

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 1 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

Sumário

1. Objetivo	2
2. Abrangência.....	2
3. Definições	2
4. Fundamentos.....	3
5. Estrutura de Gestão de Riscos.....	3
6. Diretrizes	5
6.1. Identificação de Riscos.....	5
6.2. Análise dos Riscos	5
6.3. Avaliação dos Riscos.....	6
6.3.1. Definição do Apetite ao Risco	6
6.3.2. Mensuração dos Riscos (Severidade).....	6
6.4. Tratamento dos Riscos.....	7
6.5. Monitoramento dos Riscos	7
7. Instrumentos - Controles	7
8. Atribuições e Responsabilidades	9
8.1. Conselho de Administração.....	9
8.2. Diretoria e Presidente:	9
8.3. Comitê de Auditoria (por delegação do Conselho de Administração):	10
8.4. Área de Gestão de Riscos e Controles Internos	10
8.5. Área de Compliance	10
8.6. Auditoria Interna (com base nas diretrizes do Conselho de Administração e Comitê de Auditoria):.....	11
8.7. Colaboradores:	11
8. Infrações e Sanções	11
9. Vigência	11
10. Histórico de Revisões	11

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 2 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

1. Objetivo

Esta política tem como objetivo estabelecer diretrizes, controles, procedimentos e responsabilidades relacionadas à identificação, avaliação, análise, tratamento e monitoramento dos riscos que possam afetar a Companhia, a fim de conduzir o apetite à tomada de risco no processo decisório na busca do cumprimento de seus objetivos, criação, preservação e crescimento de valor da Companhia.

Há como fundamento: as diretrizes de governança corporativa do estatuto social da Companhia e suas alterações, o “*Código de Conduta*” aplicável às empresas do grupo econômico da Companhia e o Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão.

2. Abrangência

Esta política aplica-se a todos os colaboradores, parceiros, contratados, terceiros, fornecedores, prestadores de serviços e outras pessoas físicas ou jurídicas que prestam serviços para a Boa Vista e demais partes interessadas que utilizam o ambiente físico e/ou lógico da Boa Vista.

Aplica-se, ainda, a todos os macroprocessos e operações de negócio da Companhia, sendo obrigatória a sua observância por todos os seus colaboradores.

3. Definições

Apetite a Risco: quantidade e tipo de riscos que uma organização está preparada e disposta a assumir e gerenciar para atingir seus objetivos, de acordo com os limites estabelecidos pelo Conselho de Administração da Companhia.

COSO - Committee of Sponsoring Organizations of the Treadway Commission: entidade que emite pronunciamentos e materiais a respeito das melhores práticas para gerenciamento de riscos e controles internos.

COSO ERM: material técnico emitido pelo COSO com orientações sobre as melhores práticas para gerenciamento de riscos corporativos.

Key Risk Indicators (KRI's): são componentes fundamentais de uma estrutura de controle e das boas práticas de gestão de risco. Principais indicadores de riscos da Companhia que sinalizam as causas das mudanças no nível de risco dos objetivos de negócio. Se percebidos em tempo hábil, ajudam a Companhia a agir preventivamente e reduzir perdas e/ou aproveitar novas oportunidades de criar, proteger e crescer seu valor.

Key Performance Indicators (KPI's): principais indicadores de performance da Companhia que auxiliam no monitoramento do desempenho do negócio e das áreas funcionais de suporte, permitindo avaliar e implantar melhorias necessárias para se atingir os objetivos da Companhia.

Mapa de Riscos: documento que formaliza todos os riscos identificados e seus componentes (avaliação, respostas aos riscos, indicadores que os medem e outros).

Riscos: são os eventos incertos que podem causar impactos negativos, impedindo ou dificultando o cumprimento dos objetivos estabelecidos pela Boa Vista.

Risco Cibernético: é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou um conjunto de ativos, impactando na confidencialidade, integridade, disponibilidade e autenticidade das informações.

Risco de Conformidade: é o 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 ética e conduta e das políticas e procedimentos internos. Incluem os riscos de fraudes em demonstrações financeiras e de desvios de ativos, de corrupção, de violação da privacidade, de vazamento de dados e de crimes cibernéticos.

