

POLÍTICA DE GESTÃO DE RISCOS DA REDE D'OR SÃO LUIZ S.A.

1. OBJETIVO, ABRANGÊNCIA E PRINCÍPIOS

- 1.1 A presente Política de Gestão de Riscos da Rede D'Or São Luiz S.A. ("Companhia") ("Política") tem por objetivo estabelecer os princípios, diretrizes, conceitos, ações e responsabilidades a serem observados pelos administradores da Companhia no processo interno de gerenciamento de eventos incertos que possam causar impactos negativos no cumprimento dos objetivos da Companhia, de forma a possibilitar a adequada identificação, avaliação, tratamento, monitoramento, análise crítica e comunicação dos riscos existentes na Companhia.
- 1.2 A Política é aplicável à Companhia e às suas controladas, no Brasil e no exterior, incluindo as unidades assistenciais, clínicas oncológicas, laboratórios, áreas corporativas e outros negócios da Companhia ("Unidades").
- 1.3 O processo de gestão de riscos da Companhia foi definido com base nos seguintes princípios:
- (i) agregar valor e proteger o ambiente institucional;
 - (ii) contribuir para o alcance dos objetivos e metas da organização;
 - (iii) ser parte integrante dos processos da organização;
 - (iv) atuar como segunda linha de defesa contra os riscos corporativos em resguardo e subsídio às Unidades;
 - (v) fomentar a cultura de prevenção de riscos e incidentes;
 - (vi) subsidiar a tomada de decisões;
 - (vii) ser sistemática, interdisciplinar, estruturada e oportuna;
 - (viii) ser baseada nas melhores informações disponíveis;
 - (ix) estar alinhada com o contexto da organização e com o perfil de risco;
 - (x) considerar os fatores humanos;
 - (xi) ser transparente e participativa;
 - (xii) ser dinâmica, interativa e passível de mudança;
 - (xiii) apoiar a melhoria contínua da organização; e
 - (xiv) ser devidamente relatada e adequadamente registrada.
- 1.4 Com base nas classificações de suas matrizes de riscos, as Unidades devem promover ações de tratamento, com base na hierarquização na forma do item 4.5.1 abaixo. Em especial as Unidades posicionadas no quadrante de "Alto Risco", devem realizar tratativas dos riscos através de Planos de Ação (conforme abaixo definido), a fim de promover ações de mitigação em especial para os riscos que originem tal classificação. Para todas estas Unidades, devem ser realizadas Auditorias Especiais (conforme abaixo definido), com o objetivo de averiguar a eficiência dos planos de ação adotados.

- 1.5 Todas as Unidades e áreas de negócio da Companhia devem conhecer e tratar seus riscos, a fim de mitigá-los, cabendo à Diretoria de Riscos e Controles Internos, o papel de segunda linha de defesa.
- 1.6 A Diretoria de Riscos e Controles Internos deve elaborar o "Relatório Anual de Gestão de Riscos" contendo um sumário executivo das atividades realizadas nos últimos 12 (doze) meses e submeter à apreciação do Comitê de Auditoria.

2. APROVAÇÃO

- 2.1 Compete exclusivamente ao conselho de administração da Companhia aprovar quaisquer alterações à presente Política.

3. CONCEITOS

"Auditorias Especiais" tem o significado previsto no item 4.3 abaixo, inciso (iii) desta Política.

"Auditorias Programadas" tem o significado previsto no item 4.3 abaixo, inciso (ii) desta Política.

"Companhia" tem o significado previsto no item 1.1 acima desta Política.

"Evento" significa um incidente ou ocorrência de fontes internas ou externas que pode causar impacto negativo (riscos negativos), positivo (riscos positivos ou oportunidades) ou ambos sobre os objetivos da Companhia e/ou de suas controladas.

"Gestão de Riscos" significa a estrutura personalizada, integrada e interdisciplinar. É concebida de forma inclusiva, abrangente e planejada de forma gradual, focada nas atividades significativas e funções da Companhia. Considera limitações, incertezas, expectativas, fatores humanos e culturais na identificação, análise, avaliação e tratamento dos riscos em seu escopo, contexto e critério.

