gerencianet	POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS	Emissão 02/06/2021	Classificação Pública
Identificação PUB POL GER		Versão 2.0	Tipo Documento Política

1. OBJETIVO

Esta política tem por objetivo estabelecer princípios, diretrizes, papeis e responsabilidades a serem observadas no processo de gestão dos riscos corporativos, de forma a possibilitar a sua adequada identificação, avaliação, resposta/tratamento, controle, comunicação e monitoramento.

2. APLICABILIDADE

Esta política é aplicável ao Conglomerado Gerencianet, devendo ser cumprida por todas as áreas envolvidas.

3. REFERÊNCIAS

- Circular nº 3.681/13
- Resolução CMN nº 4.553/17
- Resolução CMN nº 4.557/17
- Resolução CMN nº 4.606/17
- COSO ERM - Enterprise Risk Management
- Guia de Orientação para Gerenciamento de Riscos Corporativos - IBGC (Instituto Brasileiro de Governança Corporativa)
- NBR/ISO 31000:2018: Gestão de Riscos - Diretrizes
- NBR ISO/IEC 31010:2012: Gestão de Riscos - Técnicas para o processo de avaliação de riscos
- ABNT ISO GUIA 73: Gestão de Riscos - Vocabulário
- Novo Modelo das Três Linhas do IIA (Institute of Internal Auditors)

4. DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os termos e definições contidos no "Anexo I - Glossário".

5. DIRETRIZES

I. O processo de gestão de riscos corporativos consiste na aplicação sistemática de metodologias, procedimentos e práticas de gestão, incorporadas na cultura organizacional e adaptadas aos processos da organização;

II. A partir das diretrizes do COSO ERM (Enterprise Risk Management), a gestão de riscos corporativos na Gerencianet é estruturada em oito componentes, conforme apresentados a seguir:

5.1. Ambiente Interno

I. Resultado da filosofia da empresa com relação a riscos e dos valores gerais da organização, colocados em função do ambiente em que ela atua. O ambiente interno define as possibilidades de atuação da organização;

II. O mercado, as leis, a cultura local e a filosofia dos gestores, bem como todos os fatores que definem a personalidade institucional, compõem o ambiente interno.

5.2. Fixação de Objetivos

I. Definidos pela alta administração, os objetivos devem ser divulgados a todos os componentes da organização, antes da identificação dos eventos que possam influenciar na consecução dos objetivos. Eles devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

5.3. Identificação de Eventos

I. Eventos são situações em potencial (que ainda não ocorreram) que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Por meio da identificação de eventos, é possível planejar o tratamento adequado para os riscos;

II. Após a identificação de eventos, realizar-se-á avaliação de riscos, quando se determinará a forma de tratamento para cada risco identificado e qual o tipo de resposta a ser dada a esse risco.

5.4. Avaliação de Riscos

I. Os riscos são analisados com relação à sua magnitude (resultado da avaliação do impacto e da probabilidade de ocorrência de certo evento);

II. A organização e seus gestores devem estar conscientes dos riscos relevantes que envolvem o negócio, bem como devem identificar as ameaças e agir para reduzir as possibilidades de danos decorrentes de sua materialização.

5.5. Resposta a Riscos

I. Medidas para alinhamento dos riscos com a tolerância e com o apetite ao risco. Conhecidos os riscos e mensuradas suas dimensões, a ação de resposta pode ser decidida;

II. Para cada risco identificado, será prevista uma resposta, que poderá ser:

- **Aceitar o risco:** não será tomada nenhuma ação em relação ao risco. Pode ocorrer quando a avaliação do risco demonstra sua irrelevância em relação ao atingimento dos objetivos, ou que o risco inerente já esteja dentro das tolerâncias ao risco, ou ainda quando o custo de implementação

de uma medida para responder a determinado risco fique muito alto, maior até do que os benefícios que a resposta traria para a organização.

- **Evitar o risco:** por considerar o risco muito elevado, a organização decide não correr o risco, ainda que parcialmente, o que implica em descontinuar as atividades que geram os riscos - ou seja, renunciar aos objetivos.
- **Mitigar o risco:** implantação de atividades e sistemas de controle que mantenham os riscos a níveis aceitáveis. Envolve a adoção de medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos.
- **Compartilhar (ou transferir) o risco:** Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma parte do risco.

