MARR GESTÃO DE RECURSOS LTDA.

REGRAS, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

Julho de 2023

FOLHA DE CONTROLE

Informações Gerais

Título	Regras, Procedimentos e Descrição dos Controles Internos
Elaborador	Ana Carolina Paifer
Data da Próxima Revisão	31/07/2024
Área Proprietária da Política	Compliance e Riscos Operacionais
Procedimentos e Outros Documentos Relacionados	Resolução CVM nº 21/2021; Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e Lei 13.709, de agosto de 2018 (Lei Geral de Proteção de Dados)

SUMÁRIO

1. INTRODUÇÃO

Este documento tem como objetivo apresentar as Regras, Procedimentos e Descrição dos Controles Internos da MARR Gestora de Recursos a serem observados pelos profissionais da área de Compliance (“Colaboradores”), visando a verificação do cumprimento da legislação e regulamentação aplicável.

Este documento também tem como objetivo apresentar as Regras referentes à Política de Segurança de Informações da gestora, estabelecendo diretrizes e responsabilidades para o gerenciamento da segurança da informação, de acordo com a sensibilidade dos dados e das informações sob responsabilidade da MARR. Esta Política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida (integridade) e permitir que a informação esteja disponível quando for necessário (disponibilidade).

Este Manual aplica-se a todos os sócios, funcionários e integrantes de cargos de administração ou gestão da MARR, bem como aos profissionais e demais prestadores de serviço que tenham, ou possam vir a ter, acesso a informações confidenciais ou de natureza estratégica, financeira, técnica, comercial ou negocial relativa à MARR.

Os Colaboradores têm o dever de ler, entender e aderir a este Manual. O descumprimento das diretrizes estabelecidas por este documento poderá resultar em penalidades que, conforme o caso, poderão incluir advertência, treinamento de reciclagem, demissão e/ou notificação aos órgãos reguladores.

2. REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

I. Estrutura de Compliance

Diretor de Compliance: a MARR conta com um diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos, assim como da legislação e regulamentação aplicável conforme exigido pela Instrução CVM N° 21/21 (“Diretor de Compliance”), que é sócio executivo da MARR com senioridade suficiente para exercer suas atividades com independência. O Diretor de Compliance, assim como os colaboradores que o auxiliam com os controles internos, não atua em funções relacionadas à administração de carteiras de valores mobiliários, ou ainda em qualquer atividade que limite a sua independência.

Comitê de Compliance: parte dos objetivos do Comitê de Compliance da MARR ("Comitê") é deliberar sobre questões relacionadas a regras, procedimentos e controles internos elaborados para o cumprimento da legislação e regulamentação aplicável à MARR e sobre situações atípicas, não contempladas nesta Política. A composição do Comitê e suas regras de funcionamento estão descritas no Formulário de Referência disponibilizado no website da MARR.

II. Testes de Compliance

O Diretor de Compliance possui rotinas periódicas para fins de promoção de testes de conformidade, com o intuito de verificar o fiel cumprimento pelos colaboradores das normas e procedimentos definidos internamente, bem como as diretrizes trazidas pelas normas que regulam a atividade de gestão profissional de recursos de terceiros, de maneira a mitigar os principais riscos aos quais a MARR está sujeita.

Para tanto, compete ao Diretor de Compliance a adoção das seguintes rotinas no tocante às

matérias abaixo relacionadas:

a. Manuais e Políticas

Apresentar, anualmente, o Código de Ética e Conduta da MARR aos colaboradores e demais políticas internas pertinentes, coletando à adesão aos mesmos, bem como quando do ingresso de um novo colaborador; e validar anualmente ou na periodicidade definida em cada uma das políticas internas ou, ainda, sempre que julgar necessário, todos os regulamentos e normas de conduta interna, rotinas e procedimentos, adequando-os às normas e instruções dos órgãos reguladores da atividade desenvolvida pela MARR.

b. Treinamento

Ao ingressar à MARR e anualmente, todos os administradores, sócios, empregados e colaboradores que possuam acesso às informações confidenciais, participem do processo de decisão de investimento ou participem do processo de distribuição de cotas de fundos de investimentos são sujeitos aos treinamentos de Prevenção à Lavagem de Dinheiro, de Prevenção à Corrupção, Confidencialidade e Insider Trading, bem como demais regras e procedimentos descritos nos manuais e políticas adotados internamente. Estes treinamentos são coordenados pelo Diretor de Compliance e poderão ser realizados através de reuniões, apresentações, cursos, e-mails ou palestras e deverá ser compatível com a atividade desempenhada pelo administrador, sócio ou funcionário.

