SPM
INVESTIMENTOS

POLÍTICA DE COMPLIANCE, REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

INFORMAÇÕES GERAIS

Esta Política estabelece as regras de controles internos visando garantir o permanente atendimento às normas, políticas e regulamentações vigentes, às melhores práticas de administração de valores mobiliários e aos padrões éticos e profissionais.

INFORMAÇÕES DA INSTITUIÇÃO

SUPERMARINE ADMINISTRAÇÃO DE CARTEIRAS DE VALORES MOBILIÁRIOS LTDA
CNPJ: 34.118.647/0001-34

ROD JOSÉ CARLOS DAUX, 5500 – EDIF SQUARE CORPORATE – TORRE LAGOA B - SALA 207 – 88.032-005 - CENTRO - FLORIANÓPOLIS - SANTA CATARINA

TELEFONE: (48) 3879-1936

EMAIL: compliance@spminvestimentos.com.br

INFORMAÇÕES DO MANUAL

NOME DO MANUAL: POLÍTICA DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS
VERSÃO: 5

DATA DE REGISTRO (REVISÃO): 20 DE MAIO DE 2024
DATA DE VIGÊNCIA: 20 DE MAIO DE 2025

SPM
INVESTIMENTOS

SUMÁRIO

CAPÍTULO I - OBJETIVO E ABRANGÊNCIA

OBJETIVO

A presente Política tem por objetivo estabelecer princípios e regras para a Gestora, com destaque para:

I. garantir, por meio de controles internos adequados, o permanente atendimento às normas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissionais.

II. assegurar que todos os profissionais que desempenham funções na empresa, especialmente funções ligadas à administração de carteiras de valores mobiliários, atuem com imparcialidade e conheçam os normativos da empresa, legislação e regulamentação aplicáveis, bem como as disposições relativas a controles internos;

III. identificar, administrar e eliminar eventuais conflitos de interesses que possam afetar a imparcialidade das pessoas que desempenham funções ligadas à administração de carteiras de valores mobiliários;

IV. assegurar o controle de informações confidenciais a que tenham acesso seus administradores, empregados e colaboradores;

V. assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico;

VI. implantar e manter programa de treinamento de administradores, empregados e colaboradores que tenham acesso a informações confidenciais, participem de processo de decisão de investimento ou participem de processo de distribuição de cotas de fundos de investimento;

VII. garantir a segregação física de instalações entre áreas responsáveis por diferentes atividades prestadas relativas ao mercado de valores mobiliários;

VIII. assegurar o bom uso de instalações, equipamentos e informações comuns em mais de um setor da empresa;

IX. preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas;

X. restringir o acesso a informações e permitir a identificação das pessoas que tenham acesso a informações confidenciais;

XI. promover prevenção e combate a atividades ilícitas.

ABRANGÊNCIA

Todos os sócios e colaboradores da Gestora deverão respeitar os termos desta Política, tendo atestado expressamente o seu conhecimento acerca das regras estabelecidas e comprometendo-se a cumpri-las, mediante assinatura do Termo de Ciência e Compromisso - Anexo I, antes do início do seu trabalho na Gestora.

Os sócios da empresa e o Diretor de Gestão de Riscos, Compliance e Controles Internos, estão à disposição para orientar em relação àinterpretação ou aplicabilidade das regras contidas nesta Política.

CAPÍTULO II – COMPLIANCE E CONTROLES INTERNOS

ESCOPO DE ATUAÇÃO DA GESTORA

A Supermarine Administração de Carteiras de Valores Mobiliários Ltda (doravante referida como "SPM" ou "Gestora") tem como objeto social somente a administração de valores mobiliários e possui como foco de atuação a gestão discricionária de carteiras administradas e fundos de investimento.

O processo de investimento adotado pela Gestora tem início no estudo da estrutura patrimonial do cliente, avaliando seu objetivo, necessidade e perfil de investimento, para que seja definido, então, um benchmark de entrega/resultados e um orçamento de volatilidade. Com tais parâmetros definidos, buscam-se ativos que respeitem os limites estabelecidos.

O desenvolvimento das atividades da Gestora, tendo em vista seu pequeno porte e a proximidade direta com os clientes, pode ser considerado de baixa complexidade, uma vez que as políticas de investimentos são pré-definidas para cada portfólio e devem ser seguidas em todos os seus termos.