5.6. Atividades de Controle

I. São as políticas e os procedimentos que asseguram a adequada resposta aos riscos. Para que os riscos sejam mantidos em níveis aceitáveis, a organização define políticas, que são filosofias de abordagem da questão; e os aspectos que devem direcionar a forma como os controles internos serão desenhados e exercidos por meio dos processos;

II. As atividades de controle não são exclusividade de determinada área da organização, sendo realizadas em todos os níveis, compreendendo uma série de atividades, como aprovações e autorizações, verificações, conciliações/reconciliações, segregação de funções, indicadores de desempenho, revisão de desempenho operacional, atribuição de autoridade e limites de alçada, revisão segregada, programas de contingência e planos de continuidade de negócios, entre outros.

5.7. Informações e Comunicações

I. Alinhamento das informações e comunicações necessárias geradas pela organização, para que haja fluência em todos os níveis da organização;

II. Esse elemento da gestão de riscos garante o conceito de atuação sistêmica da gestão, em que os processos e controles são interdependentes, e é um reconhecimento de que a avaliação da efetividade do controle interno não pode ser feita de forma isolada, e sim levando em consideração o funcionamento geral do sistema.

5.8. Monitoramento

I. Compreende o acompanhamento da qualidade do controle interno, visando a assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos. Pressupõe uma atividade desenvolvida ao longo do tempo;

II. O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno pode "reagir" de forma dinâmica, ajustando-se conforme as condições o determinem;

III. O monitoramento é realizado por meio de atividades contínuas e por avaliações independentes (auditorias internas e externas). As atividades contínuas são incorporadas às demais atividades normais da organização, e as avaliações independentes garantem a eficácia do gerenciamento dos riscos ao longo do tempo;

IV. Diferentemente das atividades de controle, que são concebidas para dar cumprimento aos processos e às políticas da organização e visam a tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de melhorias.

6. ESTRUTURA SIMPLIFICADA DE GERENCIAMENTO CONTÍNUO DE RISCOS

I. A Gerencianet possui uma estrutura simplificada de gerenciamento contínuo de riscos, adequada ao seu perfil de risco, proporcional à dimensão e à relevância de suas exposições aos riscos, e compatível com a natureza das operações e a complexidade das atividades, processos, produtos e serviços oferecidos;

II. A estrutura visa a identificação, mensuração, avaliação, monitoramento, reporte, controle e a mitigação dos riscos a que a Gerencianet está exposta de maneira relevante, porém, não se limitando ao risco operacional, de liquidez e de crédito;

III. A Organização constantemente aprimora políticas, normas, procedimentos, manuais, sistemas e controles internos, objetivando a criação de mecanismos que possibilitem uma constante mitigação aos riscos;

IV. A Gerencianet dispõe de documentos institucionais internos que dão as diretrizes sobre a gestão dos riscos operacionais, de liquidez e de crédito.

6.1. TAXONOMIA (CLASSIFICAÇÃO) DOS RISCOS

I. Tendo em vista as inúmeras definições de riscos e a necessidade de uma linguagem comum a todos os agentes envolvidos no processo, a Gerencianet adota um dicionário de riscos através da segmentação dos riscos em categorias, considerando as características e o ambiente de negócio da empresa;

II. O dicionário de riscos da Instituição contempla informações segregadas em quatro principais temas com seus respectivos desdobramentos:

- **Estratégico:** Eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos do setor ou Companhia. Exemplos: um projeto que altere o portfólio de produtos/serviços da empresa, início da operação de uma filial em outro local, diminuição de demanda do mercado por produtos e serviços da empresa causada por obsolescência em função de desenvolvimento de novas tecnologias/produtos pelos concorrentes etc.
- **Operacional:** Eventos que podem comprometer as atividades do departamento, normalmente associados a perdas resultantes de falhas, deficiências ou inadequação de processos internos,

pessoas, infraestrutura e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves etc. Exemplos: erros de lançamento de informações, fraudes, atrasos de entrega etc.