Todo o treinamento interno proposto, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Os treinamentos relacionados ao conteúdo das políticas internas serão realizados, com periodicidade mínima anual, pela Diretora de Compliance sendo obrigatórios a todos os Colaboradores e controlados por lista de presença. A referida Diretoria poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às políticas internas.

c. Relatórios Anuais de Conformidade e Suitability

O Diretor de Compliance é responsável por elaborar o Relatório Anual de Conformidade, nos termos da Instrução CVM N° 21/21. O Relatório Anual de Conformidade deverá ser apresentado aos Comitês de Compliance e Executivo da MARR, bem como à Diretoria, até o último dia útil do mês de abril de cada ano, com as seguintes considerações:

- Conclusões dos testes de compliance realizados ao longo do ano anterior;
- Recomendações a respeito de eventuais deficiências encontradas, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
- Manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo Diretor de Risco, a respeito das deficiências encontradas nas verificações e das medidas planejadas de acordo com cronograma específico, ou das medidas efetivamente adotadas, para saná-las.

Adicionalmente, compete ao Diretor de Compliance a revisão do relatório anual a ser enviado à ANBIMA sobre as atividades de distribuição e suitability, em linha com as Diretrizes ANBIMA para Suitability.

d. Conflitos de Interesse

Compete ao Compliance a verificação de potenciais situações de conflito de interesses entre os colaboradores, os investidores, clientes e a própria Gestora, orientando os envolvidos e tomando as providências cabíveis. Neste sentido, o Compliance deverá promover a avaliação prévia de atividades externas praticadas pelos colaboradores, com ou sem fins lucrativos, a fim de identificar eventuais riscos à reputação e imagem da Gestora, assim como eventual influência na discricionariedade do colaborador no desempenho de suas funções. No que se refere aos potenciais conflitos de interesse decorrentes de investimentos pessoais dos colaboradores no mercado financeiro e de capitais, compete ao Diretor de Compliance, semestralmente, recolher e verificar as informações indicadas pelos colaboradores na Tabela de Detalhamento dos Investimentos Pessoais, a fim de verificar a sua adequação à Política de Investimentos Pessoais definida e adotada pela MARR.

e. Prevenção e Combate à Lavagem de Dinheiro

Assegurar o respeito à Política de Prevenção e Combate à Lavagem de Dinheiro adotada pela MARR.

f. Conduta dos Colaboradores

Analisar, sempre que existente, eventuais infrações às normas constantes das políticas e manuais adotados internamente e à legislação vigente, sugerindo ao Comitê Executivo as sanções administrativas cabíveis.

Nessa linha, compete ao Compliance a avaliação da ocorrência ou indícios de violação da legislação que incumba a CVM fiscalizar, alinhando com o Comitê Executivo a comunicação à CVM, no prazo máximo de 10 (dez) dias úteis da ocorrência ou identificação, bem como arquivando a documentação relativa à avaliação realizada que tenha fundamentado a decisão de comunicar ou não à CVM.

g. Contratação de funcionários, prestadores de serviço e demais parceiros

Elaborar e garantir a manutenção de controles internos visando o conhecimento de funcionários e parceiros da MARR com o objetivo de assegurar padrões elevados de seus quadros e evitando a contratação de pessoas de reputação não ilibada ou que possam, de qualquer forma, prejudicar a imagem e reputação da instituição, observados os parâmetros definidos na Política de Seleção, Contratação e Monitoramento de Prestadores de Serviço;

Certificar-se de que todos os colaboradores possuem as habilitações necessárias ao desempenho das respectivas funções na MARR, coordenando a manutenção das informações a serem imputadas na Base de Dados ANBIMA

h. Prestação de Informações

Enviar as informações periódicas e eventuais exigidas pela CVM, bem como a toda e qualquer entidade autorreguladora à qual a MARR esteja vinculada;

Manter as informações cadastrais da MARR junto aos órgãos reguladores e autorreguladores devidamente atualizadas, bem como aquelas disponibilizadas através do site da MARR na internet, em especial no que se refere aos manuais e políticas adotados, bem como aquelas relacionadas à equipe e produtos sob gestão.

3. SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

I. Diretrizes

As diretrizes dessa Política compreendem as seguintes definições e regras que deverão se seguidas por todos os colaboradores:

O comprometimento com a melhoria contínua dos procedimentos relacionados com a Segurança da Informação;

As informações da MARR, seus colaboradores, seus 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 mauuso e exposição indevida;

A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

Toda informação deve ser classificada conforme o nível de risco que ela representa, bem como, o nívelde confidencialidade que ela requer;

O acesso às informações e recursos só deve ser feito, se devidamente autorizado;

A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o comoresponsável pelas ações realizadas;

Haverá necessidade de segregação de instalações, equipamentos e informações comuns, quando aplicável.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acessosomente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança das informações da MARR devem ser reportados à área de Compliance; e

As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

II. Confidencialidade

Para os efeitos deste Manual, considera-se Informação Privilegiada aquela relacionada a qualquer emissor de valores mobiliários negociados no mercado brasileiro (como companhias abertas e fundos de investimento) que preencha, cumulativamente, as duas seguintes condições: (a) seja confidencial, assim entendida a informação que não tenha sido ainda divulgada ao mercado de maneira oficial, peloemissor ou pelo terceiro detentor da informação relacionada ao emissor; (b) seja relevante, assim entendida a informação capaz de afetar a decisão dos investidores de negociar com valores mobiliários do emissor.

As regras e controles de sigilo e conduta aqui relacionados e adotados serão cabíveis aos sócios, administradores, colaboradores e funcionários, e servem para identificar os detentores de informações privilegiadas, de forma a estabelecer uma barreira de informações com os demais funcionários:

- Monitoramento do efetivo trancamento das estações de trabalho;
- Monitoramento da realização de backup das informações arquivadas na Gestora;
- Verificação da implementação das regras de acesso e barreiras da informação, assegurando que pastas, diretórios e bases de dados somente sejam acessíveis a pessoas autorizadas;
- Verificação do eventual esquecimento de documentos em cima das mesas e/ou nas impressoras;
- Coordenação de testes periódicos de segurança para os sistemas de informações, em especial os mantidos em meio eletrônico e, inclusive, para os fins do plano de continuidade de negócios adotada pela Gestora.
- Coleta de Termo de Adesão e Confidencialidade dos colaboradores, através do qual estes se comprometem à observância e cumprimento das diretrizes definidas nos manuais e políticas internas;
- Coleta de Termo de Confidencialidade dos prestadores de serviço da Sociedade que tenham acesso a informações confidenciais, caso no Contrato firmado não haja cláusula com esta finalidade.

III. Responsabilidades

A governança da Segurança da Informação é exercida pela Alta Administração da MARR, com a supervisão do Departamento de Compliance, observando-se as responsabilidades e atribuições claramente definidas, as quais incluem, adicionalmente, as áreas de Compliance, de Tecnologia da Informação, de Controles Internos, de Auditoria Interna, os Colaboradores e Terceiros.

IV. Gestão da Segurança da Informação

Para assegurar que as informações sejam adequadamente protegidas a MARR Gestão de Recursos Ltda. adota os seguintes procedimentos e controles:

Gestão de Ativos da Informação: os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados;

Identificação da Informação: O profissional que recebe ou prepara uma informação deve identificar a natureza desta, conforme o item a seguir.

Classificação da Informação: As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Confidencial, Restrita, Interna e Pública. Para a classificação devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Controles para informações classificadas como “Confidencial”: Informações confidenciais devem ser identificadas como tal: e-mails, apresentações, documentos. Os e-mails e arquivos com informações confidenciais devem ser protegidos. O acesso às informações confidenciais deve ser controlado. Qualquer documento pessoal que seja disponibilizado a terceiros deve ser enviado com a identificação do terceiro, editada em marca d’água. Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros.

