VALEC ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A.

**RESOLUÇÃO NORMATIVA VALEC Nº 12/2022/CONSAD-VALEC**

Brasília, 23 de maio de 2022.

Dispõe sobre o Processo de Gestão de Riscos e Controles Internos no âmbito da VALEC - ENGENHARIA, CONSTRUÇÕES e FERROVIAS S.A., conforme Manual de Gestão de Riscos e Tutorial de Gestão de Riscos.

O CONSELHO DE ADMINISTRAÇÃO da VALEC - ENGENHARIA, CONSTRUÇÕES e FERROVIAS S.A., no exercício de sua competência prevista no inciso XII do art. 42 do Estatuto Social vigente e considerando o deliberado na 396ª Reunião Ordinária, realizada em 28 de abril de 2022, conforme consta no processo 51402.107129/2021-99,

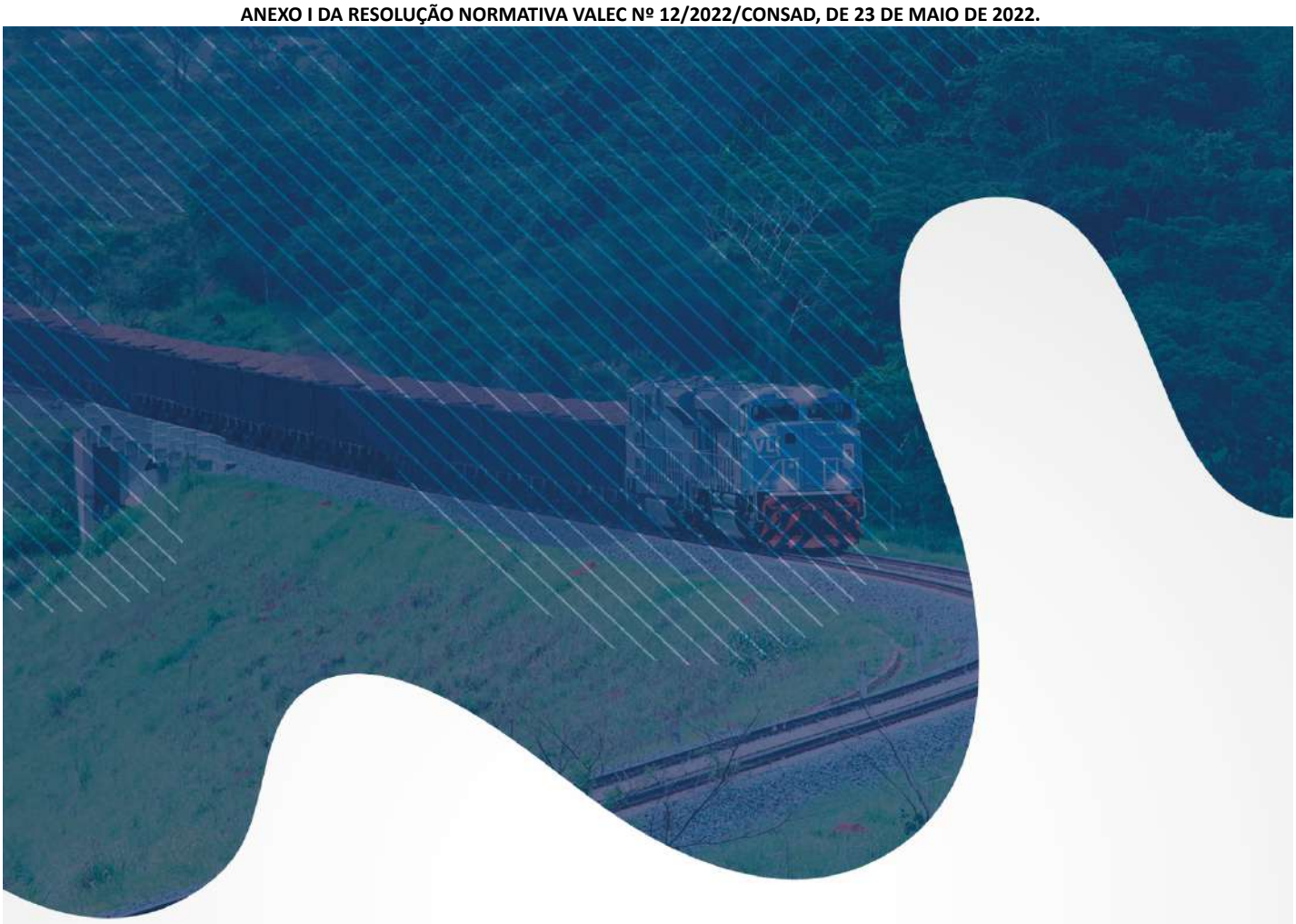
RESOLVE:

