SUMÁRIO

POLÍTICA DE GERENCIAMENTO DE RISCOS DA MÉLIUZ S.A.

CAPÍTULO I - DEFINIÇÕES

1.1. Quando não definido em outros dispositivos desta Política, os termos iniciados em letra maiúscula, estejam no singular ou no plural, no masculino ou no feminino, terão os seguintes significados:

"Administradores" significa os membros do Conselho de Administração, Diretores Estatutários e não Estatutários e membros dos Comitês de Assessoramento da Companhia, estatutários e não estatutários, e seus respectivos suplentes, conforme aplicável.

"Apetite a Riscos" significa o grau de exposição a Riscos que a Companhia está disposta a assumir para atingir seus objetivos.

"Colaboradores" significa, em conjunto com os Administradores, toda pessoa que mantém vínculo estatutário ou empregatício com a Companhia e suas Controladas, tais como: empregados em tempo integral e temporário, empregados terceirizados, estagiários e demais colaboradores da Companhia e de suas Controladas quando realizarem quaisquer atos ou transações, em nome da Companhia.

"Companhia" significa a Méliuz S.A.

"Comitês de Assessoramento" significa todo e qualquer comitê de assessoramento do Conselho de Administração, do Comitê de Auditoria ou outros comitês criados com o objetivo de auxiliar a Companhia e seus Administradores na condução das atividades em conformidade com as políticas, códigos e regimentos da Companhia, bem como da legislação e regulamentação aplicáveis, sendo instalados em caráter não estatutário, podendo ou não ser permanente, de acordo com as necessidades da Companhia.

"Controladas" significam as sociedades subsidiárias e/ou controladas da Companhia.

"COSO" significa o Comitê de Organizações Patrocinadoras da Comissão Treadway (*Committee of Sponsoring Organizations of the Treadway Commission*), uma organização privada dedicada a fornecer orientações e diretrizes sobre gerenciamento de riscos corporativos, controles internos e prevenção de fraudes.

"Gerenciamento de Riscos" significa o sistema intrínseco ao planejamento estratégico de negócios, composto por processos contínuos e estruturados para identificar, monitorar e responder a eventos de Risco da Companhia, visando a redução da probabilidade de incidência de tais eventos e o impacto de perdas, com a consequente criação de valor e preservação da longevidade dos negócios.

"Instrução CVM 358/02" significa a Instrução CVM nº 358, de 03 de janeiro de 2002, conforme alterada, que dispõe sobre a divulgação e uso de informações sobre Ato ou Fato Relevante relativos às companhias abertas.

"Matriz de Riscos" significa a ferramenta indicada no item 3.4 (ii) abaixo, que expressa graficamente os riscos: (i) de baixa probabilidade e baixo impacto; (ii) de baixa probabilidade e alto impacto; (iii) de alta probabilidade e baixo impacto; e, por fim, (iv) de alta probabilidade e alto impacto, auxiliando na definição de Apetite a Risco e na implementação do Gerenciamento de Riscos pela Companhia e por suas Controladas.

"Política" significa esta Política de Gerenciamento de Riscos.

"Risco" significa fator ou evento incerto cuja materialização pode: (i) causar impactos negativos no cumprimento dos objetivos da Companhia e suas Controladas; e/ou (ii) subsidiar o processo de tomada de decisão quando representar uma oportunidade.

"Termo de Adesão" significa o termo de adesão referente à presente Política, nos moldes do Anexo I desta Política.

