KORA SAÚDE PARTICIPAÇÕES S.A.

POLÍTICA DE GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS

1. OBJETIVO

1.1. Esta Política de Gerenciamento de Riscos e Controles Internos ("Política") tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observados no processo de gerenciamento de riscos e controles internos inerentes às atividades de negócio da Kora Saúde Participações S.A. ("Companhia"), de forma a identificar e monitorar os riscos relacionados à Companhia ou seu setor de atuação, além de garantir a permanente aderência da Companhia e suas controladas referente às suas atividades e aos padrões ético e profissionais, que devem ser cumpridos pelos Colaboradores e Terceiros que, em virtude de suas funções, tenham acesso a informações relevantes sobre a Companhia, seus clientes e estratégias.

2. ABRANGÊNCIA

2.1. Esta Política aplica-se à Companhia e suas controladas, bem como a todos os empregados, gerentes, diretores estatutários e não estatutários, membros do Conselho de Administração, membros de comitês, membros do Conselho Fiscal (se aplicável), Colaboradores, representantes e Terceiros, direta ou indiretamente relacionados com a Companhia e suas controladas.

3. CONCEITOS

3.1. Para fins de aplicação desta Política, os seguintes conceitos devem ser utilizados:

- Colaboradores: consideram-se os estagiários, funcionários, diretores, conselheiros e acionistas.

- Limite (ou apetite) do Risco: é a exposição e/ou impacto máximo do Risco que a Companhia está disposta a aceitar, na busca dos seus objetivos e geração de valor. Nem todos os tipos de Riscos são passíveis de aceitação. Portanto, a proposta de limites deverá obrigatoriamente ser fundamentada e formalizada pelas seguintes análises: (i) avaliação do retorno tangível e intangível relacionado ao limite de Risco proposto; (ii) capacidade da Companhia de suportar o impacto do limite de Risco proposto (iii) decisão se o Risco deve ou não ser aceito conforme sua tipologia; (iv) viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do Risco e respectivo retorno; e (v) disponibilidade de recursos (investimento e esforço) para implantação.

- Matriz/Modelagem de Riscos: visa estabelecer uma comparação individual dos Riscos a partir graus de impacto e probabilidades de ocorrência para fins de priorização e gestão. A matriz de riscos é um organismo em constante evolução e

atualizada, sempre que necessário e tempestivamente com o surgimento de eventos de Risco emergentes.

- Risco(s): a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos da sociedade.

- Terceiros: prestadores de serviço e fornecedores.

4. REFERÊNCIAS

4.1. Esta Política tem como referências: (i) as regras de governança corporativa do Estatuto Social da Companhia e dos Regimentos Internos do Conselho de Administração e do Comitê de Auditoria e *Compliance*; (ii) o Código de Ética e Conduta da Companhia; (iii) a Política de Divulgação de Informações e de Negociação de Valores Mobiliários; (iv) a Política de Transações com Partes Relacionadas e Administração de Conflitos de Interesse; (v) o Código Brasileiro de Governança Corporativa – Companhias Abertas; e (vi) o Regulamento do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão.

5. DIRETRIZES

5.1. A Companhia está comprometida com a dinâmica de gerenciamento de Riscos, de forma a preservar e desenvolver seus valores, ativos, reputação, competitividade e perenidade dos negócios.

5.2. O objetivo da gestão de Riscos é entendê-los, avaliar e definir ações de resposta para que eventuais perdas sejam previstas e reduzidas, visando manter os Riscos em níveis aceitáveis. A análise de Riscos deve auxiliar o processo de tomada de decisão nos diversos níveis de gestão da Companhia.

5.3. O gerenciamento de Riscos contribui para o monitoramento e para a realização dos objetivos da Companhia. A abordagem da Companhia é integrar o gerenciamento de Riscos no dia a dia na conduta dos seus negócios por meio de um processo estruturado.

5.4. Os riscos são estruturados de acordo com a seguinte classificação:

(a) Estratégico: são riscos associados com as decisões estratégicas da Companhia para atingir os seus objetivos de negócios, e/ou decorrentes da falta de capacidade ou habilidade;

(b) Operacional: riscos relacionados à operação da Companhia (processos, pessoas e tecnologia), que afetam a eficiência operacional e utilização efetiva e eficiente de recursos, que tornem impróprio o exercício das atividades da Companhia e decorrem de falha, deficiência ou inadequação de processos internos, pessoas e sistemas ou de eventos externos. Podem se manifestar de diversas maneiras, como por exemplo, atos fraudulentos, interrupção do negócio, conduta incorreta de empregados, incapacidade produzir e/ou distribuir seus produtos nas condições e prazos estabelecidos, resultando

em perdas financeiras, comerciais, multas fiscalizatórias e/ou impactos jurídicos e reputacionais;