Risco de Crédito: definido como a possibilidade de perda resultante da incerteza quanto ao recebimento de valores pactuados com tomadores de empréstimos, contrapartes de contratos ou emissões de títulos. Esse risco é principalmente proveniente das contas a receber de clientes e de caixa e equivalentes de caixa da Companhia.

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 3 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

Risco de Liquidez: possibilidade de perda decorrente da incapacidade de realizar uma transação em tempo razoável e sem perda significativa de valor ou da possibilidade de falta de recursos para honrar os compromissos assumidos em função do descasamento entre os ativos e passivos.

Risco de Mercado: risco de que alterações nos preços de mercado, tais como taxas de câmbio, taxas de juros e preços, possam afetar os ganhos da Companhia ou o valor de seus instrumentos financeiros.

Risco Estratégico: são aqueles 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. Também podem ser causados pela qualidade na gestão de eventos internos relativos às suas finanças (ambiente econômico, geração de caixa operacional, rentabilidade, endividamento, alavancagem, aplicação e captação de recursos financeiros), e às operações (cultura empresarial, e gestão de pessoas, de processos e de demais recursos).

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 (*marketing*, vendas e comercial) e como também à gestão de áreas de suporte ao negócio, tais como administrativas (contabilidade, controladoria, controles, suprimentos, saúde e segurança do trabalho, meio ambiente, tecnologia da informação e relações sindicais).

4. Fundamentos

As atividades de controle e de gerenciamento dos riscos devem ser desempenhadas em todos os níveis da Companhia e em vários estágios dentro dos processos corporativos.

Os processos, procedimentos e controles internos devem permitir que a administração e os demais gestores envolvidos gerenciem os Riscos de acordo com as políticas e os limites estabelecidos pelo Conselho de Administração para a Companhia, buscando um ambiente de continuidade e sustentabilidade dos negócios.

A gestão de riscos da Companhia está fundamenta nas boas práticas de mercado, nas orientações do *COSO ERM* e no processo de gestão de riscos sugeridos pela norma ISO 31000:2018, com intuito de:

- aumentar a probabilidade de atingir as metas estabelecidas pela Companhia;
- melhorar a identificação de oportunidades e ameaças;
- atender às políticas, normas e requisitos legais e regulatórios, padronizando conceitos e práticas;
- aperfeiçoar o *report* das informações ao mercado, elevando a confiança das partes interessadas e buscando garantir a transparência na comunicação a todos os stakeholders, analistas de mercado e agências de crédito;
- garantir base confiável de dados para a tomada de decisão e planejamento, fornecendo um fluxo dinâmico e eficiente de informação;
- alocar e utilizar eficazmente os recursos da Companhia, melhorando o ambiente de controles;
- melhorar a governança corporativa, assegurando que seja seguida e criticamente analisada;
- prevenir ou minimizar perdas, envolvendo todos os agentes da estrutura em alguma etapa;
- melhorar a eficácia e eficiência operacional, aumentando a resiliência da Companhia.

5. Estrutura de Gestão de Riscos

A estrutura de gestão de riscos da Companhia considera a atuação conjunta dos órgãos de governança corporativa e de gestão, de acordo com o conceito do modelo das três linhas:

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 4 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022



Corpo Administrativo: refere-se ao Conselho de Administração. Reporta e presta contas a todos os stakeholders e é responsável por:

- determinar a direção da organização, definindo a visão, missão, valores e Appetite organizacional a riscos; e
- delegar a responsabilidade pelo atingimento dos objetivos da organização à gestão, juntamente com os recursos necessários.

1ª Linha: refere-se à gestão operacional, representada pelas diretorias, gerências e demais colaboradores que atuam nas operações da Companhia. Reporta-se à Diretoria e, junto com ela, é responsável por:

- identificar, avaliar, monitorar e mitigar os Riscos (tratamento) de acordo com as diretrizes desta política;
- implantar planos de ação e controles; e
- comunicar/reportar, em tempo hábil, informações relevantes relacionadas à gestão de riscos.