CAPÍTULO II - OBJETIVO E APLICAÇÃO

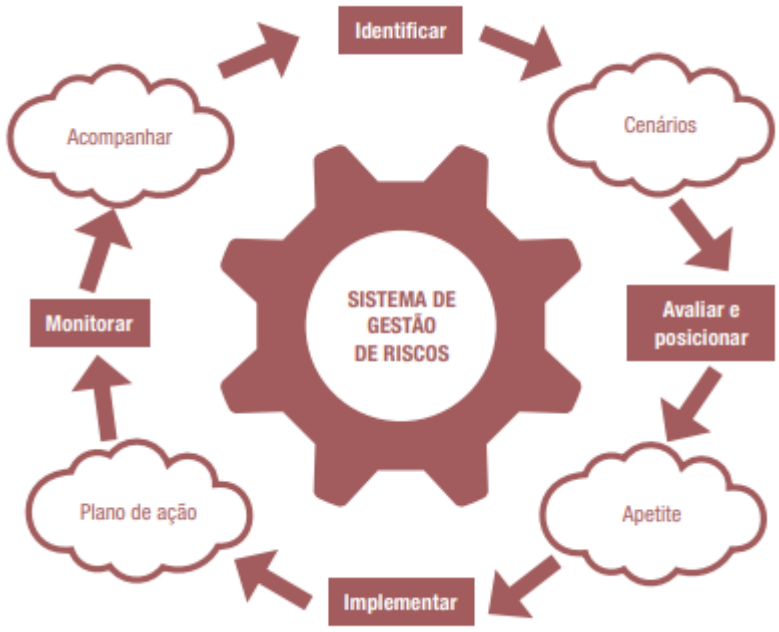
2.1. A presente Política tem por objetivo estabelecer os princípios, diretrizes e responsabilidades gerais a serem observados no processo de Gerenciamento de Riscos da Companhia e de suas Controladas, visando a perpetuidade dos negócios.

2.2. Esta Política se aplica a todos os Administradores e demais Colaboradores da Companhia e de suas Controladas, de forma a possibilitar a adequada identificação, avaliação, direcionamento, monitoramento e comunicação dos Riscos aos quais a Companhia e suas Controladas estão ou podem ser expostas, contribuindo para o gerenciamento dos mesmos e para a tempestiva tomada de decisões e medidas aplicáveis.

CAPÍTULO III - GERENCIAMENTO DE RISCOS

3.1. O Gerenciamento de Riscos é responsabilidade de todos os Administradores e Colaboradores, e requer a participação ativa de todas as áreas da Companhia, na extensão de suas competências, integrando-se às metas e objetivos estratégicos dos negócios da Companhia e de suas Controladas.

3.2. A estrutura organizacional dos processos de Gerenciamento de Riscos da Companhia é baseada nas diretrizes estabelecidas pelo Instituto Brasileiro de Governança Corporativa – IBGC e pelo COSO, especialmente no que que diz respeito ao fluxo de identificação, avaliação, implementação e monitoramentos dos Riscos aos quais a Companhia e suas Controladas estão expostas. Referidas diretrizes foram adaptadas conforme a natureza do negócio, características operacionais e demais especificidades da Companhia, nos termos estabelecidos nesta Política.



Fonte: Caderno de Governança Corporativa do IBCG: Gerenciamento de Riscos Corporativos - Evolução em Governança e Estratégia. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21794

3.3. O Gerenciamento de Riscos possui relacionamento direto com os objetivos da Companhia e de suas Controladas, impactando nas estratégias de negócios, na definição de seus controles operacionais internos e na busca da excelência na gestão empresarial.

3.4. A Companhia não adota parâmetros objetivos para tomar decisões a respeito da aceitação ou não aceitação de determinados riscos. O processo de Gerenciamento de Riscos da Companhia é composto das seguintes etapas:

(i) identificação e classificação dos Riscos conforme categorias descritas no item 4.1 abaixo;

(ii) análise dos Riscos identificados e indicação gráfica daqueles de baixa probabilidade e baixo impacto; de baixa probabilidade e alto impacto; de alta probabilidade e baixo impacto; e de alta probabilidade e alto impacto, conforme a seguinte representação gráfica ("Matriz de Riscos"):

Fonte: Caderno de Governança Corporativa do IBCG: Gerenciamento de Riscos Corporativos - Evolução em Governança e Estratégia. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21794

(iii) definição e implementação das ações de resposta aos Riscos; e

(iv) definição dos procedimentos de monitoramento e comunicação.

3.4.1. As seguintes abordagens e instrumentos podem ser adotados pela Companhia durante o processo de Gerenciamento de Riscos:

- Questionários de risco: A liderança da Companhia é solicitada a preencher um questionário específico para que indique possíveis Riscos aos quais a Companhia está exposta. Os cenários de risco são observados e catalogados;

- Ciclos de entrevistas: Os cenários de risco são identificados e discutidos com determinados Colaboradores. Os resultados também são documentados como parte da avaliação;

- Auditorias de processos: Os processos da Companhia são auditados e avaliados, a fim de verificar eventuais Riscos aos quais está exposta. Neste processo, Matrizes de Riscos são criadas/atualizadas. Tais registros

contribuem para a identificação de Riscos dentro da Companhia, funcionando como uma fonte de possíveis ameaças ou fraquezas.