(c) Imagem: Perda de credibilidade e reputação perante os clientes, concorrentes, fornecedores, órgãos governamentais, mercado de atuação ou comunidade, decorrentes de ações, atos e atitudes indevidas e impróprias;

(d) Financeiro: está associado à exposição das operações financeiras/contábeis da Companhia e confiabilidade do balanço patrimonial. Pode se materializar em decorrência da não efetividade na administração dos fluxos de caixa visando a maximização e a geração de caixa operacional, retornos das transações financeiras, captação/aplicação de recursos financeiros, possibilidade de emissão de relatórios financeiros, gerenciais e fiscais incompletos, não-exatos ou intempestivos, expondo a Companhia à multas e penalidades;

(e) Legal, Regulatório e/ou de *Compliance*: riscos relacionados ao cumprimento de normas e legislação, considerando leis aplicáveis ao setor de atuação, leis gerais, nacionais e internacionais (ambiental, trabalhista, cível e tributário/ fiscal), acordos, regulamentos, código de conduta e/ou demais políticas e perda de reputação e má formalização de operações (por exemplo, com órgãos reguladores, operações em desacordo com as políticas e procedimentos internos ou lavagem de dinheiro;

(f) 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;

(g) Risco de Imagem: possibilidade de ocorrência de evento, geralmente ocasionado por outros riscos, que possa causar danos à reputação, credibilidade ou marca da Companhia, inclusive em razão de publicidade negativa, verdadeira ou não;

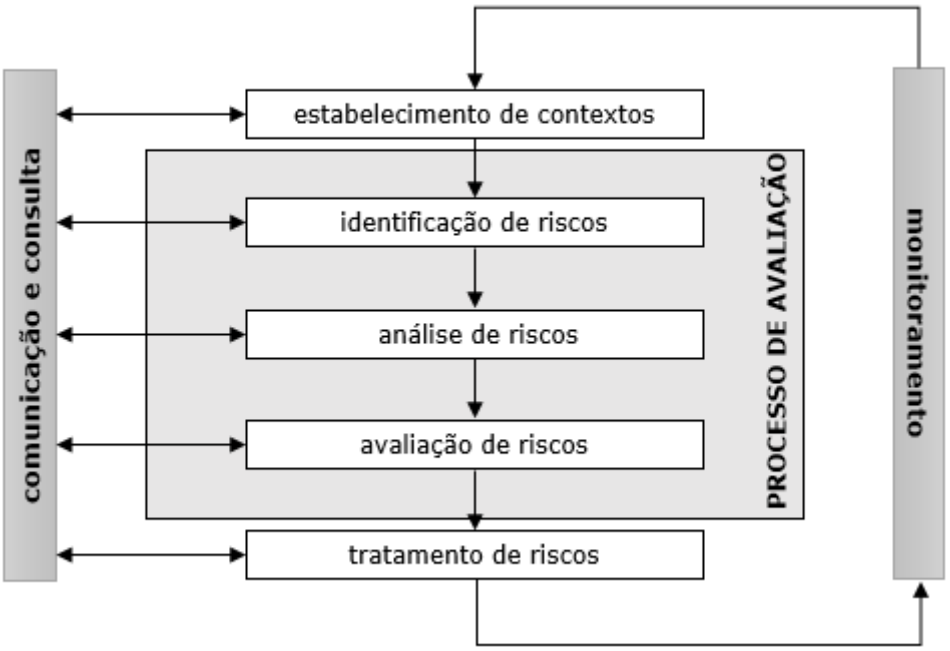
5.5. As Modelagens de Risco devem compor as ferramentas de análise e apoio às decisões da Diretoria, cabendo à área de Gestão de Riscos e Controles Internos da Companhia fornecer o apoio necessário à Diretoria para o desenvolvimento da gestão de Riscos e controles internos.

5.6. É fundamental o entendimento e disseminação entre os órgãos e executivos envolvidos da correta diferenciação de impactos causados por eventos e situações que não envolvem diretamente a gestão de Riscos como: (i) falhas de controles internos em processos; (ii) decisões estratégicas malsucedidas; ou (iii) falha na governança. Este entendimento visa aperfeiçoar e fortalecer o modelo de governança corporativa da Companhia.

5.7. Todos os Riscos, bem como os limites aprovados, deverão ser formalizados em relatórios detalhados, explicativos, com planos de ação, se for o caso, bem como a identificação dos responsáveis e prazos de conclusão dos planos de ação.

