



POLÍTICA DE GESTÃO DE RISCOS

2025



BIOTIC****
A cidade viva da inovação

1. FINALIDADE

- 1.1. Instituir a Política de Gestão de Riscos no âmbito da Biotic S.A., que compreende:
 - a) o objetivo;
 - b) os princípios;
 - c) as diretrizes;
 - d) as responsabilidades;
 - e) o processo de gestão de riscos.
- 1.2. A Política de Gestão de Riscos tem como premissa o alinhamento ao Planejamento Estratégico da Empresa e do Governo do Distrito Federal.
- 1.3. A Política de Gestão de Riscos tem por objetivo estabelecer os princípios, as diretrizes, as responsabilidades e o processo de gestão de riscos na Biotic S.A., com vistas à incorporação da análise de riscos à tomada de decisão, em conformidade com as boas práticas de governança adotadas no setor público.
- 1.4. A política definida deverá ser observada por todas as áreas e níveis de atuação da Biotic S.A., sendo aplicável aos respectivos processos de trabalho, projetos, atividades e ações.
- 1.5. Todos os gestores deverão, com uma periodicidade anual, realizar treinamento sobre a política de gestão de riscos e suas práticas. O treinamento deverá ser realizado pela área de risco e de recursos humanos que deverão registrar, de maneira formal, a participação dos gestores.
- 1.6. A Política de Gestão de Riscos promoverá:
 - a) a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais;
 - b) o alinhamento do apetite ao risco com as estratégias adotadas;
 - c) o fortalecimento das decisões em resposta aos riscos;
 - d) o aprimoramento dos controles internos administrativos.

2. CAMPO DE APLICAÇÃO

- 2.1. Biotic S.A.

3. FUNDAMENTAÇÃO LEGAL

- 3.1. Norma ABNT NBR ISO 31000:2009, que estabelece princípios e diretrizes para a implantação da Gestão de Riscos.
- 3.2. *Committee of Sponsoring Organizations of the Treadway Commission – COSO 2013 – Internal Control – Integrated Framework (ICIF).*
- 3.3. Decreto nº 37.302, de 29/4/2016, que estabelece os modelos de boas práticas gerenciais em Gestão de Riscos e Controle Interno a serem adotados no âmbito da Administração Pública do Distrito Federal.

4. DISPOSIÇÕES GERAIS

4.1. DOS PRINCÍPIOS DE GESTÃO DE RISCOS

4.1.1. A gestão de riscos observará os seguintes princípios:

- a) criar e proteger valores institucionais;
- b) ser parte integrante dos processos organizacionais;
- c) ser parte da tomada de decisões;
- d) abordar explicitamente a incerteza;
- e) ser sistemática, estruturada e oportuna;
- f) ser baseada nas melhores informações disponíveis;
- g) estar alinhada ao contexto e ao perfil de risco da instituição (ser feita sob medida);
- h) considerar fatores humanos e culturais;
- i) ser transparente e inclusiva;
- j) ser dinâmica, interativa e capaz de reagir a mudanças;
- k) facilitar a melhoria contínua da organização.

4.2. DAS DIRETRIZES DE GESTÃO DE RISCOS

4.2.2. Para fins desta Norma considera-se:

- a) riscos – efeito da incerteza nos objetivos a serem atingidos pela instituição;
- b) gestão de riscos – atividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco;

- c) estrutura de gestão de risco – conjunto de elementos que fornecem os fundamentos e disposições organizacionais para conceber, implementar, monitorar, rever e melhorar continuamente a gestão do risco em toda a organização;
- d) política de gestão de risco – declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;
- e) atitude perante o risco – abordagem da organização para avaliar e eventualmente buscar, manter, assumir ou afastar-se do risco;
- f) apetite pelo risco – quantidade e tipo de riscos que uma organização está preparada para buscar, manter ou assumir;
- g) aversão ao risco – atitude de afastar-se de riscos;
- h) plano de gestão de riscos – esquema dentro de uma estrutura de gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;
- i) proprietário do risco – pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;
- j) processo de gestão de riscos – aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto e na identificação, avaliação, tratamento, monitoramento e análise crítica dos riscos;
- k) parte interessada – pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade;
- l) processo de avaliação de riscos – processo global de identificação de riscos, análise de riscos e avaliação de riscos;
- m) fonte de risco – elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;
- n) evento – ocorrência ou alteração em um conjunto específico de circunstâncias;
- o) consequência – resultado de um evento que afeta os objetivos;
- p) probabilidade – chance de algo acontecer;
- q) perfil de risco – descrição de um conjunto qualquer de riscos;

- r) critérios de risco – termos de referência contra a qual o significado de um risco é avaliado;
- s) nível de risco – magnitude de um risco expressa na combinação das consequências e de suas probabilidades;
- t) controle – medida que está modificando o risco;
- u) risco residual – risco remanescente após o tratamento do risco;
- v) risco inerente – risco ao qual se expõe face à inexistência de controles que alterem o impacto ou a probabilidade do evento;
- w) tolerância ao risco – é o nível de variação aceitável quanto à realização dos seus objetivos;
- x) impacto – efeito resultante da ocorrência do evento.