Art. 1º Aprovar o Manual de Gestão de Riscos e o Tutorial de Gestão de Riscos da Valec, nos termos dos anexos desta Resolução.

Art. 2º Esta Resolução entra em vigor a partir da data da sua publicação.

(*assinado eletronicamente*)
MARCELLO DA COSTA VIEIRA
Presidente do Conselho de Administração

**ANEXO I DA RESOLUÇÃO NORMATIVA VALEC Nº 12/2022/CONSAD, DE 23 DE MAIO DE 2022.**



# MANUAL DE GESTÃO DE RISCOS DA VALEC

VALEC Engenharia, Construções e Ferrovias S.A.

MINISTÉRIO DA INFRAESTRUTURA

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

**MANUAL DE GESTÃO DE RISCOS**

**VALEC - ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A.**
Edifício Sede - SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5 - Asa Sul - 70.070-010 –
Brasília – DF - tel: +61 2029 6100
https://www.valec.gov.br
**Diretor-Presidente**
André Kuhn
**Superintendente de Integridade**
Nelbe Ferraz de Freitas
**Gerente de Riscos e Controles Internos**
Paulo Cézar Rabelo
**Equipe da Gerência de Riscos e Controles Internos**
Pablo Anderson Alves

## SUMÁRIO

## 1. Objetivo

O Manual e Tutorial de Gestão de Riscos têm como objetivo estabelecer as diretrizes a serem observadas no Processo de Gestão de Riscos da Valec Engenharia, Construções e Ferrovias S.A., com vistas à definição de estratégias, ao alcance de objetivos e na tomada de decisões fundamentadas, tendo como pressupostos:

I. Apoiar a governança da Valec;
II. Aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas;
III. Aprimorar os controles internos;
IV. Resguardar a Administração da Valec e os demais gestores quanto à tomada de decisão e à prestação de contas;
V. Explicitar o apetite de risco da Valec;
VI. Manter a estrutura apropriada de governança de risco;
VII. Estabelecer critérios e parâmetros para identificação, avaliação, monitoramento e controle dos riscos relevantes da empresa;
VIII. Disseminar a cultura de Gestão de Riscos, especificando o perfil de risco adotado, introduzindo uma linguagem comum para o assunto "riscos" em todos os níveis da organização;
IX. Garantir que os processos e procedimentos relacionados a Gestão de Riscos da Valec atendam aos requerimentos regulatórios vigentes, bem como às melhores práticas nacionais e internacionais; e
X. Integrar as informações relacionadas a riscos e controles de gestão ao processo de Planejamento Estratégico da Valec, para a consecução dos objetivos institucionais.

## 2. Princípios

A Gestão de Riscos da Valec, tendo como referências as melhores práticas internacionais de gestão de riscos, focando a criação e proteção de valor para a empresa, observará princípios, que servem de orientação para que a gestão de riscos seja eficiente e eficaz. A Gestão de Riscos eficaz requer (precisa ser/ter) os seguintes elementos:

I. Integrada. A gestão de riscos é parte integrante de todas as atividades organizacionais;
II. Estruturada e abrangente. Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis;
III. Personalizada. A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos;
IV. Inclusiva. O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada;
V. Dinâmica. Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna;
VI. Melhor informação disponível. As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes;
VII. Fatores humanos e culturais. O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio; e
VIII. Melhoria contínua. A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

As diretrizes e princípios estabelecidos no Manual de Gestão de Riscos se aplicam aos órgãos sociais e estatutários; aos colaboradores e aos prestadores de serviços diretos e indiretos naquilo que couber.