"Matriz de Risco" tem o significado previsto no item 4.5(i) desta Política.

"Plano de Ação" tem o significado previsto no item 4.5.4 abaixo desta Política.

"Política" tem o significado previsto no item 1.1 acima desta Política.

"Risco" significa o efeito da incerteza nos objetivos ou a possibilidade de que um evento ocorra e afete, positivamente ou negativamente, os objetivos.

"Riscos Corporativos": significa os riscos existentes em uma organização. Possuem níveis (estágios) e naturezas distintas. É específico e dinâmico a cada cenário, podendo emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem.

"Relatório de Avaliação de Riscos" tem o significado previsto no item 4.4.4 abaixo desta Política.

"SESMT" tem o significado previsto no item 4.3.2 abaixo desta Política.

"Unidades" tem o significado previsto no item 1.2 desta Política.

4. PROCESSO DE GESTÃO DE RISCOS

- 4.1 Tipos de Riscos. Os riscos identificados pela Companhia são classificados como:

- (i) Risco de Crédito: consiste no risco de a Companhia e as suas controladas sofrerem perdas decorrentes da inadimplência de seus clientes, de instituições financeiras depositárias de recursos de caixa e equivalentes de caixa ou contrapartes de seus instrumentos financeiros;
- (ii) Risco de Liquidez: consiste no risco de a Companhia e suas controladas não disporem de recursos suficientes para cumprir com suas obrigações associadas aos passivos financeiros que serão liquidados com caixa e equivalentes de caixa ou aplicações financeiras, tais como o saldo de fornecedores, empréstimos, financiamentos e debêntures, salários, provisões e encargos sociais a recolher, contas a pagar por aquisições e outros passivos;
- (iii) Risco de Taxa de Juros: consiste no risco relacionado à variação das taxas de juros que a Companhia e as suas controladas estão expostas, uma vez que possuem aplicações financeiras, empréstimos, financiamentos e debêntures contratados em moedas locais e sujeitos às flutuações dos índices previstos nos referidos contratos que formalizaram tais operações, principalmente da taxa médias diárias dos DI – Depósitos Interfinanceiros de um dia (Taxa DI), do Índice Nacional de Preços ao Consumidor Amplo (IPCA) ("IPCA") e da Taxa de Juros de Longo Prazo ("TJLP");
- (iv) Risco Cambial: consiste no risco de o valor justo dos fluxos de caixa futuros de um instrumento financeiro flutuar devido a oscilações em moeda estrangeira;
- (v) Risco de Conformidade: consiste no risco de imposição de sanções legais ou regulatórias, de perda financeira ou de reputação que a Companhia pode sofrer como resultado do descumprimento de leis, acordos, regulamentos, código de conduta e das políticas e procedimentos internos. Incluem-se aqui, por exemplo, os riscos de fraudes em demonstrações financeiras e de desvios de ativos, de corrupção e de crimes cibernéticos;
- (vi) Risco Estratégico: consiste nos riscos associados à estratégia da Companhia na busca de criação, proteção e crescimento de valor. São causados por eventos de mudanças no ambiente externo, tais como político, econômico e social, mercado, competidores, fusões e aquisições, disponibilidade, inovações, tecnologias e portfólio de produtos e/ou serviços e também pela qualidade na gestão de eventos internos relativos às suas finanças e operações;
- (vii) Risco Operacional: decorre da inadequação ou falha na gestão de processos internos e pessoas que possam dificultar ou impedir o alcance dos objetivos da Companhia. Estes riscos estão associados tanto à operação do negócio (como a prestação dos serviços de saúde); quanto à gestão de áreas de suporte ao negócio (como contabilidade, controladoria, controles internos, suprimentos, tecnologia da informação etc.);
- (viii) Risco Cibernético: possibilidade de determinada ameaça explorar vulnerabilidades de um ativo ou um conjunto de ativos, impactando na confidencialidade, integridade e disponibilidade das informações;
- (ix) Risco Tecnológico: possibilidade de determinada ameaça explorar vulnerabilidades de um ativo ou um conjunto de ativos, impactando na confidencialidade, integridade e disponibilidade das informações. A Companhia coleta e armazena em sua rede

informações sensíveis, incluindo propriedade intelectual, informações comerciais e informações pessoais de seus pacientes e funcionários. A manutenção segura destas informações e tecnologia é fundamental para as operações da Companhia;