4.2.3. A Política de Gestão de Riscos abrange as seguintes categorias de riscos:

- a) estratégicos – riscos decorrentes da falta de capacidade ou habilidade da unidade em proteger-se ou adaptar-se às mudanças que possam interromper o alcance de objetivos e a execução da estratégia planejada;
- b) de conformidade – riscos decorrentes do órgão/entidade não ser capaz ou hábil para cumprir com as legislações aplicáveis ao seu negócio e não elabore, divulgue e faça cumprir suas normas e procedimentos internos;
- c) financeiros – riscos decorrentes da inadequada gestão de caixa, das aplicações de recursos em operações novas/desconhecidas e/ou complexas de alto risco;
- d) operacionais – riscos decorrentes da inadequação ou falha dos processos internos, pessoas ou de eventos externos;
- e) ambientais – riscos decorrentes da gestão inadequada de questões ambientais como, por exemplo: emissão de poluentes, disposição de resíduos sólidos e outros;
- f) de tecnologia da informação – riscos decorrentes da indisponibilidade ou inoperância de equipamentos e sistemas informatizados que prejudiquem ou impossibilitem o funcionamento ou a continuidade normal das atividades da instituição; representado, também, por erros ou falhas nos sistemas informatizados ao registrar, monitorar e contabilizar corretamente

transações ou posições;

- g) de recursos humanos – riscos decorrentes da falta de capacidade ou habilidade da instituição em gerir seus recursos humanos de forma alinhada aos objetivos estratégicos definidos;
- h) de integridade - riscos decorrentes de atos de corrupção, fraude, abuso de poder, conflitos de interesse, nepotismo, desvio de recursos e outros.

4.2.4. São elementos estruturantes da Gestão de Riscos da Biotic S.A. a Política de Gestão de Riscos, o Comitê de Integridade, Governança e Gestão de Riscos da Biotic S.A., o Processo de Gestão de Riscos e o Controle.

5. DAS RESPONSABILIDADES DE RISCOS

5.1. São considerados proprietários dos riscos, em seus respectivos âmbitos e escopos de atuação, os responsáveis pelos processos de trabalho, projetos, atividades e ações desenvolvidos nos níveis estratégicos, táticos ou operacionais da Biotic S.A.

5.2. Compete aos proprietários dos riscos, relativamente aos processos de trabalho e iniciativas sob sua responsabilidade, decidir sobre:

- a) a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica, considerando a dimensão dos prejuízos que possam causar;
- b) os níveis de risco aceitáveis, considerando o Plano de Gestão de Risco previsto nesta norma;
- c) quais riscos deverão ser priorizados para tratamento por meio de ações de caráter imediato, a curto, médio ou longo prazos ou de aperfeiçoamento contínuo;
- d) as ações de tratamento a serem implementadas, assim como o prazo de implementação e avaliação dos resultados obtidos.

5.3. Compete aos órgãos colegiados e demais estruturas de controle da empresa as seguintes responsabilidades:

- a) Conselhos de administração – deliberar sobre as questões estratégicas concernentes ao processo de gestão de riscos, tais como o grau de apetite a

riscos das empresas, o papel das Diretorias Executivas e da Presidência, no gerenciamento dos riscos, e a política que deve nortear todo o processo;

- b) Diretoria Executiva e Presidência – patrocinar a implantação da gestão de riscos nas empresas; alocar recursos necessários ao processo e definir a infraestrutura apropriada às atividades de gerenciamento de riscos; aprovar normas específicas e o grau de apetite a riscos das empresas; deliberar sobre decisões estratégicas considerando as análises dos riscos relatadas pela unidade pertinente;
- c) Comitê de Risco – constituído, deve acompanhar a gestão integrada de riscos, validando e revisando periodicamente a matriz de riscos das empresas, bem como a sua estrutura de controles internos e as ações tomadas para minimizar a ocorrência de eventos que comprometam a realização de seus objetivos; promover assuntos estratégicos e operacionais no processo de gestão de riscos; levar ao conhecimento das Diretorias Executivas as análises dos riscos priorizados para apoiar a tomada de decisão;
- d) Divisão de Compliance e Gestão de Riscos – coordenar e definir os padrões a serem seguidos, no que tange aos processos de gestão de riscos, aos seus sistemas de suporte e às formas e à periodicidade de seus reportes; apoiar e garantir a identificação e o monitoramento dos riscos pelas áreas proprietárias, de acordo com a política e técnicas aprovadas pela empresa;
- e) Coordenação de Governança – gerir os riscos operacionais inerentes ao negócio da Companhia; elaborar e atualizar, periodicamente, o plano de gestão de riscos da empresa;
- f) Conselho Fiscal – conhecer os riscos mais significantes para a Companhia e monitorar se a Administração está tratando-os de forma adequada;
- g) Consultoria/Assessoria Jurídica – orientar a Companhia em relação às normas aplicáveis e alterações legislativas pertinentes;
- h) Outros gestores da Biotic S.A. – coordenar, promover e acompanhar as ações de gestão de riscos na sua área de atuação; avaliar continuamente seus processos, analisar riscos envolvidos e garantir a efetividade dos controles e conformidade dos processos; atuar conforme os princípios de conduta e ética da Companhia; desenvolver e aprimorar metodologias de seu processo de forma a potencializar a identificação, tratamento e monitoramento dos riscos específicos, em consonância com esta política e com as diretrizes; e fornecer à