Portanto, a Política de Compliance e Controles Internos ("Política") descrita no presente documento visa a manutenção da atuação da Gestora em conformidades com as regras que recaiam sobre si, especialmente a Resolução CVM n. 21, o Código de Administração de Recursos de Terceiros – ANBIMA, a Resolução CVM n. 50 e a Lei Geral de Proteção de Dados.

DISPONIBILIZAÇÃO/ACESSO

A Gestora tem definido que esta Política esteja disponível e acessível a todos os seus profissionais, de forma a assegurar que os procedimentos e as responsabilidades atribuídas aos diversos níveis da organização sejam conhecidos.

Antes da contratação de qualquer colaborar ou da entrada de qualquer futuro sócio, é obrigatória a leitura integral dos manuais e políticas estabelecidas no âmbito da Gestora, a fim de

que todas as pessoas envolvidas com o desenvolvimento das atividades estejam cientes e devidamente aderidas aos conceitos de conformidade, compliance, controles internos e PLDFT.

A íntegra da presente Política estará disponível no site da Gestora sempre em sua última versão atualizada.

RESPONSABILIDADES - ÁREA DE GESTÃO DE RISCOS, COMPLIANCE E CONTROLES INTERNOS

A área de Gestão de Riscos, Compliance e Controles Internos é a responsável pela elaboração, revisão e atualização periódica dos Códigos, Manuais e Políticas da Gestora, pela implementação e manutenção dos controles internos, realização de testes de aderência e realização de treinamentos dos Colaboradores.

O Diretor de Riscos, Compliance e Controles Internos, conforme definido pelo contrato social da SPM, é o principal responsável pela disseminação e supervisão das regras, controles e procedimentos internos, com o objetivo de mitigar riscos operacionais, regulatórios, morais e legais das atividades da Gestora, visando, principalmente, a preservação da boa reputação e idoneidade da SPM.

A área de Gestão de Riscos, Compliance e Controles Internos não se subordina a nenhuma outra área da Gestora, tendo seus poderes em relação a qualquer integrante de forma inde- pendente, se reportando somente ao Conselho de Administração da Gestora.

Constitui responsabilidade primordial da área de Gestão de Riscos, Compliance e Controles Internos as seguintes entregas periódicas:

I. Preencher o Formulário de Referência (ANEXO E da Resolução CVM n. 21) e enviar à CVM até o dia 31 de março de cada ano, a fim de certificar a aptidão para o exercício das atividades pela Gestora, bem como manter a versão atualizada do referido formulário disponível no site.

II. Encaminhar ao Conselho de Administração da Gestora, até o último dia do mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: a) as conclusões dos exames efetuados; b) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e c) manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

PROCEDIMENTOS DE GESTÃO DE RISCO DE COMPLIANCE E CONTROLES INTERNOS

A área de Gestão de Riscos, Compliance e Controles Internos envidará os melhores esforços para prevenir quaisquer desvios de conformidade com a normas que regem as atividades desenvolvidas pela Gestora.

Por intermédio da utilização do sistema de gerenciamento de compliance *COMPLIASSET*

(www.compliasset.com), faz-se uso da contratação de software desenvolvido por terceiros para a manutenção da rotina das obrigações da Gestora em relação aos controles internos e compliance. Referida plataforma auxilia a área no diagnóstico de eventuais riscos assumidos pela Gestora na sua atuação como administradora de carteira de terceiros.

Ao realizar diagnósticos periódicos na Gestora, a área de Gestão de Riscos, Compliance e Controles Internos deverá identificar eventuais fatos ou atos que possam causar entraves na Gestora e, em relatório adequado, defini-los em 3 (três) categorias, conforme a seguir dispostas:

RISCO BAIXO
Pequeno potencial de dano reputacional e/ou baixa complexidade na resolução do problema

RISCO MÉDIO
Considerável potencial de dano reputacional e/ou média complexidade na resolução

RISCO ALTO
Grande potencial de dano reputacional e/ou alta complexidade na resolução

Diante da identificação do potencial risco lesivo à Gestora, a área de Gestão de Riscos, Compliance e Controles Internos da Gestora enviará relatório diretamente para a pessoa responsável pela resolução do problema para que sejam adotadas as medidas cabíveis no prazo de 24 (vinte e quatro) horas.

Não havendo a adoção de medidas por parte do responsável ou não sendo solucionado o problema, o Diretor de Gestão de Riscos, Compliance e Controles Internos primeiramente diligenciará pela eliminação dos riscos identificados e, após, realizará procedimentos disciplinares em face da pessoa que deu causa ao risco identificado.