- (x) Risco Regulatório/Legal: possibilidade de que leis ou regulamentos, inclusive suas modificações ou não observância total ou parcial, possam trazer impactos estratégicos, de imagem e/ou financeiros para a Companhia e suas controladas, e/ou afetar significativamente a habilidade da Companhia e suas controladas em administrar eficientemente os seus negócios; e
- (xi) Risco Socioambiental: risco de perdas em consequência de efeitos negativos no meio-ambiente e na sociedade decorrentes de impacto ambiental, impactos em povos e comunidades nativas e proteção da saúde humana, de propriedades culturais e da biodiversidade.

4.2 Processo de Avaliação dos Riscos: A avaliação dos riscos da Companhia e de suas controladas é estruturada por meio das seguintes etapas: (i) identificação dos riscos; (ii) análise e avaliação dos riscos; (iii) tratamento dos riscos; (iv) monitoramento e análise crítica dos riscos; e (v) registro e relato às partes interessadas (*stakeholders*).

4.3 Identificação de Riscos. A Companhia identifica eventos que podem impactar seus objetivos e estratégia, considerando os contextos em que estão inseridos, por meio da utilização das seguintes técnicas:

- (i) Matriz de Risco: Com base nos registros e relatos fruto da identificação dos riscos, a Diretoria de Riscos e Controles Internos elabora conjunto de análises de natureza técnica que combina classificações qualitativas e quantitativas, a fim de produzir níveis ou classificações de riscos para orientar na construção das medidas para a tratativa de respostas aos riscos a serem adotadas pela Companhia ("Matriz de Risco"). Desta forma, a Matriz de Risco serve de subsídio à Diretoria de Riscos e Controles Internos na avaliação da necessidade de adequação dos riscos identificados, e seus respectivos impactos em função da probabilidade de efetivação dos riscos;
- (ii) Auditorias Programadas: Consistem em auditorias programadas realizadas com a finalidade de revisar a Matriz de Riscos com base em roteiro ligado a avaliação necessária e com a checagem de ações pendentes em planos de ações ligados aos potenciais riscos verificados ("Auditorias Programadas"). As Auditorias Programadas são realizadas anualmente ou caso haja necessidade de avaliação ligada à Matriz de Risco;
- (iii) Auditorias Especiais: Consistem em auditorias não-programadas realizadas com a finalidade de verificar *in loco* o cenário atribuído aos potenciais riscos de forma mais específica e/ou em caráter extraordinário com base em roteiro ligado a avaliação necessária e com a checagem de ações pendentes em planos de ações ligados aos potenciais riscos verificados ("Auditorias Especiais"). As Auditorias Especiais poderão ser realizadas nas seguintes situações: (a) análise e avaliação mensal dos principais fatores de risco no caso de riscos classificados no quadrante superior direito da Matriz de Risco, na forma descrita no item 4.4.1 abaixo, relacionados às