Coordenação de Governança as informações necessárias para a avaliação integrada dos riscos, o monitoramento e o reporte para a alta administração.

6. DOS PROCESSOS DE RISCOS

6.1. Serão adotados como referências técnicas para a gestão de riscos a norma ABNT NBR ISO 31000:2009, agregada ao COSO 2013 - Controles Internos – Estrutura Integrada, compreendido pelas seguintes fases:

- a) comunicação e consulta – Processos contínuos e interativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos. A comunicação durante todas as etapas do processo de gestão de riscos deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pelo mercado. A transparência dever ser notória entre os interessados e os aspectos legais considerados, principalmente sob a ótica de mercado.
- b) estabelecimento do contexto – definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e ao estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos;
- c) identificação dos riscos – busca, reconhecimento e descrição dos riscos, mediante a identificação das fontes de risco, eventos suas causas e suas consequências potenciais, devendo ser realizada com a participação dos envolvidos nos processos de negócio da Biotic S.A.
- d) análise dos riscos – compreensão da natureza do risco e determinação do respectivo nível mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis;
- e) avaliação dos riscos – processo de comparação dos resultados da análise de risco com os critérios do risco para determinar se o risco e/ou sua respectiva magnitude é aceitável ou tolerável, devendo considerar as principais ameaças que o contexto empresarial vive e o fato de o processo determinar se o risco é aceitável ou não, identificando a tolerância do risco;
- f) tratamento dos riscos – processo que visa modificar e cuidar dos riscos, com a definição de tratamento que será dado aos riscos priorizados e como esses

deverão ser monitorados e reportados às diversas partes envolvidas, além de considerar o grau de apetite da Companhia, com a devida homologação pela Diretoria Executiva e decidir: (i) evitá-los, eliminando potencialidades de risco; (ii) mitigá-los, pela definição de planos de ação e controles internos; (iii) compartilhá-los com os agentes envolvidos; e (iv) aceitá-los;

- g) monitoramento dos riscos – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado; além da necessária verificação do alcance das metas das ações estabelecidas por intermédio de atividades gerenciais contínuas que garantam que os controles sejam aprimorados com o fito de: detectar mudanças no contexto externo e interno, identificando riscos emergentes; e analisar as mudanças nos eventos de risco, tendências, sucessos e fracassos e aprender com eles;
- h) identificação dos controles – identificação dos procedimentos, ações ou documentos que garantam o alcance dos objetivos do processo e diminuam a exposição aos riscos;
- i) estabelecimento dos controles – políticas e procedimentos que assegurem o alcance dos objetivos da administração, diminuindo a exposição das atividades aos riscos que acontecem ao longo do processo organizacional, em todos os níveis e em todas as funções, incluindo, aprovações, autorizações, verificações, reconciliações, revisões de desempenho operacional, segurança de recurso e segregação de funções.

6.2. Eventuais conflitos de atuação decorrentes do processo de gestão de riscos serão dirimidos pelo Comitê de Gestão de Riscos ou, caso não constituído, pela Coordenação de Governança.

6.3. O processo de gestão de riscos deve ser realizado em ciclos não superiores a 1 (um) ano, abrangendo os processos de trabalho das áreas de gestão da Biotic S.A.

7. DAS DISPOSIÇÕES FINAIS

7.1. Os proprietários dos riscos a que se refere esta norma deverão implantar a presente política de gestão de riscos a partir da publicação.

7.2. Os casos omissos ou excepcionais serão analisados pelo o Comitê de Integridade, Governança e Gestão de Riscos da Biotic S.A. ou, enquanto não

constituído, pela Coordenação de Governança, de acordo com as orientações e normas gerais sobre a matéria e submetidos à Diretoria Executiva.