3.4.2. A etapa prevista no item 3.4 (i) acima é finalizada com o desenvolvimento de um mapa de riscos, que é avaliado anualmente. O mapa pode ser atualizado devido a: (i) novos cenários (interno, político, econômico, entre outros); (ii) resultados de auditorias, entrevistas, questionários, observações e demais atividades; ou (iii) evolução da cultura de integridade e mitigação de Riscos.

3.4.3. Após a conclusão da etapa prevista no item 3.4 (i) acima, deve ser realizada a análise do grau de cada Risco. A metodologia utilizada para realização desta análise considera: impacto/consequência do potencial de perdas financeiras, degradação da imagem, penalidades legais etc. e a probabilidade/vulnerabilidade de ocorrência de Risco com base em quão robustos os controles internos relacionados são. O perfil do risco é determinado ao se combinar o impacto/consequência e probabilidade/vulnerabilidade esperadas do Risco.

3.5. A Companhia determina como cada cenário de risco será respondido, considerando: (i) *terminar*, ou seja, eliminar Riscos, redefinir os objetivos e/ou estratégias de negócios; (ii) *diversificar*, ou seja, intensificar o nível de gestão e/ou melhorar os controles internos; (iii) *aceitar*, ou seja, não realizar nenhuma ação adicional e continuar o monitorando, especialmente quando não é possível ou prático respondê-lo; ou (iv) *passar adiante*, transferindo a responsabilidade para terceiros (por exemplo, no risco de incêndio, o custo do sinistro pode ser transferido para seguradoras).

3.5.1. As recomendações previstas no item 3.5 acima se desdobram em ações detalhadas, pilotos, testes, validações e ajustes necessários para assegurar a eficácia do tratamento e controle dos Riscos aos quais a Companhia está exposta. A partir dos Riscos identificados e ações recomendadas, a Companhia deverá implementar os planos de ação a fim de garantir o tratamento dos Riscos.

3.6. Além dos instrumentos descritos acima, são utilizados procedimentos de pré-avaliação cadastral de novos clientes, disseminação dos códigos, condutas e procedimentos da Companhia, treinamentos, com a finalidade de identificar e mitigar os Riscos aos quais a Companhia está exposta.

CAPÍTULO IV - CATEGORIAS DE RISCOS

4.1. Após a análise dos Riscos, conforme o item 3.4 (i), os Riscos serão divididos em categorias, de acordo com a probabilidade de materialização e expectativa de grau de impacto no cumprimento dos objetivos da Companhia e de suas Controladas, e podem ser classificados da seguinte forma:

- Riscos operacionais: são riscos decorrentes de falhas, erros, deficiências e/ou inadequações de processos internos, de gestão de pessoas e de uso de tecnologia, ou, ainda, riscos oriundos de eventos externos e que podem afetar a operação de nossos negócios.

- Riscos macroeconômicos: são riscos decorrentes de efeitos não esperados no cenário econômico, político e nas tendências de mercado que podem ter reflexo no comportamento dos clientes e consumidores, tais como taxa de juros, inflação, investimentos financeiros, dentre outros.

- Riscos de *compliance*: são riscos causados pela falha no cumprimento de leis, regras, regulamentos e de nossos códigos e políticas internas, e também dos códigos, políticas e regras de clientes ou de fornecedores com os quais nos relacionamos, ou pela existência de processos em aberto ou processos futuros que podem resultar em perda financeira.

- Riscos corporativos: são os principais riscos de cunho estratégico, operacional, financeiro, regulatório, de mercado, de mão de obra, políticos, socioambientais, que podem impactar as atividades ou nossos objetivos.

- Riscos estratégicos: são os riscos oriundos da implementação de uma estratégia malsucedida ou ineficaz que deixe de alcançar os retornos pretendidos.

- Riscos regulatórios: são os riscos resultantes de modificações nas regulamentações e ações de órgãos reguladores, seja em âmbito internacional ou nacional, que podem resultar na crescente pressão competitiva, aumentar os custos das atividades da Companhia ou até mesmo inviabilizá-la.