Salvaguarda da Informação: A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento e Descarte. O profissional responsável pela informação gerada deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte. Na dúvida do tempo regulatório, questionar o Jurídico. O descarte de informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

Mesa Limpa: Nenhuma informação confidencial deve ser deixada à vista. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Gestão de Acessos: Os acessos físicos e do ambiente devem ser rastreáveis, a fim de garantir que todas as ações sejam passíveis de auditoria e possam identificar individualmente o Colaborador, para que o mesmo seja responsabilizado por suas ações. Os equipamentos, ferramentas e sistemas concedidos aos colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis às MARR

Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de negócio e Back ups: Os riscos e incidentes de Segurança da Informação devem ser reportados ao Responsável pelo Compliance, que adotará as medidas cabíveis. Plano de contingência e de continuidade dos principais sistemas e serviços deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. As cópias de segurança / Back up também deverão ser testadas anualmente.

Controles físicos - são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta. Exemplos de mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas entre outros; e

Controles lógicos - são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada. Exemplos de mecanismos de segurança que apoiam os controles lógicos: autenticação, a criptografia, a prevenção e a detecção de intrusão, entre outros.

Propriedade Intelectual: Tecnologias, marcas, metodologias e quaisquer informações que pertençam à MARR não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

Rastreamento: É permitido o uso pessoal dos equipamentos de informática e de comunicação utilizados pelos colaboradores para a realização das atividades profissionais. Lembrando que como tais recursos, como e-mails, sistemas, computadores, telefones e gravação de voz pertencem às MARR, são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria e/ou exigência judicial. O acesso interno às informações e gravações deve ser previamente autorizado pelo “Head da área” e copiado o responsável pelo Compliance.

Termo de Conhecimento: Os profissionais devem aderir formalmente a um termo, comprometendo- se a agir de acordo com a política de Segurança da Informação.

Treinamento: Os profissionais que tenham acesso a informações confidenciais ou participem de processo de decisão de investimento devem ser treinados a respeito de Segurança da Informação.

Os colaboradores detentores de Informações Confidenciais ou Privilegiadas, em função de

seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas: Os profissionais devem evitar circular em ambientes externos à MARR com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao desenvolvimento do projeto e no interesse do cliente, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso; O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico; As informações que possibilitem a identificação de um cliente da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da MARR ou do próprio cliente; Os profissionais devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc; Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos; A senha de acesso do Colaborador ao sistema da MARR é pessoal e intransferível; O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora, e poderá ser monitorado pela área de Compliance sempre que necessário. O uso do e-mail corporativo para fins pessoais por parte Colaboradores será admitido desde que não haja impacto no desempenho de suas funções na Gestora.

V. Propriedades básicas da Segurança da Informação

As seguintes propriedades devem ser observadas na gestão da Segurança da Informação:

Confidencialidade - propriedade que limita o acesso à informação tão somente aos usuários considerados legítimos, ou seja, àqueles autorizados pelo proprietário da informação;

Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida;

Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação

Autenticidade - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;

Irretratabilidade ou não repúdio - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;

Conformidade - propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

VI. Testes Periódicos de Segurança

Testes de Controles: A efetividade da política de Confidencialidade e Segurança da Informação é verificada por meio de testes periódicos dos controles existentes. Um plano de teste deve ser efetuado pelo responsável por Tecnologia da Informação assegurando que: recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação, adequado nível de confidencialidade e acessos as informações confidenciais, segregação física e lógica, recursos computacionais, de controle de acesso físico e lógico, estejam protegidos, manutenção de registros que permita a realização de auditorias e inspeções.

Para assegurar o respeito à Política de Segurança da Informação e Segurança Cibernética adotada pela MARR, os testes períodos incluem dedicação aos sistemas de informações confidenciais, não apenas, mas em especial para os mantidos em meio eletrônico, por parte

dos sócios, administradores, colaboradores e funcionários que as possuem. Esses testes também identificam os detentores das informações para responsabilização, em caso de vazamento.

O acesso a todos os sistemas, incluindo os que controlam informações confidenciais, é liberado com base no princípio da necessidade da informação para a execução da função (need-to-know/need-to- have principle). O controle é feito por meio dos perfis de acesso, que segregam as funções. Cada colaborador possui um conjunto de perfis relacionados às suas atividades, e a MARR dispõe de controles internos para que o acesso seja liberado mediante aprovação. Todos os colaboradores recebem treinamento sobre segurança da informação e assinam o termo de ciência da Política de Segurança da Informação.