6. Processo de Gerenciamento

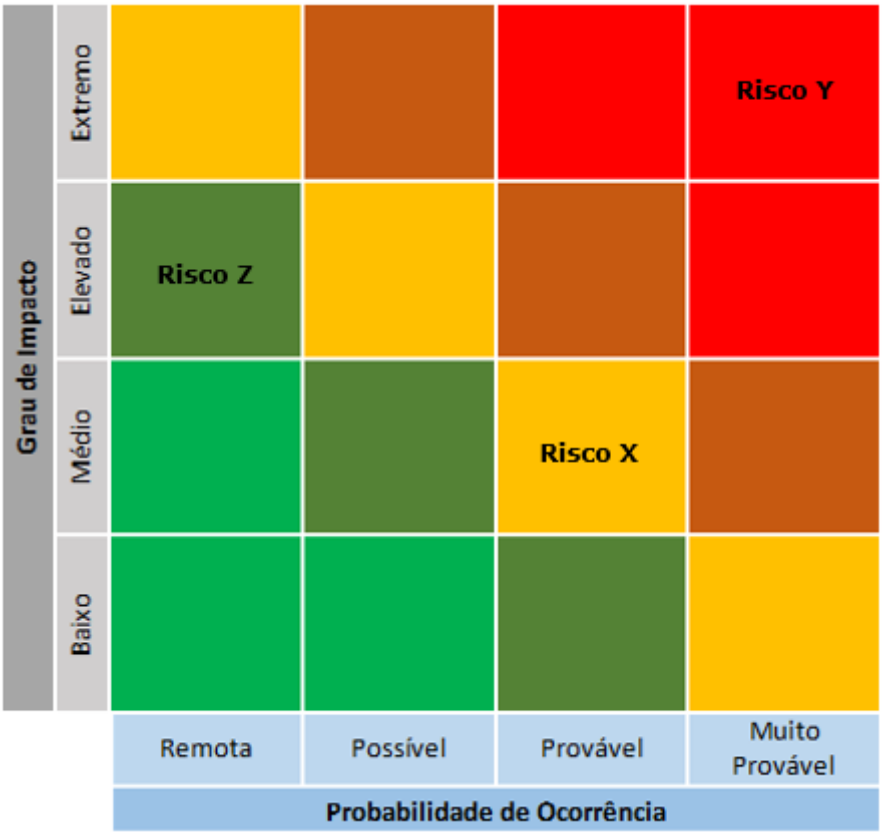
6.1. O processo de gerenciamento de Riscos adotado pela Companhia foi elaborado à luz do disposto no "ISO 31000:2009 – Princípios e Diretrizes da Gestão de Riscos":



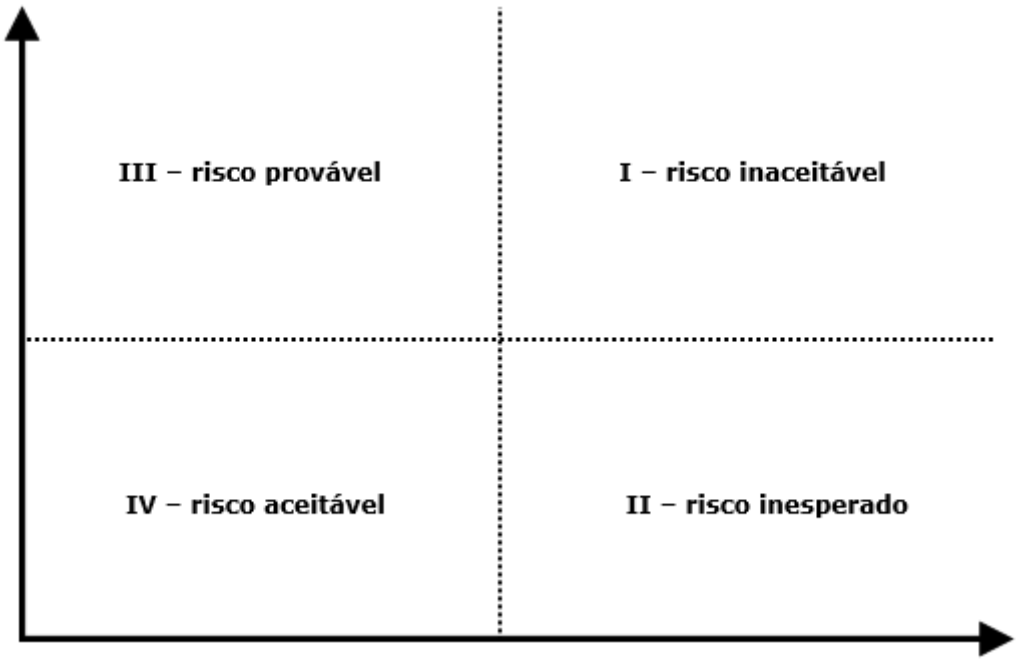
Processo de Avaliação

6.2. A avaliação dos Riscos é realizada, principalmente, de acordo com o previsto abaixo:

(a) identificação dos fatores (causas) de Riscos e implicações nos objetivos (metas e resultados) projetados;
(b) análise dos principais Riscos suscetíveis de afetar os seus objetivos, por meio da determinação do grau de impacto e probabilidade de ocorrência dos Riscos, conforme Matriz de Risco abaixo:



(c) priorização e definição do Limite (ou apetite) de cada Risco que a Companhia e seus acionistas estão dispostos a correr na busca pelo retorno e geração de valor, classificando os Riscos como de acordo com a matriz de priorização de riscos e as definições abaixo:



• **I - Risco Inaceitável**: Riscos são inaceitáveis e demandam ação gerencial prioritária para eliminar a componente de risco ou reduzir sua severidade e/ou frequência.
• **II - Risco Inesperado**: Riscos inesperados, com alto impacto e baixa frequência. Riscos devem ser quantificados e monitorados regularmente para direcionar continuamente as estratégias de mitigação e/ou planos de contingência. O objetivo é estar preparado caso o evento venha a acontecer.
• **III - Risco Provável**: Riscos de menor criticidade devido ao menor nível de impacto no valor do negócio – Foco deve ser o de definir níveis aceitáveis de perda por eventos e limites de competência que evitem que o nível de impacto suba ao longo do tempo. Tratamento sujeito à viabilidade de contratação de seguros como resposta a estes riscos.
• IV - Risco Aceitável: Riscos de baixo impacto e frequência, não havendo necessidade de monitoramento contínuo.

Tratamento

6.3. Após a avaliação, os Riscos devem ser tratados por meio de inciativas definidas e implantadas pela Diretoria, com auxílio da área de Gestão de Riscos e Controles Internos da Companhia, de forma a adequar a exposição da Companhia aos Limites do Risco aprovado.

6.4. As ferramentas utilizadas no processo de tratamento dos Riscos devem objetivar sua (i) eliminação, (ii) mitigação ou (iii) transferência à Terceiros.

Comunicação e Consulta

6.5. A comunicação dentro da estrutura de governança, deverá proporcionar as informações necessárias para que o Conselho de Administração, a Diretoria, o Comitê de Auditoria e *Compliance* e a área de Gestão de Riscos e Controles Internos exerçam suas responsabilidades e atividades na Gestão de Riscos.

6.6. A comunicação deve ser focada no desenvolvimento de uma compreensão clara e oportuna dos Riscos da Companhia.

6.7. A frequência e o nível de detalhamento das comunicações entre o Conselho de Administração e o Comitê de Auditoria e *Compliance* e entre a Diretoria e a área de Gestão de Riscos e Controles Internos devem ser suficientes para permitir o entendimento dos resultados das avaliações e seus impactos, bem como a reação em tempo hábil às indicações de eficácia.

6.8. A comunicação e a consulta entre os Colaboradores da Companhia, sobre Riscos e seu gerenciamento, deve ocorrer de forma contínua, visando o compartilhamento de informações e melhorias necessárias nos processos de gerenciamento de Riscos pela área de Gestão de Riscos e Controles Internos.

6.9. O processo de gerenciamento de Riscos deve ser observado em todos os processos de tomada de decisão da Companhia, incluindo o planejamento estratégico, as decisões de investimento e a gestão de projetos, desde o momento em que são

criados e ao longo de todo o seu desenvolvimento.

Monitoramento

6.10. A partir da identificação dos Riscos, estes deverão ser monitorados de forma contínua, de acordo com a divisão de responsabilidades descrita no item 7 abaixo.

Coordenador do Comitê de Auditoria e Compliance

6.11. O Coordenador do Comitê de Auditoria e *Compliance* é o responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos por esta Política, em conformidade com as boas práticas, com o apoio e suporte da MCGC Consultoria em Governança Corporativa Ltda. ("MCGC").

6.12. O Coordenador do Comitê de Auditoria e *Compliance* não deve atuar em funções ou em qualquer atividade que limite a sua independência.

6.13. Cabe Coordenador do Comitê de Auditoria e *Compliance* encaminhar à Diretoria da Companhia, as conclusões dos testes de controles internos efetuados pela MCGC, as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento e planos de ação, quando for o caso, a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico para saná-las.