O procedimento disciplinar acimar referido deverá ser devidamente documentado, preferencialmente pela plataforma de gerenciamento de compliance ou, na impossibilidade do uso deste, por e-mail.

A pessoa que estiver na condição de objeto de investigação do procedimento disciplinar terá direito de apresentar sua defesa com manifestação por escrito acompanhada de eventuais documentos ou declarações de terceiros que abonem a sua ação ou omissão.

O procedimento disciplinar deverá seguir o seguinte rito:

I. Instauração do procedimento disciplinar por escrito, com os fundamentos que o acompanham, devendo ser instaurado em prazo não superior a 30 (trinta) dias da data do conhecimento dos fatos;

II. O profissional objeto do procedimento disciplinar será comunicado oficialmente por escrito, a fim de que, no prazo de 5 (cinco) dias úteis, apresente sua defesa acompanhada de documentos e/ou testemunhas;

III. O Diretor de Gestão de Riscos, Compliance e Controles Internos receberá a defesa e, no prazo de 5 (cinco) dias úteis, proferirá sua decisão acerca de eventual aplicação de sanção disciplinar;

IV. Havendo a aplicação da sanção disciplinar, o profissional sancionado poderá, no prazo de 2 (dois) dias úteis, apresentar recurso ao Comitê de Gestão de Riscos da empresa;

V. O Comitê de Gestão de Riscos analisará o recurso na primeira reunião subsequente ao pedido, seja ela ordinária ou extraordinária, e proferirá decisão quanto à manutenção da sanção imposta ou pelo provimento do recurso, fazendo constar em ata.

O Diretor de Gestão de Riscos, Compliance e Controles Internos é a pessoa responsável/autoridade pela avaliação da defesa apresentada e, de acordo com sua discricionariedade, poderá aplicar ao infrator as seguintes sanções:

I. Advertência;

II. Suspensão;

III. Demissão/Exclusão da sociedade.

Aplicar-se-á a sanção de suspensão sempre que alguma pessoa da Gestora receber 3 (três) advertência consecutivas, bem como será demitido/excluído da sociedade o infrator que tiver recebido 3 (três) suspensões consecutivas.

CAPÍTULO III – SEGREGAÇÃO DE ATIVIDADES

CONTEXTO ESTRUTURAL DA GESTORA

Como mencionado na presente Política, a Gestora possui atuação em administração de carteiras de terceiros com baixa complexidade e estrutura de pequeno porte, não desenvolvendo atividades que possam ser conflitantes entre si.

A Gestora tem como preocupação principal preservar a segregação física e independência funcional da área responsável pela Administração de Recursos de Terceiros, uma vez que lida com informações sensíveis de clientes e da própria empresa.

Por outro lado, a Gestora preserva também a segregação e independência das atividades da área de Gestão de Riscos, Compliance e Controles Internos, a fim de que possa manter sua autoridade enquanto responsável pela manutenção da conformidade da Gestora com a legislação e pela fiscalização do respeito ao enquadramento à política de investimentos prevista para os portfólios geridos.

Da Segregação das Atividades

***a) Segregação Física*:**

A Gestora possui fisicamente segregadas entre si as áreas de Administração de Recursos de Terceiros e de Gestão de Riscos, Compliance e Controles Internos. Os sócios e colaboradores deverão evitar o trânsito entre as salas durante o desenvolvimento das suas respectivas atividades, a fim de evitar prejuízo de performance da área, da Gestora ou, ainda, acesso às informações das quais não deveriam ter ciência.

Havendo identificação de trânsito excessivo de pessoas entre as áreas, caberá ao Diretor de Gestão de Riscos, Compliance e Controles Internos instaurar o procedimento disciplinar nos moldes descritos no Capítulo II da presente Política, apurar as responsabilidades e aplicar eventuais sanções.

***b) Segregação de Instalações Tecnológicas*:**

A Gestora possui segregação de instalações tecnológicas, especialmente em relação ao sistema de armazenamento de arquivos na nuvem (Google), a fim de que a área de Gestão de Riscos, Compliance e Controles Internos tenha total independência de atuação, mantendo sua autoridade sobre todas as demais áreas da Gestora.

Nesse sentido,quando estiver atuando na fiscalização do atendimento às regras de conformidade e enquadramento, o Diretor de Gestão de Riscos, Compliance e Controles Internos possui acesso a todos os arquivos da Gestora, tanto em vias físicas quanto digitais.