- **Financeiro:** Relacionados com a incapacidade da empresa de expressar informações fidedignas para os tomadores de decisão e gerenciar seus ativos financeiros, bem como bem como à confiabilidade dos lançamentos contábeis e das suas demonstrações financeiras. Exemplos: erros de contabilização que afetam as demonstrações financeiras, alteração proposital das informações para benefício de outrem, câmbio etc.
- **Legal:** Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Exemplos: processos trabalhistas, embargos, autuações, regulamentação de mercado etc.

III. Os desdobramentos da taxonomia de riscos são apresentados no dicionário de riscos da Instituição.

6.2. Modelo das Três Linhas do IIA

I. A estrutura de gestão de riscos da Gerencianet considera a atuação conjunta de todos os departamentos e colaboradores da organização, segregado em três linhas, cada uma com um papel distinto a ser desempenhado na estrutura de governança corporativa da Companhia, de acordo com o "Novo Modelo das Três Linhas do IIA":

- **1ª linha:** Constituída pelos Gestores dos departamentos. São os responsáveis pelos processos, riscos e controles inerentes ao negócio. Os gestores dos processos possuem propriedade sobre os riscos e são os responsáveis por implementar as ações corretivas com o objetivo de solucionar as deficiências de controle e de processo, mitigando os riscos relacionados.
- **2ª linha:** Constituída pelas áreas de Compliance e Jurídico e de Controles Internos e Gestão de Riscos, a qual possuem como responsabilidade suportar a 1ª linha na prática da gestão de riscos da Companhia, em especial em aspectos de controles internos, conformidade, procedimentos, normas, apoio das políticas de gestão, definição de papeis e responsabilidades, identificação de mudanças de apetite de risco da Companhia, auxílio no mapeamento de processos, controles e procedimentos.
- **3ª linha:** Constituída pela Auditoria Interna, responsável por prestar avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Reporta suas descobertas à gestão e ao órgão de governança para promover e facilitar a melhoria contínua. Ao fazê-lo, pode considerar a avaliação de outros prestadores internos e externos.

7. REVISÃO E ATUALIZAÇÃO

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência, conforme entendimento da Gestão da Gerencianet.

8. VIGÊNCIA

Esta política entra em vigor na data de sua publicação.

9. CONSIDERAÇÕES FINAIS

Outras políticas, normas, procedimentos ou termos, bem como outros complementares que detalhem ou evidenciem esta matéria, serão mantidas à disposição dos colaboradores, reguladores e auditorias.

ANEXO I - GLOSSÁRIO

- **ALTA ADMINISTRAÇÃO:** gestores que integram o nível mais elevado da organização com poderes para estabelecer as políticas, os objetivos e conduzir a implementação da estratégia para realizar os objetivos da organização.
- **APETITE A RISCOS:** representa o nível de risco que a organização pode aceitar, conforme estabelecido por sua visão e missão, indicando o grau de exposição aceitável na sua busca de valor.
- **CONTROLE:** medida que está modificando o risco. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco. Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.
- **CRO:** sigla de *Chief Risk Officer*, ou Diretor de Riscos.
- **EVENTO:** incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.
- **PLANO DE AÇÃO:** conjunto de medidas adotadas para tratar os riscos identificados, de forma a evitar a materialização dos riscos ou reduzir a probabilidade e/ou o impacto dessa materialização, levando esses fatores a níveis compatíveis com o apetite a riscos da Gerencianet. Pode abranger quaisquer áreas da Companhia e passar por criação, melhoria e/ou auditoria de processos e controles, utilização de sistemas e instrumentos específicos de identificação e proteção, entre outros.
- **POLÍTICA:** a administração estabelece aquilo que deverá ser feito para efetuar o controle. Uma política serve de base para a definição dos procedimentos e sua implementação.
- **POLÍTICA DE GESTÃO DE RISCOS:** declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.
- **RAS:** sigla de *Risk Appetite Statement*, ou Declaração de Apetite a Riscos.
- **RISCO:** possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos da Companhia. O risco é medido em termos de impacto e probabilidade.
- **RISCO INERENTE:** risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.
- **RISCO RESIDUAL:** risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.
- **STAKEHOLDERS:** partes interessadas que são afetadas pela organização, como os acionistas, as comunidades nas quais a organização opera, os empregados, os clientes e os fornecedores.
- **TOLERÂNCIA AO RISCO:** a variação aceitável relativa à realização de um objetivo.