6.14. Neste sentido, são obrigações do Coordenador do Comitê de Auditoria e *Compliance,* em conjunto com a MCGC, buscar que as atividades desempenhadas pela Companhia sejam exercidas de forma a:

(a) assegurar que a linha de negócio opere em conformidade com as leis e regulamentos aplicáveis;

(b) fazer interface com os órgãos reguladores, ambientais de vigilância e de fiscalização, com respeito às solicitações formais e promover ações corretivas no que for exigido;

(c) desenvolver, implementar e atualizar políticas, procedimentos e processos para atender os requisitos de *Compliance*;

(d) identificar as necessidades de treinamento e assegurar que todos os membros de staff realizaram os treinamentos necessários;

(e) assegurar que a Companhia e seus membros de staff tenham todos os registros exigidos e licenças para conduzir seus negócios;

(f) monitorar as atividades da Companhia de maneira proativa para detectar e prevenir violações potenciais às regras;

(g) conduzir exames de *Compliance* regulares para assegurar que a Companhia esteja aderente a um nível satisfatório de *Compliance*;

(h) conduzir investigações internas, quando necessário;

(i) rever e aprovar material de marketing, notadamente aqueles que têm necessidade de divulgação; e

(j) quando (e se houver) houver potencial quebra/violação de qualquer princípio, lei, regulamento ou requisito legal por um Colaborador, o Coordenador do Comitê de Auditoria e *Compliance* deverá informar o Conselho de Administração da Companhia.

Comitê de Auditoria e Compliance

6.15. O Comitê de Auditoria e *Compliance* tem total autonomia para executar suas funções e tem a atribuição de fornecer consultorias frente a questões especificas de *compliance* e controles internos, bem como, fomentar discussões de temas pertinentes, analisar casos/situações excepcionais e definir as ações a serem tomadas.

6.16. Dessa forma, a Companhia busca assegurar que as decisões sejam tomadas pelo Comitê de Auditoria e *Compliance* de maneira autônoma, tendo total discricionariedade no âmbito da sua área de atuação, inclusive para a apuração de eventuais descumprimentos às normas internas de conduta e legislação.

Segurança da Informação

6.17. A área de Segurança da Informação da Companhia é responsável por revisar as Diretrizes da Política de Segurança da Informação e sempre que houver necessidade de discussão e revisão dessas diretrizes, o Coordenador do Comitê de Auditoria e *Compliance* deve ser consultado.

6.18. A Companhia entende que deve garantir que as informações geradas, armazenadas, processadas e disponibilizadas pela Companhia sejam confiáveis e seguras.

6.19. Deve-se analisar o risco para toda liberação de acesso lógico, a funcionários e Terceiros, sendo o mesmo liberado somente a ambientes necessários à execução do trabalho. Periodicamente, este tipo de acesso deve ser auditado, verificando se o acesso concedido está de acordo com as necessidades da atribuição.

6.20. O Coordenador do Comitê de Auditoria e *Compliance* é o responsável por manter a Política de Segurança da Informação atualizada e, poderá a qualquer momento, e sem aviso prévio, verificar o conteúdo dos arquivos disponíveis no diretório interno e dos e-mails enviados e recebidos pelos profissionais da Companhia, sem que isto configure quebra de sigilo, com vistas ao cumprimento das normas de *Compliance*. Para que isso ocorra no que tange ao sigilo das informações produzidas ou recebidas pela Companhia, todos os Colaboradores devem seguir firmemente os princípios abaixo:

(a) estar ciente de que as informações processadas, mantidas ou registradas em áreas de acesso restrito não podem ser transferidas ou transmitidas, por qualquer meio, a

Terceiros ou Colaboradores de outras áreas da Companhia, independentemente de seu nível hierárquico, comprometendo-se a manter sigilo absoluto sobre elas e restringir o seu uso às estritas necessidades das funções que exerce;

(b) ser responsável pela guarda dos documentos relativos às suas atividades, certificando-se de que documentos confidenciais não permaneçam expostos, sendo ao final do expediente trancados devidamente armazenados em gavetas e arquivos;

(c) ter ciência de que as senhas de acesso à rede, bem como as senhas de acesso aos diversos sistemas utilizados na Companhia, são pessoais e intransferíveis, devendo ser mantidas em estrito sigilo;

(d) comprometer-se a não acessar informações para as quais não tenha sido autorizado, ou que não estejam relacionadas às suas atividades profissionais;

(e) não efetuar qualquer comentário ou revelação a outros Colaboradores ou a Terceiros sobre informações confidenciais, inclusive conversas de negócios em locais públicos, devendo restringi-las ao contexto de suas práticas profissionais;

(f) estar ciente que os e-mails enviados e recebidos por todos os Colaboradores da Companhia em ambiente interno e externo podem em eventual necessidade ser acessados para fins de controles internos;

Uso da Internet

6.21. Todos os computadores utilizados pelos Colaboradores da Companhia para fins estritamente profissionais possuem senhas pessoais e intransferíveis e com prazo de expiração de sua validade, de modo a permitir constantemente a identificação do seu usuário.