- Unidades da Companhia; (b) investigação dos incidentes e os principais fatores que desencadearam a ocorrência do riscos indicados no item 4.2 acima, inciso (iii)(a); e
- (iv) Investigação de Incidentes: Consiste no processo de análise de incidentes com a finalidade de verificar as principais vulnerabilidades e fatores contribuintes ("Investigação de Incidentes"). Durante uma Investigação de Incidente, a Diretoria de Riscos e Controles Internos pode identificar riscos, propor ações para a mitigação de tais riscos e aprimorar a gestão de riscos corporativos.
- 4.3.1 As Auditorias Programadas e Auditorias Especiais podem ser realizadas tanto pela Diretoria de Riscos e Controles Internos quanto pela área de Segurança Física da Companhia, desde que devidamente treinadas e capacitadas.
- 4.3.2 A realização das Auditorias Programadas, Auditorias Especiais e Investigação de Incidentes dependerá da participação de pelo menos um dos seguintes colaboradores da Companhia vinculados às Unidades da Companhia nos quais tenham sido verificados potenciais riscos: representante do serviço especializado em engenharia de segurança e em medicina do trabalho ("SESMT"), representante da área de Segurança Física da Companhia e/ou representante da área de Qualidade da Companhia.
- 4.4 Análise e Avaliação dos Riscos: A Companhia analisa e avalia os riscos identificados, classificando-os em quadrantes ligados ao nível de criticidade.
- 4.4.1 *Análise do impacto em função da probabilidade (Matriz de Risco)*: Uma vez identificados e/ou revisados os fatores de risco, a Diretoria de Riscos e Controles Internos realiza a análise da probabilidade de ocorrência e o impacto do risco avaliado para cada Unidade da Companhia e aloca os referidos riscos no quadrante referente ao seu grau de risco.
- 4.4.2 *Análise do Impacto*: No processo de alocação dos riscos na Matriz de Riscos, os impactos são baseados nos seguintes critérios:
- (i) Financeiro: Baseado no somatório das importâncias seguradas para danos materiais e lucros cessantes de cada Unidade da Companhia, ordenando-se do maior para o menor. Estes dados são fornecidos pela área financeira da Companhia;
- (ii) Imagem: As Unidades da Companhia são escalonadas por ordem decrescente de impacto de imagem para a Companhia, conforme definido pela Diretoria de Riscos e Controles Internos;
- (iii) Vida: Baseado no somatório de pessoas que circulam nas Unidades da Companhia (população fixa e flutuante). Estes dados são fornecidos pela área de Segurança Física da Companhia; e
- (iv) Licenciamento: Avaliação do status de atualização/regularização das licenças pertencentes às Unidades da Companhia. Estes dados são fornecidos pela área de Licenciamento da Companhia.
- 4.4.3 *Análise de Probabilidade*: Para a composição deste eixo são consideradas avaliações de itens pertinentes ao risco avaliado especificamente de forma a alocar as Unidades em quartis (100%, 75%, 50% e 25%).
- 4.4.4 *Relatório de Avaliação de Riscos (RAR)*: Consiste na avaliação de risco voltada para instalações e/ou equipamentos através da realização de estudo técnico ("Relatório de

Avaliação de Riscos"). O Relatório de Avaliação de Riscos deve ser encaminhados às Unidades e às áreas corporativas relacionadas ao assunto da Companhia para a mitigação dos riscos.