A MARR oferece avaliações e treinamentos periódicos aos quais os colaboradores são submetidos durante o ano, com o objetivo de conscientizá-los sobre confidencialidade das informações, cyber segurança, engenharia social, phishing, entre outras potenciais ameaças à integridade dos sistemas de informação, além da conscientização sobre essas ameaças e de como se proteger delas e respondera elas. A MARR dispõe de tecnologias de defesa contra possíveis ataques aos seus sistemas e realiza testes periódicos no sistema disponível na rede mundial de computadores (SITE), denominados Penetration Test. Adicionalmente, a MARR realiza testes anuais de contingência para validar o Plano de Continuidade de Negócios.

A efetividade da política de Confidencialidade e Segurança da Informação será verificada por meio de testes periódicos dos controles existentes, portanto um plano de teste deve ser efetuado pelo responsável por TI. A fim de verificar a integridade dos sistemas, inclusive com relação aos sistemas de informações confidenciais mantidas em meio eletrônico, a equipe de TI realiza testes semestrais, que são formalizados por meio de um reporte enviado ao Diretor de Compliancee Riscos.. Semestralmente a equipe de TI confirmará com os respectivos coordenadores de cada Colaborador a lista de todos os sistemas ao qual possuem acesso e os coordenadores deverão confirmar se os acessos devem ser mantidos a cada um desses sistemas. O reporte a ser enviado ao Diretor de Compliance deverá conter a lista de todos os sistemas e respectivos colaboradores que possuem acesso, juntamente com a confirmação dos respectivos coordenadores, além de eventuais inconsistências detectadas em cada sistema.

O Plano de testes assegura que:

1 – Os recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação;

2 – Adequado nível de confidencialidade e acessos as informações confidenciais;

3 – Segregação lógica de dados;

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

5 – Manutenção de registros que permita a realização de trilhas de auditorias e inspeções de atividades, garantindo assim, a identificação dos detentores das informações para responsabilização em caso de vazamento.

O Diretor de Compliance deverá revisar a lista, confirmando a adequação dos acessos de cada Colaborador e adotando eventuais medidas cabíveis para correção das inconsistências detectadas.

VII. Segurança Cibernética

a) Definição: Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI.

b) Elementos da Segurança Cibernética: Elementos como segurança de aplicações e bancos de dados, gerenciamento de identidade, segurança para dispositivos móveis, times de exercícios de segurança, Threat Hunting, recuperação de desastres/planejamento de continuidade de negócios (relativos a TI), educação do usuário final, entre outros, são alguns exemplos aplicados em segurança cibernética.

c) Plano de Respostas a Incidentes:

O Plano de Resposta a Incidentes considera o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da MARR.

Este Plano abrange também os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da MARR.

Além disso, são elaborados cenários de incidentes considerados nos testes de continuidade de negócios. Além disso, será requerida a classificação dos dados e as informações quanto à relevância, conforme critérios estabelecidos. Adicionalmente, deverão ser definidos os parâmetros a serem utilizados na avaliação da relevância dos incidentes.

A MARR deverá elaborar relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, com data base de 1 de setembro.

VIII. Processamento e Armazenamento de Dados

A MARR tem critérios definidos para contratação de serviços relevantes de processamento e armazenamento de dados e incluem a identificação e segregação de dados dos clientes, além de garantia de confidencialidade, integridade, disponibilidade e recuperação de dados e informações processadas ou armazenadas.

A área de TI é responsável pela prestação de serviços de processamento e armazenamento de dados e conta com um servidor próprio de propriedade da gestora com redundância no servidor, cujo controle é feito através de mecanismos lógicos e físicos.

4. REVISÃO DESTA POLÍTICA

O Diretor de Compliance deverá realizar uma revisão desta política a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, incluindo no relatório anual de compliance eventuais deficiências encontradas. A versão atualizada da Política será divulgada a todos os colaboradores e no website da MARR: www.marrcapitalgestora.com.br.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da MARR e acontecimentos regulatórios relevantes.