6.22. Os Colaboradores comprometem-se a não instalar qualquer software ou programa, de qualquer procedência, nos computadores da Companhia, exceto quando expressamente autorizado pela área responsável.

6.23. Coordenador do Comitê de Auditoria e *Compliance*, bem como o responsável por TI devem ser notificados sobre suspeitas de violações a essas regras.

6.24. A Companhia possui procedimentos rotineiros de segurança e realiza treinamentos sobre a confidencialidade de informações de modo a evitar qualquer tipo de violação ou vazamento de informações.

Controle de Acesso Lógico

6.25. Os sistemas e *softwares* que fornecem informação material aos negócios da Companhia devem ser mantidos e operados com controles adequados de processamento de dados. Direitos de acesso a vários sistemas e *softwares* são controlados e mantidos pelo responsável por TI.

Testes Periódicos de Segurança

6.26. O procedimento para a realização dos testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico são de responsabilidade da área de Segurança de Informação.

Controle de Acesso Físico

6.27. O acesso às dependências da Companhia é permitido somente a Colaboradores, Visitantes e Prestadores de Serviços contínuos, devidamente autorizados, conforme previsto no Procedimento de Acesso às Dependências, garantindo a segurança e integridade dos Colaboradores dentro das dependências da Companhia.

Treinamentos

6.28. A Companhia deve possuir uma rotina de treinamentos de modo a deixar seus Colaboradores a par das regras, manuais e políticas. O Coordenador do Comitê de Auditoria e *Compliance* determina a frequência dos treinamentos e quais pessoas devem estar envolvidas, de acordo com a análise dos riscos a que a Companhia esteja exposta. Podem ser necessários treinamentos extras por ocasião de mudança na legislação ou por mudanças em processos relevantes que, implicam em alterações das políticas ou manuais.

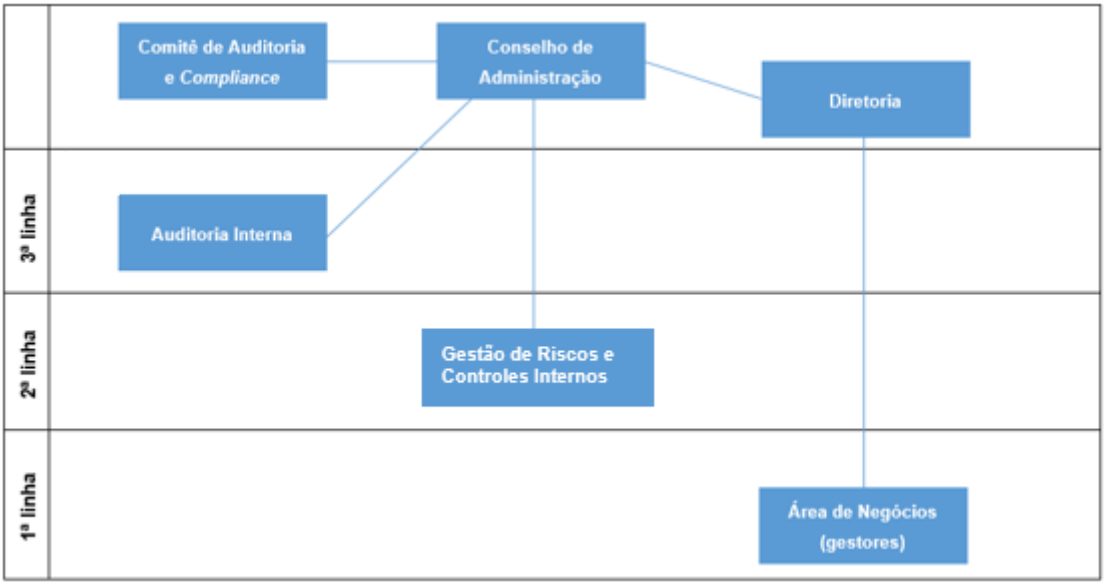
6.29. Os principais temas abordados nos treinamentos serão: Código de Ética, Procedimentos de Acesso às Dependências, Segurança e Confidencialidade da Informação, Política Anticorrupção, Conflito de Interesses bem como o conteúdo de outras políticas que se façam necessárias.

6.30. Mesmo com a rotina de treinamentos, é responsabilidade Coordenador do Comitê de Auditoria e *Compliance* assegurar que todas as normas, políticas e disposições relativas a controles internos, incluindo o código de ética e demais manuais e procedimentos estejam disponíveis para todos os Colaboradores.