- 4.5 Tratamento dos Riscos: A Companhia define ações e medidas de tratamento do risco, visando a modificação do nível do risco.
- 4.5.1 Matriz de Risco: A Companhia adota as seguintes respostas aos riscos identificados
- (i) Otimizar (Reter): Aprimorar o nível do risco expresso por ajustes em termos da combinação dos seus impactos e probabilidades, evoluindo continuamente o seu desempenho em termos de sua avaliação de sua significância;
 - (ii) Certificar (Assegurar): Promover garantias que assegurem e melhorem a eficiência de resultados na configuração de significância (critérios) do nível do risco no cenário assumido;
 - (iii) Acompanhar (Controlar): Observar de forma crítica e contínua, a fim de identificar mudanças (vulnerabilidades) nos níveis esperados da configuração de significância do risco, buscando evolução no seu nível de classificação; e
 - (iv) Mitigar (Reduzir): Abrandar ou minimizar o nível do risco constatado (tender a zero), tomando ações eficazes junto aos efeitos adversos identificados.
- 4.5.2 Na medida em que ocorra a evolução da gestão de riscos com a abordagem de riscos elencados a outras naturezas, a Companhia deverá considerar as seguintes respostas: (i) retenção; (ii) compartilhamento; (iii) transferência; e (iv) ações para assumir riscos, dependendo do seu contexto estratégico.
- 4.5.3 A atualização da Matriz de Riscos deverá ser refletida no roteiro e/ou checklist das Auditorias Programadas ou Auditorias Especiais.
- 4.5.4 Plano de Ação: Baseado nos resultados das Auditorias Programadas ou Auditorias Especiais, um plano de ação é elaborado pela própria Unidade para o devido tratamento dos riscos ("Plano de Ação"). No Plano de Ação deverá constar a ação que será executada, a área responsável pela ação a ser desenvolvida, o prazo para a execução, identificação dos recursos necessários e o status de cada ação planejada. O Plano de Ação, após concluído, é enviado imediatamente a Diretoria de Riscos e Controles Internos para possíveis orientações e acompanhamento.
- 4.5.5 Avaliação de Normas: Consiste na avaliação das normas da Companhia relacionadas às áreas de SESMT, Segurança Física e de Infraestrutura, Manutenção e Operação, a fim de verificar os alinhamentos necessários com as normas de risco, bem como os devidos papéis e responsabilidades na execução das atividades em vigor. Caso necessário, deve ser proposto complementação de conteúdo ligados a ações para a mitigação de possíveis riscos.
- 4.5.6 Treinamentos: Os colaboradores envolvidos nos riscos identificados deverão participar de treinamentos com a finalidade de garantir a implementação das diretrizes previstas nesta Política, conforme matriz de treinamento a ser elaborado pela Diretoria de Riscos e Controles Internos ("Treinamento").

4.5.7 A Diretoria de Riscos e Controles Internos realizará nas Auditorias Programadas avaliação da aplicabilidade do Treinamento e de sua disseminação, sugerindo no relatório, quando necessário, recomendações.