2ª Linha: refere-se à área de Gestão de Riscos e Controles Internos e à área de Compliance. Reporta-se à Diretoria, ao Conselho de Administração e Comitê de Auditoria, sendo responsável por:

- analisar, avaliar, e monitorar os riscos identificados pela gestão operacional;
- facilitar e monitorar a implantação das práticas de gestão de riscos pela gestão operacional (1ª linha) de acordo com o Appetite a Risco da Companhia;
- comunicar/reportar, em tempo hábil, informações relevantes relacionadas à gestão de riscos; e

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 5 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

- auxiliar na identificação de riscos e no desenvolvimento de processos e controles.

3ª Linha: Refere-se à atuação da Auditoria Interna na avaliação e supervisão da aderência e eficácia do processo de gerenciamento de riscos na Companhia. Atua de forma independente e objetiva, reportando-se periodicamente ao Comitê de Auditoria e, no mínimo, semestralmente ao Conselho de Administração, ou quando julgar necessário.

6. Diretrizes

A Companhia identifica e trata os riscos a que está exposta de forma a garantir o cumprimento das metas estabelecidas em seu planejamento estratégico.

Anualmente, a alta administração define o perfil de riscos consolidado da Companhia por meio dos direcionadores e metas estratégicas para o Comitê de Auditoria. O Comitê de Auditoria, como base das orientações da alta administração, desempenha suas atribuições e faz suas recomendações periódicas para análise, avaliação e a tomada de decisões pelo Conselho de Administração da Companhia.

O processo de gestão de riscos da Companhia é composto pelas seguintes etapas:

6.1. Identificação de Riscos

A Companhia deve identificar eventos que podem impactar seus objetivos e estratégia. As principais técnicas utilizadas são:

- walkthrough (“passo a passo”) em entrevistas com pessoas chaves dos processos;
- entrevistas com profissionais do mercado com reconhecida capacidade técnica (auditores, consultores, advogados e outros);
- reuniões com participação de profissionais de diferentes funções e níveis hierárquicos para identificação de eventos de risco utilizando o conhecimento coletivo;
- análise de dados históricos para identificação de tendências;
- indicadores de risco; e/ou
- análise dos processos organizacionais, fluxogramas e descritivos para auxílio na identificação de suas entradas, processamentos, saídas e responsabilidades.

6.2. Análise dos Riscos

Os riscos identificados são analisados em conjunto com o dono do risco, área de controle e outras áreas da empresa, quando aplicável com sua capacidade de contribuição, visando a identificação correta dos riscos, das áreas e dos processos afetados diretamente ou indiretamente.

Os riscos devem ser classificados em categorias e para cada um deve-se dar um nome para codificação e referência. Os riscos identificados são classificados entre:

- Risco de Conformidade
- Risco de Crédito
- Risco de Liquidez
- Risco de Mercado
- Risco Estratégico

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 6 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

- Risco Operacional
- Risco Cibernético

6.3. Avaliação dos Riscos

O processo de avaliação dos riscos é aplicado aos riscos inerentes, e posteriormente, a partir das medidas de tratamento e resposta aos riscos, é aplicado aos riscos residuais:

Risco inerente: é risco para a Companhia sem considerar nenhuma ação para diminuí-lo, ou seja, não considera controles internos.

Risco residual: é o risco remanescente após ações ou implementação de controles internos.

A Companhia entende que o risco residual sempre estará presente e é função do Conselho de Administração determinar o quanto de risco residual é aceitável. Esta determinação está refletida no Apetite ao Risco.

6.3.1. Definição do Apetite ao Risco

Os direcionadores de Apetite ao Risco resultam das iniciativas conduzidas e propostas pela área de Gestão de Riscos e Controles Internos, alinhadas com o Comitê de Auditoria, e aprovadas pelo Conselho de Administração, valendo-se das análises e percepções de toda a Companhia, considerando aspectos de conformidade, financeiros, estratégicos, operacionais e tecnológicos.

A Boa Vista deve utilizar as seguintes premissas qualitativas para disseminar uma visão consolidada da companhia sobre o seu Apetite ao Risco:

- Os riscos assumidos precisam estar de acordo com a exposição de Apetite ao Risco da Boa Vista e oferecer retornos ajustados ao risco.
- A Boa Vista objetiva assumir apenas os riscos que a Companhia possa identificar, avaliar, medir, responder e comunicar.
- O Comitê de Auditoria deverá controlar a revisão anual do Apetite ao risco que deverá ser aprovada pelo Conselho de Administração.