Monitoramento de Atividades

A área responsável pela Gestão de Riscos, Compliance e Controles Internos realizará o monitoramento constante do plano de negócios da Gestora, cujo objetivo é a identificação de possíveis futuras atividades a serem desenvolvidas que possam ser consideradas conflitantes.

Diante da identificação de ideação de eventual desenvolvimento de atividade conflitante no âmbito da Gestora, a presente Política deverá ser atualizada para constar novas regras pertinentes à segregação e mitigar todo e qualquer conflito de interesses.

Empresa Sob Controle Comum e Conflitos de Interesse

A SPM informa que a JB3 Assessor de Investimento Ltda., inscrita no CNPJ/MF sob o n. 13.895.778/0001-58 (“AI”) atua como escritório de assesor de investimento, nos termos da Resolução CVM nº 178, de 14 de fevereiro de 2023 (“Resolução CVM 178”), estando sob controle comum com a SPM pela empresa JB3 Controle S/A, inscrita no CNPJ/MF sob o n. 52.996.012/0001-11. Neste sentido, a SPM adota medidas para tratamento dos potenciais Conflitos de Interesse existentes entre as atividades desenvolvidas pelo AI e pela SPM, as quais estão detalhadas no Código de Ética e Conduta da SPM.

CAPÍTULO IV – SEGURANÇA E SIGILO DAS INFORMAÇÕES

Objetivo

A presente Política tem por objetivo estabelecer mecanismos para: a) propiciar o controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso os sócios, diretores, administradores, profissionais e terceiros contratados da Gestora; b) assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico; e c) implantar e manter treinamento para os sócios, diretores e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas e participem do processo de decisão de investimento.

As regras estabelecidas nesta Política visam resguardar a Gestora e seus clientes da divulgação de informações confidenciais obtidas por meio da atividade de administração de ativos e carteiras de valores mobiliários.

Para fins da presente Política serão consideradas:

Informações Confidenciais: Todas e quaisquer informações e/ou dados de natureza confidencial, incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais, know-how, cópias, diagramas, modelos, amostras, programas de computador, informações relacionadas a estratégias de investimento, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora, seus sócios e clientes, bem como quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividadede administração de ativos e carteiras de valores mobiliários desenvolvida pela Gestora e, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui contempladas.

Informações não confidenciais: As Informações Confidenciais não incluem informações que:

(a) sejam de domínio público, sem violação do disposto nesta Política; ou (b) tenham sido recebidas de boa fé pelo colaborador de terceiros que tenham o direito de divulgá-las, sem obrigação de confidencialidade.

Monitoramento das Informações

Todos os profissionais que desenvolvam atividades na Gestora, ao firmar o Termo de Compromisso presente no ANEXO I desta Política, deverão tomar conhecimento e expressamente anuir

com o que segue:

I. Expressamente obriga-se a manter o sigilo das informações Confidenciais, Reservadas ou Privilegiadas que lhe tenham sido transmitidas, fornecidas e/ou divulgadas sob ou em função de seu vínculo com a Gestora ou de relacionamento com clientes, comprometendo-se a não utilizar, reproduzir ou divulgar as referidas informações, inclusive a pessoas não habilitadas ou que possam vir a utilizá-las indevidamente em processo de decisão de investimentos próprios ou de terceiros, exceto mediante autorização expressa e escrita do respectivo titular e na medida do estritamente necessário para o desempenho de suas atividades e/ou obrigações;

II. Caso qualquer profissional seja obrigado a divulgar Informações Confidenciais, Reservadas ou Privilegiadas, por determinação judicial ou de autoridade competente, deverá comunicar à área de Gestão de Riscos, Compliance e Controles Internos sobre a existência de tal determinação previamente à divulgação e se limitar estritamente à divulgação nos limites pelos quais foi requisitada;

III. Para os propósitos do disposto nesta Política, caberá ao colaborador o ônus de provar o caráter não confidencial de qualquer informação eventualmente vazada;

IV. O acesso às Informações Confidenciais, Reservadas ou Privilegiadas será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos profissionais que atuam na Gestora. O controle de acesso a tais informações será realizado por meio de pastas compartilhadas na nuvem (Google), sendo acessadas apenas com *login* e senha pessoal, que, a critério do Diretor de Gestão de Riscos, Compliance e Controles Internos, poderão respeitar uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa;

V. O acesso aos arquivos que contenham Informações Confidenciais, Reservadas ou Privilegiadas só poderá ser realizado nos horários em que o profissional esteja desenvolvendo suas atividades relacionadas à Gestora;