5. INSTRUMENTOS PARA MITIGAÇÃO DE RISCOS

5.1 A Companhia possui os seguintes instrumentos para mitigação de seus principais riscos:

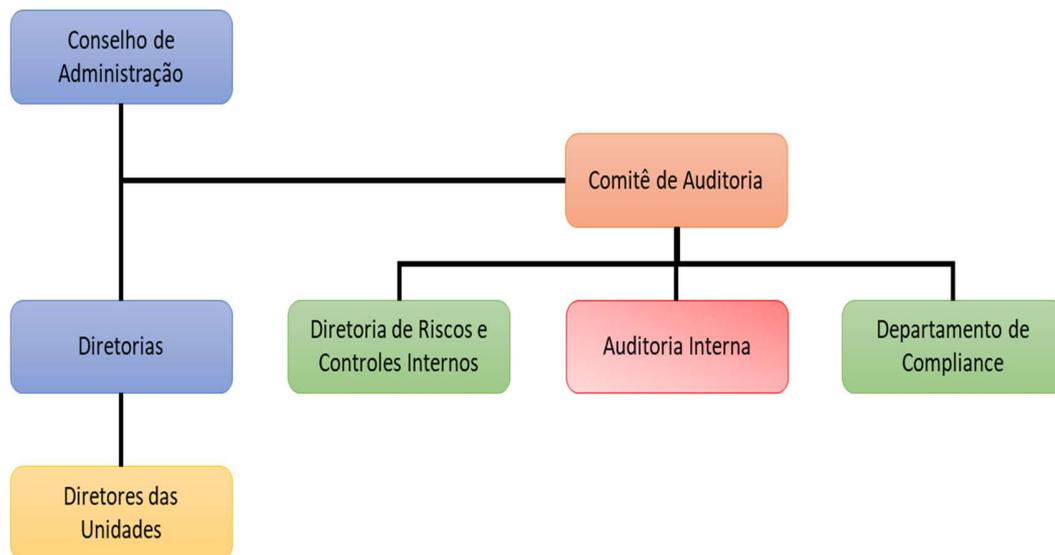
- (i) Risco de Crédito: o gerenciamento é realizado por meio de análises periódicas do nível de inadimplência dos clientes, bem como adoção de formas eficazes de cobrança. A Companhia assume o risco de crédito dos clientes seguindo critérios definidos com base em modelos estatísticos, combinados com informações internas própria do nosso negócio, assim como informações internas, sendo esses modelos periodicamente revisados com base nos índices de perdas históricas das safras da carteira. Com relação ao risco de crédito relacionado às instituições financeiras depositárias de recursos de caixa e equivalentes de caixa ou contrapartes de seus instrumentos financeiros, a Companhia prioriza a contratação de instituições financeiras de primeira linha, bem como monitora periodicamente a solidez e higidez de tais instituições financeiras e contrapartes de seus instrumentos financeiros no momento de sua contratação;
- (ii) Risco de Liquidez: o gerenciamento é realizado por meio do monitoramento contínuo dos fluxos de caixa previstos e reais e pela manutenção de relacionamento próximo com instituições financeiras, com frequente divulgação de informações para suportar decisões de crédito, quando da necessidade de recursos externos. Além disso, a Companhia não efetua aplicações financeiras de caráter especulativo e com alto risco financeiro;
- (iii) Riscos de Mercado: o departamento financeiro monitora as oscilações de taxas de juros e do câmbio que possam impactar os resultados financeiros e operacionais da Companhia, bem como contrata operações de derivativos com instituições financeiras de primeira linha com a finalidade de proteção patrimonial (*hedge*). As operações com derivativos são realizadas para a finalidade de proteção contra (i) oscilações em taxa e moeda estrangeira, para regular operações de *swap* cambial, em que a exposição decorrente da variação em moeda estrangeira é trocado pela exposição de uma taxa de juros em moeda funcional (Real); e (ii) variações de taxas de juros, para regular operações de *swap* de taxa de juros, em que a exposição decorrente de taxas de juros é trocado pela exposição decorrente de uma taxa de juros prefixada;
- (iv) Risco de Conformidade: monitoramento contínuo pela Diretoria de Riscos e Controles Internos e por prestadores de serviços terceirizados de novas leis e regulamentos aos quais a Companhia está ou possa vir a estar sujeita. Quando da identificação de fatos relevantes que podem influenciar as operações da Companhia, a Diretoria de Riscos e Controles Internos compartilha tais fatos em reunião da diretoria para definição de Plano de Ação, se necessário;
- (v) Risco Estratégico: todo final de exercício, a Companhia reúne todos os seus executivos e profissionais chave para definição do planejamento estratégico do ano

seguinte, assim como seu orçamento previsto. Para suporte à execução da estratégia, a Companhia possui programa de participação nos lucros e resultados para as pessoas-chave de sua administração com o objetivo de premiar o alcance e superação das metas pela Companhia, alinhada ao desempenho, sustentabilidade e à estratégia de crescimento do negócio da Companhia em cada exercício social. Há reuniões periódicas de avaliação de resultados onde são discutidos indicadores de desempenho relacionados às metas e definidos planos de ação para correção do curso das operações em rumo ao cumprimento das metas;

