmente o Diretor de Risco e Compliance deverá preparar um relatório relativo ao ano civil anterior contendo a conclusão dos exames efetuados e recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando necessário.

#### 4.2. Reportes Regulatórios

O Departamento de Risco e Compliance será obrigado a apresentar o Formulário de Referência à CVM, até 31 de março de cada ano, nos termos do Anexo 15-II, da Instrução CVM 558. Além disso, deverá cumprir com outros reportes regulatórios previstos na regulação aplicável, como o Relatório de Compliance e Controles Internos referido no item 3.1 acima, bem como a comunicação de não ocorrência (CNO) devida ao Conselho de Controle de Atividades Financeiras (COAF) até o dia 31 de janeiro de cada ano, entre outros.

Além disso, a MSK Asset deve manter os registros na CVM e o Formulário de Referência atualizados com relação a seus dados societários, informando à CVM, o mais rápido possível, de qualquer alteração dessas informações. O Formulário de Referência, juntamente com essa Política e todas as demais políticas da MSK Asset exigidas pela CVM, estarão disponíveis no site da MSK Asset.

### **5. Incidentes de Segurança**

Na hipótese de ocorrência do vazamento de algum dado confidencial interno da MSK Asset, o Departamento de Risco e Compliance deverá verificar a potencial extensão dos danos, bem como avaliar a necessidade de comunicação privada ou pública do vazamento das informações, a reavaliação das medidas de segurança da informação e, caso necessário, comunicar o vazamento aos órgãos competentes.

### **6. Segregação de Atividades**

A política de segregação física de atividades tem como objetivo estabelecer as regras que orientam a segregação física das instalações entre áreas responsáveis pelas atividades prestadas pela empresa, em particular, as atividades de administração de carteiras das demais atividades desenvolvidas.

As equipes envolvidas no processo de gestão de recursos são segregadas das áreas de atendimento e consultoria a clientes (comerciais), assim como da área de gestão de riscos e Departamento de Compliance.

Consequentemente, os equipamentos, rede e arquivos utilizados pela MSK Asset são organizados de modo a garantir atuação independente pelas diferentes áreas e segregação total de suas atividades. Tal organização consiste na utilização de um sistema operacional de tecnologia da informação para o controle e bloqueio de informações, a fim de preservar as informações confidenciais e permitir a identificação de pessoas que tenham acesso.

O acesso aos sistemas utilizados pela MSK Asset é restrito, regido por perfis de acesso e controlado por senhas e registros de log. Da mesma forma, o acesso físico aos servidores e equipamentos individuais também é controlado e restrito às pessoas autorizadas, de forma a garantir a integridade das informações e impedir o acesso de pessoas não autorizadas.

O Departamento de Risco e Compliance deverá monitorar os acessos concedidos aos Colaboradores, e cabe ao supervisor a responsabilidade pela análise da necessidade e verificação da correta utilização dos acessos e ferramentas concedidas.

Ainda, de acordo com o Contrato Social vigente da MSK Asset e com foco no melhor atendimento das demandas relacionadas à prestação de serviços de gestão de recursos, a MSK Asset também pretende prestar serviços correlatos, incluindo, mas não se limitando a, (i) assessoria e consultoria nas áreas de planejamento financeiro, investimentos em geral e atividades complementares, e (ii) a assessoria financeira em geral e estruturação de títulos, valores mobiliários, ativos e/ou outros produtos financeiros.

Em relação a essas outras atividades, esclarece-se que todas elas são desempenhadas no escopo de atuação da gestão de recursos e, portanto, qualquer atividade correlata deve ser contratada pelo cliente em complemento à atividade de gestão de recursos. Dessa forma, inexistem conflitos de interesse entre as atividades secundárias prestadas em benefício dos próprios clientes da gestão de recursos, quando contratadas.