VI. O acesso remoto a tais informações deverá ser devidamente justificado e comprovado que se deu em razão da atividade profissional, sob pena de ser aberto procedimento administrativo nos moldes previstos no Capítulo II da presente Política;

VII. A obrigação do profissional de observar as regras previstas na presente Política será válida mesmo após o término do vínculo dele com a Gestora, estando sujeito a responsabilização na esfera cível e penal;

VIII. Em caso de término do vínculo do profissional com a Gestora, este deverá restituir imediatamente todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder; e

IX. Caso tenham conhecimento de que qualquer profissional da Gestora tenha infringido a presente política, os demais profissionais obrigam-se a reportar tal falta ao Diretor de Gestão de Riscos, Compliance e Controles Internos, sob pena de ser considerado corresponsável com o infrator.

Todos os prestadores de serviços terceirizados que forem contratados pela Gestora deverão assinar contrato com previsão de cláusula de confidencialidade em relação às Informações Confidenciais, Reservadas ou Privilegiadas a que tiveram acesso no exercício de suas atividades.

Responsabilidades

A área de Gestão de Riscos, Compliance e Controles Internos é a responsável pelo treinamento e monitoramento de todos os profissionais que possam ter acesso a Informações Confidenciais, Reservadas ou Privilegiadas.

A Gestora conta com aparatos cibernéticos suficientes a proteger os arquivos que contenham Informações Confidenciais, Reservadas ou Privilegiadas, entretanto, todos os sócios, colaboradores e demais profissionais possuem responsabilidade sobre o sigilo das informações recebidas.

Havendo indícios de vazamento de informações confidenciais, reservadas ou privilegiadas, será instaurado o procedimento disciplinar previsto no Capítulo II da presente Política e serão imediatamente adotadas todas as medidas cabíveis para que a informação não seja transmitida, bem como para que os eventuais receptores não façam uso indevido.

CAPÍTULO V – PLANO DE CONTINUIDADE DE NEGÓCIOS

Objetivo

O Plano de Continuidade de Negócios da Gestora tem por objetivo estabelecer as medidas a serem tomadas para identificar e prevenir as possíveis contingências que poderão trazer um impacto negativo considerável sobre o desenvolvimento das atividades prestadas por seus sócios, diretores e colaboradores.

Diretrizes na Prevenção e Tratamento das Contingências

Para a eficaz implementação do Plano de Continuidade de Negócios, a Gestora busca conhecer e reparar os principais sinais de vulnerabilidade de suas instalações e equipamentos.

Para tal fim, são tomadas medidas que permitem à Gestora: a) conhecer e minimizar os danos no período pós-contingência; b) eximir riscos ou minimizar ao máximo as perdas para si, seus clientes, seus sócios e colaboradores advindos da interrupção de suas atividades; e c) retomar com brevidade as atividades de gestão.

Para redução e controle de eventuais perdas com contingências, todos os sócios e colaboradores da Gestora deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não) e melhores práticas de saúde e segurança no ambiente de

trabalho.

A identificação de eventuais incidentes que causem riscos à continuidade dos negócios da Gestora deverá ser imediatamente comunicada ao Diretor de Gestão de Riscos, Compliance e Controles Internos, a fim de que sejam tomadas as medidas necessárias para a mitigação dos riscos.

A área de Gestão de Riscos, Compliance e Controles Internos, em razão do recebimento de eventual comunicação envolvendo incidente de contingência, dará início ao procedimento de contenção/correição, no seguinte sentido:

I. Identificação do incidente;

II. Mensuração do nível do Risco;

III. Comunicação aos setores envolvidos;

IV. Conferência de equipamentos e arquivos sob ameaça;

V. Tomada de decisão quando à necessidade de adoção de medidas de correição;

VI. Comunicação imediata ao responsável pela solução do incidente; e

VII. Avaliação sobre a efetividade das medidas adotadas.

Como resultado destes procedimentos, no caso de a equipe da Gestora não conseguir acesso ao escritório, contará com todos os sistemas que a permitem voltar a operar nor- malmente, uma vez que todos os dados e informações operacionais estarão em segurançae poderão ser acessados remotamente, bastando um dispositivo tecnológico com acesso àinternet.

Na hipótese de uma contingência que inviabilize o uso do escritório por um longo período,a Gestora tem a possibilidade de manter-se operante de qualquer outro escritório, inclu- indo *home office* integral, não inviabilizando a operação normal da gestora.