- (vi) Risco Operacional: a Companhia possui auditoria interna que, no decorrer do exercício, efetua testes nos controles internos para assegurar sua eficiência e eficácia. Dentre as funções das auditorias está julgar se a forma como os controles internos foram desenhados é suficiente para mitigação dos riscos operacionais até um nível aceitável pela Companhia. Quando identificadas fragilidades nos controles internos, os auditores recomendam melhorias que são validadas pelo comitê de auditoria e implementadas pelos gestores dos processos. A equipe de auditoria interna acompanha o andamento dos planos de ação para correção das falhas nos controles até a sua conclusão, e se reporta ao comitê de auditoria ou diretamente ao conselho de administração. Além disso, há acompanhamento mensal de indicadores de desempenho dos processos organizacionais nas reuniões mensais de resultado. Para indicadores com desempenho insatisfatório, são criados planos de ação para correção das situações identificadas;
- (vii) Risco Cibernético e Tecnológico: para reforço da segurança de sua infraestrutura de tecnologia e sistemas de informação, a Companhia conta com área de TI própria cuja função é a de efetuar a revisão dos controles internos relacionados a TI com o objetivo de aumento da segurança dos sistemas de informação por meio de aprimoramento dos controles internos;
- (viii) Risco Regulatório/Legal: monitoramento contínuo pelo Departamento Jurídico e/ou por assessores jurídicos terceirizados do cumprimento de leis e regulamentos aos quais a Companhia está sujeita e de eventuais situações, fatos, notícias que possam afetar as operações ou a imagem da Companhia; e
- (ix) Risco Socioambiental: monitoramento contínuo pelo Departamento Jurídico e/ou por assessores jurídicos terceirizados dos efeitos potenciais ou efetivos gerados pelas atividades da Companhia, em especial projetos *greenfield* e *brownfield* desenvolvidos pela Companhia, no meio-ambiente e na sociedade.

6. ATRIBUIÇÕES E RESPONSABILIDADES

- 6.1 São responsáveis pela execução e acompanhamento desta Política, o conselho de administração, o comitê de auditoria, a Diretoria de Riscos e Controles Internos, o Departamento de *Compliance* e a auditoria interna.



6.2 Competirá ao conselho de administração:

- (i) aprovar esta Política e suas revisões;
- (ii) promover e incentivar a cultura de Gestão de Riscos na Companhia;
- (iii) apoiar as ações propostas para mitigação dos fatores de riscos que estejam com baixa adesão, sob o ponto de vista das Auditorias Programadas e técnicas;
- (iv) assegurar que a gestão de riscos esteja integrada em todas as atividades da Companhia;
- (v) assegurar que os recursos necessários sejam alocados para gerenciar riscos;
- (vi) atribuir/delegar autoridades e responsabilidades nos níveis apropriados dentro da Companhia;
- (vii) monitorar e reavaliar periodicamente os riscos estratégicos e de imagem; e
- (viii) reavaliar, junto ao comitê de auditoria e a Diretoria de Riscos e Controles Internos, a adequação da estratégia de riscos da Companhia.

6.3 Competirá ao comitê de auditoria:

- (i) opinar na contratação e destituição dos serviços de auditoria independente;
- (ii) avaliar as informações trimestrais, demonstrações intermediárias e demonstrações financeiras;
- (iii) avaliar e monitorar as exposições de risco da Companhia;
- (iv) avaliar, monitorar, e recomendar à administração da Companhia a correção ou aprimoramento desta Política; e
- (v) acompanhar as atividades da auditoria interna, da Diretoria de Riscos e Controles Internos e do Departamento de *Compliance*.