6.31. Anualmente, o Coordenador do Comitê de Auditoria e *Compliance* organizará e fornecerá treinamento, com o suporte da MCGC, com registro através da lista de presença sobre as atualizações em políticas, procedimentos e normas aplicáveis.

7. CARGOS E RESPONSABILIDADES

7.1. Seguindo o modelo de "Três Linhas de Defesa", o gerenciamento dos Riscos deve ser realizado sob a responsabilidade dos órgãos de governança, gestores e responsáveis diretos pelos processos, conforme descrito neste item e estrutura hierárquica apresentada abaixo:



7.2. Compete ao Conselho de Administração da Companhia:

(a) aprovar a Política de Gerenciamento de Riscos da Companhia e suas futuras revisões;
(b) determinar o Limite (ou apetite) por Risco e aprovar a Matriz/Modelagem de Risco, conforme proposta apresentada pela Diretoria, estabelecendo a cultura de Gestão do Risco dentro da Companhia;
(c) tomar as principais decisões com relação ao processo de Gestão de Riscos da Companhia, incluindo as que possam afetar o perfil de risco ou exposição da Companhia, bem como fornecer à Diretoria, sempre que necessário, sua percepção quanto ao grau de exposição a Riscos, influenciando na priorização dos Riscos a serem tratados;
(d) revisar, monitorar e aprovar as estratégias gerais da Companhia para a gestão do risco e os papéis e relatórios elaborados pelo Comitê de Auditoria e *Compliance*; e
(e) avaliar a adequação da estrutura operacional e de controles internos para o gerenciamento de Riscos, com o assessoramento do Comitê de Auditoria e *Compliance*.

7.3. Compete à Diretoria da Companhia:

(a) elaborar, para apreciação e deliberação do Conselho de Administração, as diretrizes e a Matriz/Modelagem de Risco, propondo ainda os limites de exposição, impactos, e os limites (ou apetite) aos Riscos da Companhia;
(b) definir, em conjunto com a área de Gestão de Riscos e Controles Internos, os planos de ação para mitigação dos Riscos;
(c) supervisionar o processo de avaliação de Riscos e monitorar a evolução da exposição aos Riscos e os sistemas de gerenciamento de Risco; e
(d) implementar as estratégias da Companhia aprovadas pelo Conselho de Administração com relação à Gestão de Riscos, disseminando a cultura da gestão de Riscos em toda Companhia.

7.4. Compete ao Comitê de Auditoria e *Compliance* da Companhia, o qual se reporta diretamente para o Conselho de Administração, sem prejuízo das demais atribuições previstas no regimento interno do Comitê de Auditoria e *Compliance*:

(a) avaliar, ao menos uma vez ao ano, a suficiência da estrutura e do orçamento da área de Auditoria Interna para o regular desempenho de suas atribuições;
(b) analisar e revisar os relatórios elaborados pela área de Gestão de Riscos e Controles Internos, de modo a consolidar tais informações e reportar suas conclusões trimestralmente ao Conselho de Administração, incluindo sua avaliação sobre a confiabilidade dos controles internos da Companhia;
(c) assegurar que a linha de negócio opere em conformidade com as leis e regulamentos aplicáveis;
(d) monitorar a criação de novas leis e regulamentos aos quais a Companhia está ou possa vir a estar sujeita, bem como identificar fatos relevantes que possa influenciar as operações da Companhia, cabendo-lhe compartilhar tais fatos em reunião da Diretoria para definição de plano de ação, se necessário;
(e) monitorar o 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, cabendo-lhe compartilhar tais fatos em reunião da Diretoria para definição de plano de ação, se necessário; e
(f) monitorar a tramitação de projetos envolvendo criação ou modificação de leis ou normativos e regulamentos emitidos por entidades governamentais, e seus efeitos, ainda que potenciais, sobre as atividades da Companhia, cabendo-lhe compartilhar a existência de tais mudanças em reunião da Diretoria para definição de plano de ação.

7.5. Compete aos gestores das áreas de negócio e responsáveis diretos pelos processos, como primeira linha de defesa, com reporte para a Diretoria:

(a) identificar e gerenciar os Riscos das respectivas áreas de negócio e processos de acordo com os Limites de Riscos;
(b) comunicar, tempestivamente, à área de Gestão de Riscos e Controles Internos da Companhia, se os eventos de Risco apresentarem tendência de ocorrência e/ou eventual extrapolação dos Limites de Risco;
(c) implementar e acompanhar os planos de ação para mitigação de Riscos e acompanhar as ações corretivas nas respectivas áreas e processos; e

(d) em conjunto com a área de Gestão de Riscos e Controles Internos, definir controles internos dos processos de suas respectivas áreas.