Por fim, para a retomada célere e eficaz das operações após uma contingência, a Gestora pode:

I. Utilizar alternativas para substituição de equipamentos danificados, através de fornecedores já conhecidos;

II. Manter saldo financeiro e/ou acesso a crédito para qualquer despesa de contin- gência ou compra de equipamentos ou serviços que se fizerem necessários;

III. Manter procedimentos das operações administrativas mesmo durante os efeitos da contingência, de formar remota e em localização externa; e

IV. Realizar outros procedimentos que visem a retomada das atividades.

Ademais, a Gestora ainda contará com administradores fiduciários e custodiante que, em seus próprios manuais e políticas, contam com procedimentos sólidos de continuidade de negócios, fortalecendo a preservação dos recursos e direitos dos investidores.

Recuperação do Negócio e das Atividades

A Gestora mantém a identificação atualizada de seus processos de negócios, de forma que, na eventual ocorrência de contingência, é possível retomar as ope- rações com os mínimos custos de transação de recursos humanos, físicos e materiais pos- síveis.

A Gestora conta com backup e versioning na "nuvem" através dos serviços Google - G Suite. O serviço conta com armazenamento de arquivos criptografados usando os melhores padrões de segurança existentes no mercado, podendo ser conferido no ambiente <https://workspace.google.com/intl/pt-BR/security/?secure-by-design_activeEl=data-centers>.

A Gestora possui, ainda, equipamento físico dedicado para o backup em tempo real de todos os seus arquivos presentes na nuvem, composto por dois discos rígidos com capacidade suficiente de armazenamento. Sendo assim, caso haja contingência com o armazenamento na nuvem, os discos rígidos continuarão servindo como backup e, em razão da existência de trabalho simultâneo de dois discos, se algum destes apresentas incidentes, o outro permitirá a continuidade dos trabalhos de gestão.

Desta forma, a salvaguarda dos dados dos usuários, bem como imagens das estações de trabalho (planilhas, bancos de dados, etc.) e outras informações operacionais, permitem que a Gestora recomponha rapidamente o estado operacional em caso de falhas ou contingências na sua estrutura cibernética operacional.

Disposições Gerais

Todos os sócios, diretores e colaboradores da Gestora, bem como prestadores de serviços terceirizados deverão envidar os melhores esforços para que a Gestora mantenha o desenvol vimento das suas atividades de forma ininterrupta.

CAPÍTULO VI – SEGURANÇA CIBERNÉTICA

Objetivo

A presente Política tem por objetivo a mitigação dos riscos que envolvam a Segurança Ciberné- tica, especialmente naquilo que se refere à prevenção de ataques praticados por organizações criminosas ou hackers individuais, organismos de Estado, terroristas, competidores e demais espécies de agentes invasores.

A Gestora desenvolve meios de Segurança Cibernética a fim de se preservar incidentes ilícitos que, entre outros, possuem os seguintes motivos: a obtenção ilícita de ganho financeiro; o

roubo, manipulação ou adulteração de informações; a obtenção de vantagens competitivas e informações confidenciais de empresas concorrentes; a fraude, sabotagem ou exposição indevida de dados ou informações da Gestora; a promoção de ideias políticas e/ou sociais; a prática do terror e disseminação de pânico e caos; a atuação de hackers por mero deleite pessoal.

Identificação/avaliação de riscos

A Gestora considera de suma importância a avaliação periódica dos riscos que envolvam controles de Segurança Cibernética, definindo, por tal razão, procedimentos de monitoramento, prevenção e tratamento de incidentes.

Nesse sentido, em razão do atual porte da empresa, a área de Gestão de Riscos, Compliance e Controles internos atua como grupo de monitoramento da Segurança Cibernética, cuja atribuição é acompanhar a realização de testes periódicos, emitir relatório quando identificado algum incidente capaz de criar risco ao desenvolvimento das atividades da Gestora e realizar treinamento periódico aos sócios e colaboradores da Gestora.

Por intermédio da contratação da empresa terceirizada CS2 Tecnologia, CNPJ 07.580.065/0001-00, realizam-se testes mensais de Segurança Cibernética, a fim de que sejam avaliadas vulnerabilidades e potenciais ameaças relacionadas a:

I. Invasões;

II. Malware (vírus, Cavalo de Troia, Spyware, ransomware);

III. Engenharia social (pharming, phishing, vishing, smishing, acesso pessoal);

IV. Ataque de DDoS;

As ameaças cibernéticas podem variar de acordo com a natureza, a vulnerabilidade e as informações ou os ativos possuídos pela Gestora. Tendo em vista que as consequências podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais, os possíveis impactos dependem da rápida detecção e resposta após a identificação do ataque.