- Riscos jurídicos: São aqueles que podem surgir em decorrência de processos nos quais a Companhia é autora ou ré, por descumprimento de obrigações aplicáveis ao negócio, por contratações de terceiros sem análise jurídica, perdas financeiras decorrentes de reclamações ou de indenizações/multas por eventuais danos a terceiros decorrentes das atividades que desenvolvemos;

- Riscos tecnológicos e cibernéticos: riscos relacionados ao ambiente de tecnologia da informação (infraestrutura, gestão de acessos, segurança da informação) que podem impactar os negócios da Companhia, como a ocorrência de ciberataques, vazamento e/ou perda de integridade de informações, indisponibilidade do ambiente de TI, obsolescência tecnológica, vazamento de dados/informações pessoais, roubo/vazamento de informações estratégicas, envio de arquivos confidenciais, em via digital ou telefônica, acesso inadequado a ativos e recursos de TI, acesso remoto inseguro, dentre outros.

- Riscos de imagem: são riscos resultantes da ocorrência de evento, geralmente ocasionado por outros riscos listados acima, que podem causar danos à reputação, imagem, credibilidade e/ou marca da Companhia e de suas Controladas, inclusive em razão de publicidade negativa, independentemente de sua veracidade.

CAPÍTULO V - RESPONSABILIDADES E COMPETÊNCIAS

5.1. No Gerenciamento de Riscos, o Conselho de Administração, a Diretoria da Companhia, o Comitê de Auditoria, a Auditoria Interna, a Área de Segurança da Informação, bem como as Gerências e demais Colaboradores da Companhia, possuem atribuições distintas e devem atuar de maneira integrada, conforme competências abaixo estabelecidas.

5.2. Conselho de Administração: Compete ao Conselho de Administração da Companhia:

(i) aprovar a Política de Gerenciamento de Riscos e suas revisões/atualizações;

(ii) estabelecer as diretrizes gerais das estratégias de Gerenciamento de Riscos;

(iii) estabelecer o nível de risco que a Companhia se submete na condução de seus negócios por meio da avaliação e aprovação da Matriz de Riscos apresentada pelo Comitê de Auditoria;

(iv) acompanhar e direcionar o desenvolvimento de uma sólida estrutura de Gerenciamento de Riscos, dando apoio em caso de necessidade aos demais integrantes da estrutura de Gerenciamento de Riscos da Companhia;

(v) assegurar ao Comitê de Auditoria autonomia operacional e orçamento próprio, destinado a cobrir suas despesas de funcionamento do referido comitê;

(vi) supervisionar as atividades do processo de Gerenciamento de Riscos executadas pelos demais integrantes da estrutura organizacional de Gerenciamento de Riscos da Companhia;

(vii) avaliar a adequação da estrutura (recursos humanos, financeiros e sistemas) destinada ao processo de Gerenciamento de Riscos;

(viii) acompanhar a evolução do Gerenciamento de Riscos por meio do enquadramento da Companhia aos limites estabelecidos;

(ix) monitorar o Comitê de Auditoria, bem como quaisquer outros Comitês de Assessoramento, estatutários ou não, integrantes da estrutura organizacional de Gerenciamento de Riscos da Companhia; e

(x) definir as decisões a serem tomadas nas hipóteses de conflitos e impasses, caso o Comitê de Auditoria (e, eventualmente, outros Comitês de Assessoramento integrantes da estrutura organizacional de Gerenciamento de Riscos) não cheguem a uma decisão final sobre determinado tema.

5.3. Diretoria. Compete à Diretoria da Companhia, dentre outras atribuições:

(i) implementar as estratégias e diretrizes da Companhia aprovadas pelo Conselho de Administração;

(ii) executar a Política de Gerenciamento de Riscos e, sempre que necessário, propor ao Conselho de Administração revisões às estratégias e diretrizes da Companhia ou à Política de Gerenciamento de Riscos; e

(iii) identificar Riscos preventivamente e fazer sua respectiva gestão, avaliando probabilidade de sua ocorrência e adotando medidas para sua prevenção e/ou mitigação.