6.3.2. Mensuração dos Riscos (Severidade)

Para determinação da severidade dos riscos identificados, a Companhia baseia-se na probabilidade e impacto de ocorrência de determinado evento. A metodologia de avaliação varia de acordo com o as particularidades de cada risco. A metodologia pode ser:

Qualitativa: utilizada quando há poucas informações disponíveis para quantificação ou caso a obtenção de informações não justifique o custo-benefício que dela se espera. Neste caso, a avaliação é efetuada por meio de entrevistas, reuniões e pesquisas.

Quantitativa: utilizado em atividades mais complexas e para complementar as técnicas qualitativas. Dentre as técnicas quantitativas estão a análise dos valores em riscos, histórico de ocorrência, fluxo de caixa em risco, análises de cenários, perda máxima esperada entre outros.

Quando determinadas a probabilidade e impacto de um risco, a Companhia as classifica em:

Probabilidade: Muito Alta, Alta, Média, Baixa e Muito baixa.

Impacto: Muito Alto, Alto, Médio, Baixo e Muito baixo.

Os riscos identificados e sua avaliação são formalizados em um Mapa de Riscos.

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 7 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

6.4. Tratamento dos Riscos

Após a avaliação de riscos, o Conselho de Administração da Companhia, deve definir qual a resposta desejada para cada um dos riscos e qual a prioridade a ser dada a cada um. As possíveis respostas aos riscos são:

- **Aceitar**: Nenhuma ação é tomada. Esta resposta é utilizada quando o risco está dentro do Apetite a Risco definido pela Companhia.
- **Evitar**: implica na remoção do risco. Esta resposta é utilizada quando a Companhia não encontrou alternativas para mitigação do risco até um nível aceitável, ou seja, que se encaixe em seu Apetite a Risco.
- **Reduzir**: a Companhia decide reduzir o grau do risco, pois está acima do Apetite a Risco. Neste caso, controles internos são implementados.
- **Transferir**: similar ao item reduzir, com a diferença que, ao transferir, a Companhia repassa parte do risco para terceiros (exemplo: contratação de seguro ou terceirização de atividades).

6.5. Monitoramento dos Riscos

Os riscos identificados são monitorados por meio de:

- revisão anual dos riscos;
- discussões trimestrais pelo Comitê de Auditoria e Conselho de Administração em reuniões sobre os riscos;
- revisões dos controles internos e grau de exposição ao risco pela área de Gestão de Riscos e Controles Internos; e
- acompanhamento de indicadores de risco.

7. Instrumentos - Controles

Além disso, a Companhia possui os seguintes instrumentos de controle para mitigação de seus riscos:

Risco de Conformidade: há monitoramento contínuo pelo departamento de relações governamentais e por prestador de serviço terceirizado 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, o departamento de relações governamentais compartilha tais fatos em reunião de Diretoria para definição de plano de ação, se necessário. Além disso, a Companhia possui programa de Compliance que inclui treinamentos periódicos sobre o tema, a implementação de canal de denúncia com garantia de anonimato e não retaliação ao denunciante de boa-fé, Código de Conduta e Auditoria Interna para assegurar o devido funcionamento dos controles internos relacionados a Compliance.

Risco de Crédito: O gerenciamento do risco de crédito se dá pelo próprio modelo operacional da Companhia, no qual a imensa maioria das vendas é realizada na modalidade de venda a prazo com exíguo prazo para pagamento. Ainda assim, são feitas análises periódicas do nível de inadimplência dos clientes, bem como são adotadas formas eficazes de cobrança. A concessão de crédito pela Companhia é feita seguindo critérios definidos com base em modelos estatísticos - *score*, combinados com informações internas próprias do negócio da Companhia, assim como informações internas, cadastrais ou comportamentais dos consumidores, sendo esses modelos periodicamente revisados com base nos índices de perdas históricas das safras de concessão da carteira. Além disso, o risco de crédito de saldos com bancos e instituições financeiras é administrado pela tesouraria da Companhia. Os recursos excedentes são investidos apenas em contrapartes aprovadas e dentro do limite estabelecido a cada uma, a fim de minimizar a concentração de riscos e, assim, mitigar o prejuízo financeiro no caso de potencial falência de uma contraparte.