Ações de prevenção e proteção

As ações de prevenção e proteção a ataques cibernéticos constituem um conjunto de medidas adotadas visando a manutenção da segurança das informações/dados da Gestora, especialmente no que diz respeito a acessos aos sistemas da Gestora.

Na condução dos trabalhos da Gestora, os sócios e demais profissionais terão acesso aos seus respectivos sistemas de trabalhos, desde que estejam definidos o *login* e a senha de acesso individual, com caracteres de alta complexidade (senha forte).

O acesso, uma vez concedido, será destinado apenas aos recursos relevantes para que o profissional desempenhe as suas atividades, não devendo se estender aos demais ativos e áreas

daGestora.

Todos os *logins* de acesso e senhas serão de conhecimento da Área de Gestão de Riscos, Compliance e Controles Internos da Gestora, a fim de que sejam auditáveis e rastreáveis, bem como seja possibilitada a alteração como forma de prevenção e proteção a ataques cibernéticos.

Os sócios, diretores e profissionais da Gestora deverão acessar os sistemas tecnológicos sempre por meio de equipamentos disponibilizados pela própria Gestora, a fim de que sejam mantidos os padrões de segurança estabelecidos nesta Política, principalmente em razão da instalação de sistemas de antivírus e demais meios de combate a invasores.

A Gestora conta com instalação de antivírus Norton em todos os seus equipamentos, devidamente atualizado, com capacidade suficiente para realizar a manutenção da Segurança Cibernética da Gestora.

Além disso, apesar de contar com sistema de armazenamento criptografado de arquivos em nuvem Google G-Suite, mantém dois discos rígidos físicos com capacidade suficiente e realizando backup diário de todos os dados/arquivos/informações da empresa presentes na nuvem, bem como backup entre si (*backup* do *backup*).

Também como ação de prevenção a ataques cibernéticos, a Gestora possui duas redes de internet independentes entre si, com objetivo de manter os sistemas conectados mesmo que alguma das redes venha a ser invadida e, assim, por meio da rede não invadida, adotar as medidas necessárias para resposta à invasão.

Diante da necessidade de acesso aos sistemas via dispositivo pessoal, o que se considera apenas a título de não interrupção das atividades/continuidade do negócio, o profissional deverá certificar que possui mecanismos de defesa iguais aos instalados nos equipamentos da Gestora e deverá manter consigo anotações a respeito do local, data e horário de acesso remoto aos ambientes cibernéticos da Gestora.

A área de Gestão de Riscos, Compliance e Controles Internos poderá solicitar, a qualquer tempo e de qualquer sócio, diretor ou colaborador, relatório das anotações de acesso remoto realizados, a fim de monitorar eventuais riscos assumidos pela Gestora em relação à Segurança Cibernética.

Monitoramento e testes

A área de Gestão de Riscos, Compliance e Controles Internos poderá solicitar, com auxílio da empresa terceiriza CS2 Tecnologia, CNPJ 07.580.065/0001-00, realiza monitoramento dos ativos tecnológicos da Gestora, a fim de identificar elementos estranhos à Gestora.

Na execução dos testes de monitoramento são verificados os seguintes quesitos:

I. Existência de computadores não autorizados;

II. Existência de softwares não licenciados;

III. Verificação da atualização de softwares e sistemas operacionais da empresa, especialmente plataforma Google G-Suite e sistema antivírus Norton;

IV. Possíveis vulnerabilidades na estrutura tecnológica; e

V. Realização de teste de invasão externa e phishing.

Aliada aos testes de monitoramento acima citados, a área de Gestão de Riscos, Compliance e Controles Internos da Gestora realizará verificação diária das rotinas de backup presentes naGestora.

O monitoramento dos controles de segurança cibernética na Gestora adota uma abordagem baseada em riscos, levando em consideração o contexto das atividades desenvolvidas e as necessidades emergentes.

Os testes de monitoramento serão realizados em periodicidade mensal, sendo emitido relatório quando identificado algum risco de invasão ou incidente de falha de segurança cibernética na Gestora, devendo ser encaminhado ao Diretor de Gestão de Riscos, Compliance e Controles Internos contendo as seguintes informações:

I) Identificação do incidente;

II) Grau de risco, nos termos do Capítulo II da presente Política;

III) Plano de resposta;

IV) Orçamento de custo para solução/resposta ao incidente.