#### 6.1. Segregação de Atividades entre a MSK Asset e MSK Invest

A MSK Asset é uma sociedade sob controle comum ao administrador da MSK Invest, empresa que atua no mercado de bitcoins desde 2016 prestando serviços de assessoria de investimentos em criptomoedas para seus clientes.

A estruturação da MSK Asset foi planejada de modo a garantir uma infraestrutura segregada e independente. As atividades prestadas pelas referidas sociedades são prestadas de maneira independente, na forma de seus respectivos contratos sociais. Ainda, como os respectivos mercados de atuação são diferentes, não há intercâmbio das informações que são obtidas e desenvolvidas por cada sociedade.

Consequentemente, os equipamentos, rede e arquivos, bem como o espaço físico, utilizados pela MSK Asset são organizados de modo a garantir atuação independente pelas sociedades e segregação total de suas atividades,

Tal organização consiste na utilização de um sistema operacional de tecnologia da informação para o controle e bloqueio de informações, a fim de preservar as informações confidenciais e permitir a identificação de pessoas que tenham acesso. O acesso aos sistemas utilizados pela MSK Asset e pela MSK Invest é restrito, regido por perfis de acesso e controlado por senhas e registros de log, não permitindo a interação entre as atividades de uma para com a outra sociedade. Da mesma forma, o acesso físico aos servidores e equipamentos individuais também é controlado e restrito às pessoas autorizadas, de forma a garantir a integridade das informações e impedir o acesso de pessoas não autorizadas.

Ademais, o Departamento de Risco e Compliance deverá monitorar os acessos concedidos aos colaboradores da MSK Asset, e cabe ao supervisor a responsabilidade pela análise da necessidade e verificação da correta utilização dos acessos e ferramentas concedidas.

## **7. Treinamento**

O Departamento de Risco e Compliance repassa a todos os Colaboradores as políticas e manuais da MSK Asset de forma que todos tenham conhecimento das melhores práticas e condutas, através dos treinamentos internos, para os novos Colaboradores, e de reciclagem, para os demais colaboradores. A MSK Asset incentiva que todos os colaboradores busquem atualizações em suas respectivas atividades de trabalho e que esclareçam dúvidas no ambiente interno.

Havendo necessidade, A MSK Asset promove treinamentos abertos aos colaboradores a respeito das melhores práticas de mercado.

## **8. Política de Certificação**

A MSK Asset não realiza a distribuição das cotas dos fundos por ela geridos. No entanto, é obrigatória a obtenção do CGA para aqueles Colaboradores que trabalhem na área de gestão de recursos e que tenham alçada/poder discricionário de investimento (compra e venda) dos ativos dos fundos de investimentos sob gestão.

A exigibilidade de certificação obrigatória não está relacionada ao cargo formal do profissional, mas sim às atividades efetivamente exercidas por ele.

O profissional contratado (não certificado) receberá, no momento da contratação, as instruções sobre a necessidade de certificação, a depender da atividade que exercerá dentro da MSK Asset. O Departamento de Risco e Compliance efetuará os devidos registros junto às entidades pertinentes.

O profissional que não apresentar a certificação necessária, deve ser impedido de iniciar as suas atividades. Se completado o prazo estabelecido pelo Departamento de Risco e Compliance para a retirada da certificação e o profissional não tiver apresentado, cabe ao Departamento de Risco e Compliance a comunicação ao responsável pela área em que o Colaborador foi contratado de que o profissional ainda não está habilitado a exercer as atividades pelas quais foi contratado.

Cabe ao responsável pela área que fez a contratação do novo Colaborador, a definição sobre o eventual remanejamento para uma outra área ou a sua manutenção em atividades não elegíveis, devidamente supervisionado por funcionários que possuem a certificação.

## **9. Plano de Continuidade de Negócios**



A MSK Asset possui um Plano de Contingência de forma a garantir a linearidade das operações, prevendo recursos alternativos e estratégias de continuidade em casos de ocorrências inesperadas.