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 8 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

Risco de Liquidez: a Companhia promove o gerenciamento por meio do monitoramento diário da liquidez e dos fluxos de caixa previstos e reais, para garantir que a geração operacional de caixa e a captação prévia de recursos, quando necessário, sejam suficientes para manutenção do seu cronograma de compromissos, mitigando, assim, os riscos de liquidez para a Companhia. Além disso, a Companhia monitora a combinação dos perfis de vencimento dos ativos e passivos financeiros e mantém 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, e possui como prática em relação a títulos de dívida (aplicações financeiras) o investimento em títulos que possuem grau de investimento atribuído por pelo menos uma das principais agências de risco de crédito, com exceção dos títulos do Banco do Brasil. Adicionalmente, dentre as alternativas para a mitigação do risco de liquidez, estão: captação de recursos junto a terceiros com vencimento de longo prazo, reestruturação de dívidas e, se necessário, a obtenção de recursos adicionais de acionistas.

Risco de Mercado: a área de economia da Companhia produz relatórios diários, semanais e mensais a respeito de oscilações de taxas de juros, do câmbio, dos preços das ações e dos preços de commodities que possam impactar o valor dos ativos da Companhia. Tais relatórios são produzidos com base em informações do Banco Central do Brasil, instituições financeiras, veículos de mídia de grande circulação, agências de rating e outros. Pontualmente, a Companhia contrata consultorias econômicas para avaliação de cenários que possam impactar o bom andamento de suas operações. Quando da identificação de fatos relevantes, o departamento de economia os compartilha em reunião de diretoria para definição de plano de ação, se necessário. No âmbito do risco de mercado, a Companhia pode incorrer em risco cambial, que resulta de instrumentos financeiros em moedas diferentes de sua moeda funcional, e risco de taxa de juros, que decorre de aplicações financeiras e empréstimos. Para mitigação do risco cambial, a Companhia deve utilizar derivativos por meio de swap cambial para proteger a geração de fluxos de caixa contra a variação cambial. Para mitigação do risco de taxa de juros, a administração da Companhia mantém na sua maioria os indexadores de suas exposições a taxas de juros ativas e passivas atrelados a taxas pós-fixadas. As aplicações financeiras são corrigidas pelo CDI e os empréstimos e financiamentos são corrigidos pela Taxa de Juros de Longo Prazo - TJLP, CDI, conforme contratos firmados com as instituições financeiras. Além disso, a Companhia prepara análise de sensibilidade para simular o impacto das variações nas taxas de juros das aplicações financeiras, empréstimos e financiamentos, swap e debêntures, a fim de demonstrar os saldos dos principais ativos e passivos financeiros, considerando 3 cenários sendo: (i) cenário provável (Cenário I); (ii) cenário com apreciação de 25% (Cenário II) e; (iii) cenário com apreciação de 50% (Cenário III). A Companhia revisa regularmente as estimativas e premissas utilizadas nos cálculos, no entanto, a liquidação das transações envolvendo essas estimativas poderá resultar em valores diferentes dos estimados devido à subjetividade inerente ao processo utilizado na preparação das análises.

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 resultados com a remuneração atrelada ao desempenho no cumprimento de metas (departamentais e individuais) diretamente atreladas à execução de sua estratégia. Há reuniões mensais 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. Além disso, o departamento comercial da Companhia monitora de forma contínua ações dos concorrentes que possam impactar na sua estratégia. Informações relevantes são levadas à reunião de diretoria para tomada de ação, se necessário.

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 pela área de Gestão de Riscos e Controles Internos e implementadas pelos gestores dos processos. A equipe de Auditoria Interna acompanha o andamento dos planos

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 9 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

de ação para correção das falhas nos controles até a sua conclusão, e se reporta ao Comitê de Auditoria. 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.