Plano de resposta

Em caráter emergencial, diante do recebimento do relatório contendo incidente de falha de segurança cibernética, o Diretor de Gestão de Riscos, Compliance e Controles Internos da Gestora deverá adotar imediatamente as medidas que considerar cabíveis, comunicando ao Comitê de Riscos na primeira reunião subsequente à data dos fatos.

Nos demais casos, o Diretor de Gestão de Riscos, Compliance e Controles Internos da Gestora comunicará o Conselho de Administração para que sejam adotadas as medidas necessárias a alertar todos os demais setores quanto aos riscos identificados.

Diante da existência de incidente de segurança cibernética de Risco Alto, a área de Gestão de Risco, Compliance e Controles Internos adotará medidas que assegurem a integridade dos dados, arquivos e informações da Gestora, tais como:

I. Acionamento de profissionais-chave;

II. Acionamento do setor jurídico da Gestora;

III. Acionamento de administradores fiduciários, órgãos reguladores e demais entidades envolvidas com as atividades da Gestora;

Todas as áreas da Gestora envidarão os melhores esforços para apresentar resposta imediata aos incidentes de segurança identificados, devendo manter arquivados todos os documentos relativos às medidas adotadas, a fim de que sejam encaminhados à área de Gestão de Riscos, Compliance e Controle Internos da Gestora para que se efetue registro de gerenciamento de incidentes e plano de resposta.

Governança

A área de Gestão de Riscos, Compliance e Controles Internos da Gestora realizará treinamento em periodicidade mínima anual de todos os sócios, diretores e colaboradores da Gestora, a fim de que estejam constantemente atualizados sobre os conceitos e especificidades da segurança cibernética.

Também serão realizadas em periodicidade mínima anual a alteração das senhas de acesso aos sistemas da Gestora de todos os sócios, diretores e demais profissionais, tanto em razão da prevenção e proteção a ataques cibernéticos quanto para instituir a cultura de segurança, conscientizando sobres os riscos e as melhores práticas existentes no mercado.

Todo e qualquer sócio, diretor ou profissional tem o dever de comunicar a área de Gestão de Riscos, Compliance e Controles Internos sobre eventual suspeita de invasão ou ataque cibernético, sob pena de se tornar objeto de procedimento disciplinar em razão da omissão.

Todas as dúvidas que envolvam a segurança cibernética da Gestora deverão ser enviadas à Área de Gestão de Riscos, Compliance e Controles Internos, a fim de que sejam imediatamente dirimidas, a fim de eliminar possíveis riscos à segurança.

CAPÍTULO VII – DISPOSIÇÕES FINAIS

Acessibilidade

Esta Política estará disponível na rede mundial de computadores, sempre em sua última versão atualizada, sem quaisquer bloqueios ou senha de acesso, podendo ser encontrada no sítio eletrônico da Gestora www.spminvestimentos.com.br

Quaisquer denúncias, reclamações ou sugestões que envolvam o desenvolvimento das atividades da Gestora deverão ser encaminhadas por escrito para o e-mail compliance@spminvestimentos.com.br, sendo resguardado o anonimato, quando solicitado.

ANEXO I

SPM
INVESTIMENTOS

TERMO DE CIÊNCIA E COMPROMISSO COM A POLÍTICA DE COMPLIANCE, REGRAS E CONTROLES INTERNOS DA SUPERMARINE INVESTIMENTOS.

Eu, **(QUALIFICAÇÃO COMPLETA DO DECLARANTE)**, declaro para os devidos fins que:

a) Recebi uma versão atualizada da Política de Compliance, Regras e Controles Internos da empresa SUPERMARINE ADMINISTRAÇÃO DE CARTEIRAS DE VALORES MOBILIÁRIOS LTDA, inscrita no CNPJ n. 34.118.647/0001-34, cujas regras me foram previamente explicadas e em relação às quais tive oportunidade de esclarecer minhas dúvidas;
b) Li e compreendi as regras estabelecidas e comprometo-me a observá-las no desempenho de minhas funções; e
c) Comprometo-me, ainda, a informar imediatamente à área de Gestão de Riscos, Compliance e Controles Internos sobre qualquer fato de que venha a ter conhecimento que possa gerar algum risco para a Supermarine Investimentos.

Estou ciente de que a não observância da Política poderá caracterizar falta grave, passível de punição com as penalidades cabíveis, inclusive desligamento ou demissão por justa causa.

Florianópolis, XX de XXXXX de 20XX.

_____

[NOME DO COLABORADOR]

[CPF]