5.4. Comitê de Auditoria: Compete ao Comitê de Auditoria da Companhia:

(i) avaliar e monitorar a exposição da Companhia aos Riscos que possam afetar a continuidade de seus negócios;

(ii) supervisionar as atividades das áreas financeira, controladoria e contábil da Companhia, avaliando as informações trimestrais e demonstrações financeiras;

(iii) acompanhar e supervisionar as atividades da auditoria interna e da área de controles internos da Companhia;

(iv) opinar na contratação e destituição dos serviços de auditoria independente;

(v) avaliar a efetividade do modelo de Gerenciamento de Riscos e sugerir soluções de aprimoramento de seus processos ao Conselho de Administração, quando necessário, apontando as causas e responsabilidades;

(vi) recomendar ao Conselho de Administração a revisão ou a implementação de alterações, priorizações e inclusões na Matriz de Riscos, na distribuição de competências, nas categorias de riscos, e nos processos internos de Gerenciamento de Riscos da Companhia;

(vii) assessorar o Conselho de Administração na avaliação de políticas, limites e planos de ação relacionados ao Gerenciamento de Riscos;

(viii) avaliar e monitorar o cumprimento e a efetividade desta Política e recomendar correções ou aprimoramentos necessários ao Conselho de Administração; e

(ix) receber e tratar informações acerca do descumprimento de dispositivos legais e normativos aplicáveis a nós, além de regulamentos e códigos internos.

5.4.1. O Comitê de Auditoria é órgão vinculado ao Conselho de Administração da Companhia, dotado de autonomia operacional e orçamento próprio aprovado pelo Conselho de Administração, destinado a cobrir despesas com seu funcionamento.

5.4.2. Em atendimento ao Regulamento do Novo Mercado, o Comitê de Auditoria possui regimento interno próprio, aprovado pelo Conselho de Administração, que prevê o detalhamento de suas funções e procedimentos operacionais.

5.5. Auditoria Interna. Compete à Auditoria Interna, dentre outras atribuições:

(i) auditar o processo de Gerenciamento de Riscos da Companhia;

(ii) monitorar o ambiente de controles internos e da efetividade do Gerenciamento de Riscos executado pelo Comitê de Auditoria, Diretoria e Conselho de Administração;

(iii) apresentar ao Comitê de Auditoria, periodicamente, pareceres imparciais, independentes e tempestivos contendo as suas conclusões e recomendações;

(iv) executar os testes de controles de acordo com o planejamento da auditoria;

(v) verificar a implementação dos planos de ação e sua eficácia;

(vi) identificar a necessidade de priorizar determinadas ações, bem como ampliar testes e/ou monitoramento contínuo, em função de novos Riscos ou agravamento de Riscos previamente mapeados;

(vii) identificar e apontar oportunidades de melhorias nos processos de controle internos e de gestão de Riscos; e

(viii) emitir opinião formal sobre os controles internos testados.

5.5.1. A Auditoria Interna deverá possuir estrutura e orçamento suficientes ao desempenho de suas funções. A estrutura e o orçamento da Auditoria interna estão sujeitos a reavaliação pelo Conselho de Administração, por iniciativa própria ou por recomendação do Comitê de Auditoria, ao menos uma vez ao ano.

5.6. Área de Segurança da Informação. Compete à Área de Segurança da Informação, dentre outras atribuições:

(i) identificar, monitorar e mitigar os riscos relacionados ao ambiente de tecnologia da informação (infraestrutura, gestão de acessos, segurança da informação) que possam prejudicar ou impedir o bom andamento das operações da Companhia, tais como ciberataques, destruição de servidores, restrição de acesso aos sistemas de informação, perda de informações relevantes, dentre outros;

(ii) buscar identificar fragilidades nos recursos e procedimentos empregados pela Companhia no tratamento de informações, por meio de inspeções periódicas aos parâmetros e recursos tecnológicos disponíveis;

(iii) implementar plano de ações e controles aos riscos decorrentes das fragilidades identificadas nos recursos e procedimentos empregados pela Companhia no tratamento de informações;

(iv) reportar qualquer evento relacionado ao ambiente de tecnologia da informação que possa prejudicar ou impedir o bom andamento das operações da Companhia à Diretoria e ao Comitê de Auditoria; e

(v) recomendar as ações a serem implementadas para o tratamento dos riscos em relação ao ambiente de tecnologia da informação.