Risco Cibernético: a Companhia possui um Plano de Continuidade dos Negócios implantado para diminuição do tempo de resposta em caso de incidentes tecnológicos que impeçam ou dificultem o bom andamento das operações, tais como ataques cibernéticos, destruição de servidores, restrição de acesso aos sistemas de informação, perda de informações relevantes e outros. São efetuados testes periódicos do Plano de Continuidade dos Negócios para assegurar que os profissionais estejam devidamente treinados para sua execução em tempo adequado para diminuir impactos na operação da Companhia. Além do Plano de Continuidade dos Negócios, a empresa possui Plano de Gerenciamento de Crises para garantir a agilidade necessária na resolução de eventos que impactem de forma relevante e repentina o andamento da operação. Neste plano, são definidas as funções dos profissionais e a forma de ação em caso de crises. Para reforço da segurança de sua infraestrutura de tecnologia e sistemas de informação, a Companhia poderá contar com um prestador de serviços terceirizado 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.

8. Atribuições e Responsabilidades

8.1. Conselho de Administração

- estabelecer as diretrizes gerais das estratégias de gestão de riscos da Companhia;
- avaliar e aprovar as diretrizes gerais para estabelecimento dos limites aceitáveis para Appetite a Riscos.
- supervisionar as atividades do processo de gerenciamento de riscos, executadas pelo Comitê de Auditoria e Comitê de Riscos.
- Utilizar a atuação do Comitê de Auditoria no processo de monitoramento de riscos prioritários.
- avaliar a adequação da estrutura (recursos humanos, financeiros e sistemas) destinada ao processo de gerenciamento de riscos.
- aprovar esta política e suas futuras revisões.

8.2. Diretoria e Presidente:

- promover a integração da gestão de riscos com os ciclos de gestão e planejamento da Companhia.
- promover a cultura de gestão de riscos na Companhia.
- garantir a implantação de um modelo eficiente de gestão de riscos, alinhado aos objetivos de negócios e metas operacionais.
- a partir das diretrizes gerais estabelecidas pelo Conselho de Administração, propor o nível de Appetite a Risco em função da relação "risco x retorno" que ela pretende assumir.
- acompanhar os riscos gerenciados no nível de cada macroprocesso e/ou operação, para verificar a efetividade dos controles existente.
- participar da validação e priorização dos riscos de suas respectivas áreas.
- acompanhar os indicadores e as estratégias de mitigação dos riscos prioritários.

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 10 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

- avaliar e monitorar o tratamento dos riscos de negócio quando da execução do planejamento estratégico.
- garantir a adequação da estrutura (recursos humanos, financeiros e sistemas) destinada ao processo de gerenciamento de riscos

8.3. Comitê de Auditoria (por delegação do Conselho de Administração):

- propor ao Conselho de Administração as definições gerais das estratégias de gestão de riscos da Companhia.
- acompanhar e supervisionar o processo de gestão de riscos, bem como a aplicação dos indicadores e as estratégias de mitigação dos riscos prioritários, através dos trabalhos do agente responsável pela função de gestão de riscos e controles internos e da Auditoria Interna.
- avaliar, monitorar e informar periodicamente o Conselho de Administração sobre os riscos prioritários identificados pelas revisões do agente responsável pela função de Gestão de Riscos e Controles Internos e da Auditoria Interna, bem como os planos de ação e recomendações aplicáveis.
- aprovar e acompanhar a execução do plano anual de auditoria baseado em Riscos.

8.4. Área de Gestão de Riscos e Controles Internos

- elaborar o planejamento e assegurar a operacionalização da gestão de riscos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais.
- avaliar com cada área operacional os Riscos por macroprocesso, por unidades de negócio e portfólio.
- elaborar, treinar, disseminar e recomendar os processos e procedimentos para a gestão dos Riscos prioritários.
- desenvolver, testar e implantar os modelos e metodologias para mensuração e gestão dos Riscos.
- suportar as áreas de negócio na definição do plano de ação/contingência.
- atuar como verificador da correta gestão de riscos da Companhia, e informar ao e discutir com o Comitê de Auditoria os resultados de suas avaliações através de relatórios periódicos.
- Definir a metodologia corporativa de gestão de riscos pautada na visão integrada e sistêmica das atividades da Companhia.
- Propor e analisar, em conjunto com as áreas funcionais e de negócios, as estratégias de mitigação dos riscos.
- Estabelecer ações de mitigação para os riscos prioritários.
- Consolidar e comunicar os Riscos prioritários da Companhia ao Comitê de Auditoria e à Diretoria.
- Assessorar as áreas de funcionais e de negócios na identificação e avaliação do impacto dos diversos tipos de riscos envolvidos.
- Executar as tarefas que permitirão um adequado monitoramento dos riscos prioritários (estratégicos, financeiros, operacionais e de conformidade) e informar e discutir com o Comitê de Auditoria os resultados de suas avaliações através de relatórios periódicos.