Uma vez identificada a interrupção de quaisquer dos recursos essenciais às atividades, os responsáveis pela área de TI devem ser imediatamente comunicados a fim de tomar as providências cabíveis nos termos do presente Plano de Continuidade de Negócios. Todos os colaboradores devem possuir os contatos telefônicos e e-mail dos responsáveis pela área de TI, de modo a possibilitar a comunicação da contingência ocorrida e a solução mais rápida do problema, ou quando não possível obter uma solução imediata, a opção do fluxo alternativo mais viável.

Em caso de falha de fornecimento de energia, a MSK Asset possui *nobreak* para suportar o funcionamento do ambiente até que o fornecimento seja reestabelecido, ou em caso de longa interrupção, a utilização do servidor primário em nuvem associados aos notebooks permitem a utilização da mesma infraestrutura. Em caso de evacuação, impedimento à entrada no escritório ou incêndio com danos à infraestrutura local, os recursos de TI e todas as aplicações podem ser acessados remotamente através dos notebooks configurados especificamente para utilização da MSK Asset e que se encontram fora do escritório.

Quando por alguma eventualidade a infraestrutura de TI localizada no servidor primário em nuvem é afetada e não podem mais ser utilizados, é possível dar continuidade à operação usando o servidor de contingência em nuvem. Este servidor possui a mesma estrutura lógica do servidor em uso e com uma cópia atualizada das aplicações e arquivos da MSK Asset. A manutenção do fluxo de atividades é reforçada pelo acesso Web ao e-mail e acesso ao backup em nuvem, garantindo a continuidade do fluxo de atividades. Em caso de falhas em computadores utilizados pelos colaboradores, A MSK Asset conta com máquinas de contingência para utilização e já previamente configuradas.

Links de internet de diferentes provedores garantem a redundância da rede e alta disponibilidade entre sistemas/informações da MSK Asset e clientes e fornecedores de serviços. A disponibilidade do link principal e redundante é monitorada 24/7, com alertas em casos de indisponibilidade. A rede cabeada interna e distribuída via Wi-Fi é segregada da rede para visitantes. Backups de arquivos, de estratégias e de modelos de negócios são realizados diariamente para um servidor de backup na nuvem de maneira automática, com criptografia em todas as pontas da comunicação para garantir a segurança dos dados, e com uma plataforma para recuperar em instantes qualquer arquivo caso necessário.

Em complemento, realiza-se o *backup* dos dados em servidor de contingência em nuvem, com a restauração de informações a partir do backup testada periodicamente. Serviços utilizados pela equipe de gestão, tal como o “Bloomberg Professional”, Refinitiv World-check e Britech Atlas-Market Risk podem ser acessados via Mobile ou notebooks previamente configurados, sendo que esses serviços possuem seu próprio Plano de Contingência para manutenção de seu funcionamento e disponibilidade.

O acesso à rede é verificado por controle via login e senha única por usuário, com mudanças periódicas em tais acessos, podendo ser disponibilizado acesso remoto via Virtual Private Network (VPN) para determinados usuários. O serviço de e-mail é garantido por parceiro terceirizado que oferece suporte 24/7, incluído serviço anti-spam, possibilidade de acesso via Web Mail e usuários administradores associados à camada extra de segurança via Two Factor Authentication.

Todas as atividades dos colaboradores são compartilhadas de forma a evitar que a ausência de um colaborador impeça as atividades rotineiras do departamento ou da MSK Asset. São feitos manuais dos sistemas e planilhas proprietárias utilizadas. Em situações não previstas nos termos do presente Plano de Continuidade de Negócios e que podem afetar as atividades de departamentos específicos ou atividades da MSK Asset como um todo, será feita a mobilização prioritária de recursos humanos e eventuais aquisições de software ou hardware para manutenção do fluxo de operações da gestora.