5.7. Gerências e Demais Colaboradores. Compete às Gerências e demais Colaboradores, dentre outras atribuições:

(i) observar integralmente as ações de Gerenciamento de Riscos no dia a dia da Companhia; e

(ii) participar de forma ativa na comunicação e treinamento que permita a disseminação de forma consciente do Gerenciamento de Riscos na Companhia.

5.8. Os controles internos contribuem para a mitigação dos Riscos, propiciando um ambiente mais seguro e eficaz, no que tange a eficiência operacional e a integridade dos registros e informações, considerando principalmente os seguintes aspectos:

(i) os objetivos estratégicos da Companhia;

(ii) composição e natureza das contas contábeis;

(iii) possibilidade de perdas decorrentes de erros e fraudes; e

(iv) complexidade nas transações das contas contábeis.

5.9. Para atingimento dos seus objetivos, o gerenciamento dos controles internos da Companhia está estruturado em um modelo integrado de três Linhas de Defesa, sendo:

- **1ª Linha de Defesa**: representada pela Diretoria, Área de Segurança da Informação, gerências e demais Colaboradores que atuam nas operações da Companhia. Reporta-se ao Comitê de Auditoria e ao Conselho de Administração. É responsável por: (i) identificar, avaliar, monitorar e mitigar os Riscos (tratamento) de acordo com as diretrizes da Política de Gerenciamento de Riscos; (ii) implantar planos de ação e controles; e (iii) comunicar/reportar, em tempo hábil, informações relevantes relacionadas ao Gerenciamento de Riscos;

- **2ª Linha de Defesa**: Representada pelo Comitê de Auditoria e pelo Conselho de Administração, utiliza a documentação suporte produzida pela 1ª Linha de Defesa como subsídio para revisão do ambiente de controles. Atua apoiando as áreas de negócio no desenvolvimento e implementação dos processos e controles;

- **3ª Linha de Defesa**: Auditoria Interna, responsável por analisar e avaliar de forma independente o ambiente de controles internos com base nos trabalhos executados pela 1ª e 2ª linhas de defesa, fornecendo pareceres periódicos ao Comitê de Auditoria. Pode executar trabalhos adicionais conforme necessidade identificada.

5.9.1. Posteriormente, são realizados os mapeamentos e atualizações dos processos, da matriz de riscos e dos controles e testes de controle, com a finalidade de confirmar o entendimento dos processos mapeados, bem como se os controles estão implementados e operando de forma adequada.

5.9.2. Os controles inexistentes ou considerados insatisfatórios para mitigação dos Riscos identificados são reportados para as áreas responsáveis para elaboração de planos de ação (seja a criação do novo controle ou o aperfeiçoamento dos controles existentes).

5.9.3. Os processos e controles mapeados são ferramentas fundamentais para o planejamento da Auditoria Interna. Com base nesse mapeamento, a Auditoria Interna define a estratégia e os testes de efetividade que serão realizados, com o objetivo de avaliar a correta aplicação e eficiência operacional dos controles na prevenção ou detecção de distorções relevantes.

CAPÍTULO VI - VIGÊNCIA

6.1. Esta Política foi aprovada na Reunião do Conselho de Administração da Companhia realizada em 5 de outubro de 2020, terá vigência a partir da data definida na respectiva reunião e por tempo indeterminado, podendo ser modificada por deliberação do Conselho de Administração da Companhia, nos termos do item 7.3 abaixo.

CAPÍTULO VII - DISPOSIÇÕES GERAIS

7.1. Todos os Colaboradores devem manter o sigilo e a confidencialidade a respeito dos temas relativos a suas atividades e às da Companhia, devendo tratá-las sempre em observância às políticas e regimentos internos da Companhia, não podendo, em qualquer hipótese, divulgar informações relacionadas às atividades da Companhia e aos processos de Gerenciamento de Riscos.

7.2. Quaisquer dúvidas acerca das disposições desta Política e casos omissos são resolvidos pelo Conselho de Administração da Companhia.

7.3. A presente Política poderá ser alterada mediante prévia aprovação do Conselho de Administração da Companhia, sempre que se entender necessário e/ou em decorrência de alterações legislativas e regulatórias ou de documentos de governança corporativa da Companhia.

7.4. O inteiro teor desta Política será divulgado no site da Companhia (ri.meliuz.com.br) e no site da CVM (www.cvm.gov.br).