8.5. Área de Compliance

- emitir parecer sobre a viabilidade das operações relacionadas ao Risco de Conformidade.
- fazer a interface das áreas de negócios e funcionais com a área de Gestão de Riscos e Controles Internos.

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 11 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

8.6. Auditoria Interna (com base nas diretrizes do Conselho de Administração e Comitê de Auditoria):

- elaborar o Plano Anual de Auditoria, a fim de verificar a eficácia dos controles internos e a efetividade da gestão de Riscos.
- identificar e apontar oportunidades de melhorias nos processos de controle internos e de gestão riscos.
- validar as informações e controles relacionados aos indicadores de Risco desenvolvidos e monitorados pelas áreas funcionais
- reportar periodicamente ao Comitê de Auditoria e administrativamente à Diretoria os resultados de avaliações independentes, imparciais e tempestivas sobre a efetividade da gestão de Riscos na Companhia.

8.7. Colaboradores:

- assegurar a operacionalização da gestão de riscos, fazendo parte do processo de identificação, avaliação e mensuração, implementando ações de mitigação preventivas e corretivas.
- participar de forma ativa na comunicação e treinamento que permita a disseminação de forma consciente da gestão de riscos na Companhia.

8. Infrações e Sanções

Sem prejuízo das sanções cabíveis a serem aplicadas pelas autoridades competentes, em caso de violação dos termos e procedimentos estabelecidos nesta política, estará sujeito a penalidades de acordo com a política BVS - 006 Tratamento de Incidentes e Violações.

Nos casos específicos previstos na política BVS-006 Tratamento de Incidentes e Violações, caberá ao Conselho de Administração da Companhia tomar as medidas disciplinares cabíveis no âmbito interno da Companhia, inclusive a destituição do cargo ou demissão do infrator na hipótese de infração grave, conforme previsto na Lei nº 6.385, de 07 de dezembro de 1976 e suas alterações.

Caso a infração seja praticada por terceiros, esta caracterizará inadimplemento contratual, podendo a Companhia, sem qualquer ônus, resolver o respectivo contrato e exigir o pagamento da multa estabelecida, sem prejuízo de perdas e danos.

Na hipótese, da medida cabível ser de competência legal ou estatutária da Assembleia Geral, deverá o Conselho de Administração da Companhia convocá-la para deliberar sobre o tema.

9. Vigência

Esta política aprovada em Reunião do Conselho de Administração, em 21/10/2022, entrará em vigor a partir de sua divulgação pela ferramenta de comunicação da Companhia.

A alteração desta política poderá ocorrer desde que deliberada em Reunião pelo Conselho de Administração da Companhia.

10. Histórico de Revisões

Revisão N°	Data	Descrição das Alterações
00	09/09/2019	Versão inicial

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 12 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