7.6. Compete à área de Gestão de Riscos e Controles Internos da Companhia, como segunda linha de defesa, e a qual se reporta diretamente para o Conselho de Administração:

(a) administrar o sistema de gerenciamento de Risco, monitorando a execução dos planos de ação definidos pela Diretoria;
(b) fornecer apoio metodológico aos departamentos operacionais e funcionais da Companhia por meio de ferramentas e serviços sob demanda;
(c) fornecer informações precisas, íntegras e suficientes para a modelagem de Riscos;
(d) apresentar percepção quanto à exposição ao Risco (magnitude de impacto e probabilidade de ocorrência), se possível, pautada também em indicadores de mercado;
(e) auxiliar a Diretoria na elaboração da proposta quanto às diretrizes, à Matriz/Modelagem de Risco, aos limites de exposição, os impactos e o Limite (ou apetite) aos Riscos da Companhia;
(f) supervisionar o processo de avaliação de Riscos em conjunto com a Diretoria;
(g) acompanhar a Diretoria na implantação desta Política por meio da disseminação de ferramentas e boas práticas;
(h) comunicar, tempestivamente, os eventos de Risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites, para discussão nos fóruns e alçadas apropriadas;
(i) assegurar as informações disponibilizadas à Diretoria sobre Riscos ou incidentes, bem como coordenar o sistema de gerenciamento dos Riscos em momentos de crises em caso de grandes acontecimentos;
(j) conforme orientação do Comitê de Auditoria e *Compliance*, elaborar e/ou contribuir na elaboração das políticas e normas de conduta e anticorrupção para os Colaboradores, fornecedores e clientes, atuando ativamente na sua divulgação e conscientização junto aos respectivos públicos; e
(k) conforme orientação e sob supervisão do Comitê de Auditoria e *Compliance*, garantir o funcionamento e idoneidade dos canais de denúncias em todos os níveis e para todos os públicos da organização, assim como a apuração e resolução adequada dos casos.

7.7. Compete à área de Auditoria Interna da Companhia, como terceira linha de defesa, vinculada diretamente ao Conselho de Administração:

(a) elaborar um plano anual de auditoria, a fim de verificar a eficácia dos controles internos e efetividade do processo de gerenciamento de riscos da Companhia;
(b) aferir a qualidade e a efetividade dos processos de gerenciamento de Riscos e controles internos da Companhia, sugerindo alterações ao Comitê de Auditoria e *Compliance*, quando necessário;
(c) identificar e apontar oportunidades de melhorias nos processos de controles internos, riscos e *compliance* da Companhia;

(d) fornecer, quando solicitado, informações precisas, íntegras e suficientes para a modelagem;
(e) analisar os relatórios trimestrais produzidos pela área de Gestão de Riscos e Controles Internos; e
(f) apresentar, quando solicitado, sua percepção quanto à exposição ao Risco (magnitude de impacto e probabilidade de ocorrência), se possível, pautada também em indicadores de mercado.

7.7.1. As atividades da área de Auditoria Interna poderão ser desempenhadas por auditor independente registrado na CVM contratado pela Companhia nos termos do Regulamento do Novo Mercado.

7.8. Ainda, compete à área de Segurança da Informação da Companhia:

(a) acompanhar periodicamente a integridade do sistema de gravações telefônicas;
(b) monitorar o procedimento de *backup*, sua execução e guarda;
(c) efetuar a manutenção dos servidores e acompanhamento da capacidade dos mesmos
(d) implementar melhorias nos sistemas; e
(e) administrar acesso aos sistemas, e-mails, etc.

8. DISPOSIÇÕES GERAIS

8.1. Todos os Colaboradores devem cumprir as diretrizes estabelecidas nesta Política, bem como zelar para seu cumprimento e conhecimento. Não será tolerado o descumprimento desta Política.

8.2. É obrigação de todos informar os riscos detectados podendo ser tal assunto remetido diretamente ao Conselho de Administração.

9. DÚVIDAS E DENÚNCIAS

9.1. Em caso de qualquer dúvida com relação aos termos desta Política, entre em contato com o Comitê de Auditoria e *Compliance* no e-mail comitecompliance@korasaude.com.br.

9.2. O reporte de situações de descumprimento ou possíveis violações à presente Política, às políticas aqui mencionadas, a outras normas internas da Companhia e/ou à legislação aplicável deve ser feito pelo site https://www.korasaude.com.br/investidores ou pelo telefone 0800 591 2643, de segunda-feira a sexta-feira das 09h às 17h.

10. VIGÊNCIA

10.1. Esta Política foi aprovada pelo Conselho de Administração, encontra-se em vigor a partir da presente data e somente poderá ser modificada por deliberação do Conselho de Administração da Companhia.

Cariacica, 25 de abril de 2021

*****