## **10. Política Cibernética**

A MSK Asset estabelece a presente Política Cibernética, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da organização, dos clientes e do público em geral. Considerando-se a rápida evolução das práticas e soluções de cibersegurança, exigindo constantes adaptações, esta Política será atualizada e reavaliada por diretrizes e materiais adicionais ao longo do tempo.

A Política Cibernética visa garantir a confidencialidade, disponibilidade e integridade das informações, sejam elas de terceiros ou dados da própria MSK Asset.

- **Confidencialidade:** garante que as informações tratadas pela MSK Asset sejam restritas a um grupo restrito de usuários autorizados, impedindo a exposição de dados restritos e acessos não autorizados.
- **Disponibilidade:** garante a disponibilidade de informações aos usuários autorizados sempre que necessário.
- **Integridade:** garante a veracidade e completude das informações, de forma que elas sejam íntegras e sem alterações à dados por pessoas não autorizadas que possam efetuar modificações não aprovadas.

Toda informação relacionada às operações da MSK Asset, gerada ou desenvolvida nas dependências da MSK Asset, durante a execução das atividades de prestador de serviços de correspondente no país para A MSK Asset, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da MSK Asset.

Toda informação de propriedade da MSK Asset deve ser protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas. As diretrizes adotadas são:

- a) As informações da MSK Asset, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;
- b) As senhas são utilizadas como assinatura eletrônica e não devem ser divulgadas para todos. As senhas de acesso de estações de trabalhos devem ser compartilhadas com o Diretor de Risco e Compliance e os colegas de trabalho que exercem as mesmas atividades da mesma área de forma a evitar que as atividades da empresa sejam paralisadas caso seja necessário o acesso a uma estação sem a presença do usuário. O acesso de um Colaborador a uma estação de trabalho de um colega deve ser feito pontualmente, com parcimônia e restrito a continuidade da atividade exercida no momento;
- c) Acesso a dados confidenciais são restritos a determinados usuários e bloqueados com base no login de usuário. Acessos indevidos devem ser comunicados imediatamente ao Departamento de Risco e Compliance;
- d) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes;
- e) Cada usuário é responsável pelo uso dos recursos que lhe foram entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados;
- f) Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na MSK Asset ou para outras situações formalmente permitidas;
- g) O computador disponibilizado para cada Colaborador é de propriedade da MSK Asset;
- h) A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função;
- i) Apenas os equipamentos e softwares disponibilizados e/ou homologados autorizados pela MSK Asset podem ser instalados e conectados à rede;
- j) Solicitar alterações de senha sempre que exista a possibilidade de a mesma ter sido comprometida;
- k) Alterações em diretrizes de segurança do computador são bloqueadas por senha, impossibilitando a desativação do firewall, por exemplo;
- l) Em caso de não funcionamento do software antivírus instalado em cada computador, deverá o usuário notificar prontamente a equipe de TI;
- m) Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio da MSK Asset, e só podem ser conectados à rede Wi-Fi de visitantes, exceto em casos em que o Plano de Contingência requeira essa prática e em que exista autorização explícita do Departamento de Risco e Compliance;
- n) A senha da rede de internet principal da MSK Asset e das respectivas camadas de segurança são mantidas de forma segura e não são compartilhadas com todos os usuários; e

- o) Toda violação ou desvio, tais como instalação (intencional ou não) de vírus de informática, uso de software ilegal e tentativas de acesso a informações restritas, por exemplo, é investigada para a determinação das medidas necessárias e definição de possíveis sanções, visando à correção da falha ou reestruturação de processos e evitando que casos análogos se repitam.

## **11. Revisão da Política**

A presente Política será revisada anualmente, ou a qualquer momento, sempre que se observarem mudanças relevantes nas normas, regras, formato das atividades ou em qualquer outro aspecto intrínseco ao dia-a-dia da MSK Asset, nos termos da regulamentação e diretrizes aplicáveis.

\* \* \*