01	15/07/2020	<p>Tópico 3 – Risco Legal: associação do risco à “vazamento de informação e privacidade de dados”.</p> <p>Tópico 3 – Risco de Tecnologia da Informação: associação do risco à ‘segurança da informação’</p>
02	30/09/2020	<p>Versão revisada para fins de atender Regulamento de Listagem do Novo Mercado” da B3 S.A., sendo a primeira versão aprovada pelo Conselho de Administração. Principais alterações:</p> <p>Tópico 1 – inseridos fundamentos da política, e incluídos nesse tópico Elegibilidade (anteriormente tópico 2) e Aplicações (anteriormente tópico 4).</p> <p>Tópico 2 (anteriormente Tópico 3) – inclusão dos conceitos de ‘Apetite ao Risco’, ‘KRI’, ‘Risco Cibernético’ / alteração de nomenclatura do ‘Risco Legal’ para ‘Risco de Conformidade’ / exclusão do conceito de ‘Risco de Tecnologia’</p> <p>Tópico 3 (anteriormente Tópico 5) – alteração de nomenclatura de ‘Disposições Gerais’ para ‘Princípios e Objetivos da Gestão de Riscos’ / atualização de texto e revisão dos objetivos, explicitando pontos de atendimento às políticas, normas e requisitos legais e regulatórios, assim como no reporte das informações ao mercado / exclusão do tópico ‘Apetite ao Risco’</p> <p>Tópico 4 (anteriormente Tópico 6 e 6.1) – atualização de texto / transferência das categorias ou classificação de riscos para o tópico 4.3.2, sub-item da ‘Identificação de Riscos’</p> <p>Tópico 4.3.3 – separação de mensuração da avaliação, inclusão do tópico ‘Apetite ao Risco’ com sub-item de ‘Avaliação de Riscos’</p> <p>Tópico 4.3.4 – detalhamento da etapa de mensuração, e definição de critérios nos tópicos 4.3.5 e 4.3.6</p> <p>Tópico 4.3.7 – alteração de nomenclatura de ‘Respostas’ para ‘Priorização e Respostas aos Riscos’ com definição de conceito para possíveis respostas</p> <p>Tópico 4.3.8 – atualização do texto considerando alteração de estrutura de reporte da gestão de Riscos</p> <p>Tópico 4.4 – inclusão de tópico para tratar de instrumentos de controle, com definição de controles para mitigação de cada uma das categorias de risco possíveis nos tópicos 4.4.1 a 4.4.7</p> <p>Tópico 5 (anteriormente Tópico 6.2) – alteração de nomenclatura de ‘Linhas de Defesa’ para ‘Estrutura de Gestão de Riscos’ e inclusão do Corpo Administrativo na estrutura de gestão / atualização de texto das responsabilidades de cada linha de defesa, considerando Regulamento de Listagem do Novo Mercado</p> <p>Tópico 6 (anteriormente Tópico 7) – inclusão de responsabilidades</p> <p>Tópico 7 (anteriormente Tópico 8) – alteração de nomenclatura de ‘Penalidades’ para ‘Infrações e Sanções’</p> <p>Tópico 8 – inclusão de tópico para disposições gerais</p> <p>Tópico 9 – revisão das condições para consideração da vigência da política</p> <p>Anterior Tópico 10 – exclusão do tópico de ‘Histórico de Revisões’</p>
03	22/10/2020	<p>Tópico 2 e tópico 3.3 - retirada das citações de COSO ERM /ISO31000</p> <p>Tópico 2.1.11 - inclusão do texto “de violação da privacidade, de vazamento de dados” para o risco de conformidade</p> <p>Criação do tópico 4.4.3 B1 Appetite ao risco, excluindo essa informação do tópico B Avaliação de Riscos</p> <p>Tópico 4.3.4 – acrescentado a técnica qualitativa: “histórico de ocorrência”</p> <p>Tópico 4.3.7 – retirado “Explorar” das possíveis resposta ao risco e alterado a resposta “compartilhar” por “transferir”</p> <p>Tópico 4.4.3 – atualização do texto</p> <p>Tópico 4.4.4 – atualização do texto</p> <p>Tópico 5.1 – atualização das “três linhas de defesa” para “modelo das três linhas”</p> <p>Tópico 6 – realocação das atribuições das responsabilidades entre os papéis existentes.</p>

POLÍTICA CORPORATIVA	BVS-21
Gestão de Riscos Corporativos	Página: 13 de 13
	Versão: 06
Aprovador: Conselho de Administração	Data de Emissão: 21/10/2022

		Tópico 10 – reinclusão do ‘Histórico de Revisões’
04	12/08/2021	Alterada a padronização de acordo com aprovação em Reunião do Conselho de Administração, em 12 de agosto de 2021.
05	11/11/2021	Ajustes no texto ao decorrer de toda a política. Reestruturação da ordem dos tópicos. Tópico 6.1. Excluído item de “benchmark” e inclusão de “walkthrough”.
06	21/10/2022	Emissão de nova versão após revisão anual das Políticas Corporativas.