- 6.4 **Os Diretores das Unidades e demais colaboradores, como primeira linha de defesa,** reportam-se à Diretoria e são responsáveis por:
- (i) garantir a implantação e implementação desta Política;
 - (ii) aprovar e disponibilizar para a Diretoria de Riscos e Controles Internos os Planos de Ação;
 - (iii) consultar a Diretoria de Riscos e Controles Internos em apoio a suas ações sempre que se fizer necessário; e
 - (iv) operacionalizar as ações planejadas.
- 6.5 **A Diretoria de Riscos e Controles Internos, como segunda linha de defesa,** reporta-se ao Comitê de Auditoria, e é responsável por:
- (i) promover o desenvolvimento e a revisão da Política;
 - (ii) promover o desenvolvimento e a revisão dos parâmetros e critérios utilizados na elaboração da Matriz de Riscos que subsidiam o método de gestão desenvolvido;
 - (iii) promover o desenvolvimento e a revisão de métodos de trabalho para a implantação e implementação desta Política e da metodologia no âmbito interno da Companhia;
 - (iv) fazer cumprir esta Política em todas as Unidades;
 - (v) propor normas e planos relacionados a gestão dos riscos corporativos, de acordo com a hierarquização de tratativa dos mesmos;
 - (vi) apoiar os setores corporativos na elaboração de normas, planos e procedimentos que envolvam assuntos relacionados a gestão de riscos;
 - (vii) validar documentos relacionados às diretrizes de riscos corporativos, a fim de verificar os alinhamentos necessários, bem como os devidos papéis e responsabilidades na execução das atividades;
 - (viii) propor ações para a tratativa de riscos nos diversos níveis e hierarquias de riscos sempre que identificados;
 - (ix) realizar as Auditorias Programadas anualmente em todas as unidades, visando atualizar os fatores de riscos que compõem a Matriz de Riscos;
 - (x) realizar Auditorias Especiais a fim de apontar/acompanhar a mitigação dos principais fatores de risco e durante a investigação de incidentes, nos casos aplicáveis;
 - (xi) elaborar e divulgar os relatórios das Auditorias Especiais para os Diretores, bem como para a área de auditoria interna e para o comitê de auditoria, solicitando providências/plano de ação para as não conformidades identificadas;
 - (xii) acompanhar os planos de ações estabelecidos pelas Unidades para a correção e tratamento das não conformidades;
 - (xiii) elaborar o portfólio de gestão de riscos por meio de Relatórios de Avaliação de Risco acerca de estudos técnicos sobre instalações e/ou equipamentos como método complementar em apoio as unidades;

- (xiv) avaliar e monitorar as exposições de risco da Companhia, acompanhando e supervisionando o processo de gerenciamento de riscos;
- (xv) administrar de forma proativa os riscos, por meio do recebimento regular de informações que sinalizem o nível de exposição ao risco;
- (xvi) definir os limites de tolerância aos riscos que a Companhia está exposta;
- (xvii) reportar ao comitê de auditoria os eventos de riscos identificados; e
- (xviii) manter registros de suas deliberações e decisões.

6.6. **O Departamento de Compliance compõe também a segunda linha de defesa** e reporta-se ao Comitê de Auditoria, sendo responsável por:

- (i) supervisão, monitoramento e funcionamento e da eficiência dos mecanismos e procedimentos internos de integridade da Companhia;
- (ii) adotar procedimento de *due diligence* previsto na Norma de *Due Diligence* Anticorrupção para Fusões e Aquisições – NORDOR-039, a qual objetiva a verificação e mitigação de riscos reputacionais e de corrupção que possam, de alguma forma, impactar negativamente o negócio e/ou a imagem da Companhia;
- (iii) implementação da Política de Transação com Partes Relacionadas e fiscalização do cumprimento de suas disposições; e
- (iv) monitorar e assegurar o cumprimento do código de conduta da Companhia, a fim de evitar eventuais conflitos de interesses entre a Companhia e suas partes relacionadas, em virtude das relações comerciais estabelecidas entre as partes.

6.7. **A auditoria interna, como terceira linha de defesa**, é responsável por aferir a qualidade e a efetividade dos processos de gerenciamento de riscos e controles internos, sugerindo alterações ao Conselho de Administração e à Diretoria de Riscos e Controles Internos, quando necessário.

6.7.1. A auditoria interna atua de forma independente e objetiva, reportando-se periodicamente ao comitê de auditoria e ao conselho de administração, ou quando julgar necessário. As atribuições da área de auditoria interna e a suficiência da sua estrutura e orçamento ao desempenho de suas funções são aprovadas pelo conselho de administração da Companhia.

7. DISPOSIÇÕES GERAIS

7.1 A presente Política somente entrará em vigor e seus termos e condições passarão a ter eficácia a partir da data de entrada em vigor do Contrato de Participação no Novo Mercado, a ser celebrado entre a Companhia e a B3 S.A. – Bolsa, Brasil e Balcão e permanecerá em vigor por prazo indeterminado.