## 3. Conceitos

**Apetite a risco -** Grau de exposição (nível de risco) que uma organização está disposta a aceitar na busca dos seus objetivos.

**Causas -** Elementos, situações ou condições que têm o potencial de dar origem aos eventos de riscos.

**Consequência -** Resultado e impacto no cumprimento dos objetivos da organização no caso de materialização do risco.

**Controles internos -** Conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de empregados, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:

a - Execução ordenada, ética, econômica, eficiente e eficaz das operações;

b - Cumprimento das obrigações de *accountability*;

c - Cumprimento das leis e regulamentos aplicáveis; e

d - Salvaguarda dos recursos para evitar perdas, mau uso e danos.

O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.

**Evento -** Um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.

**Gerenciamento de riscos -** Processo com estrutura orientada com vistas à identificação, análise, avaliação e tratamento dos eventos de riscos, de forma a fornecer razoável certeza quanto ao alcance dos objetivos da organização.

**Grau de exposição (nível de risco) -** Valor numérico obtido a partir multiplicação entre a pontuação atribuída à probabilidade e a pontuação atribuída ao impacto, de acordo com as escalas de probabilidade e impacto da empresa.

**Incerteza -** Incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

**Matriz de riscos -** Matriz gráfica composta pelo conjunto de combinações de probabilidade e impacto, de forma a apresentar o grau de criticidade dos eventos de riscos com base no grau de exposição (nível de risco).

**Mensuração de risco -** Significa estimar a importância de um evento de risco, bem como a probabilidade e o impacto de sua ocorrência.

**Modelo das três linhas -** Modelo que apresenta a estrutura da gestão de riscos e controles internos de uma organização, no intuito de definir os papéis e responsabilidades dos diversos setores, considerando os órgãos de governança, a gestão e a auditoria interna.

**Risco -** Possibilidade de ocorrência de um evento que venha a ter resultado e impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e probabilidade.

**Risco inerente -** Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

**Risco residual -** Risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento dos riscos.

**Tolerância a risco (limite de exposição) -** Grau de exposição (nível de risco) acima do qual o evento de risco passa a ser objeto de priorização no processo de gestão de riscos, em função de estar além do apetite a riscos da organização.

## 4. Responsabilidades

A estrutura da gestão de riscos e controles internos em uma organização é formada por três linhas. Este item trata da descrição dos papéis e responsabilidades, considerando o modelo das três linhas para gestão de riscos e controles internos no âmbito da Valec.

### 4.1 Primeira Linha

Conforme a Política de Gestão de Riscos, Controle e Conformidade, a primeira linha é composta pelas unidades organizacionais responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio da Valec. São as unidades organizacionais que executam as ações referentes a implementação da gestão de riscos e respectivos controles.

Considerando o Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020) e, Instrução Normativa Conjunta CGU/MP (Controladoria-Geral da União e Ministério do Planejamento, Orçamento e Gestão) n° 01, de 10 de maio de 2016, são papéis da primeira linha:

I. Identificar, analisar, avaliar e gerir os eventos de riscos, de forma a atingir os objetivos organizacionais;
II. Elaborar os planos de tratamento, bem como implementar e manter mecanismos de controles internos;
III. Implementar as ações efetivas para aprimorar os controles e solucionar inconsistências ou erros eventualmente identificados;

IV. Assegurar que os procedimentos efetivos de implementação de controles internos integrem as suas práticas de gerenciamento de riscos; e

V. Comunicar à segunda linha (Superintendência de Integridade-SUINT) as situações relevantes ou críticas do processo de gerenciamento de riscos, assim como os novos eventos de riscos, eventos de riscos com aumento do grau de exposição, iminência ou materialização do risco e situações com necessidades imediatas de implementação de controles.

### 4.2 Segunda Linha

Composta pela Superintendência de Integridade-SUINT, unidade organizacional de gestão de riscos vinculada à Presidência. Conforme Estatuto Social e Regimento Interno, são as atribuições:

I. Prestar apoio e suporte metodológico para a gestão de riscos e controles internos nas unidades organizacionais;

II. Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a empresa;

III. Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;

IV. Coordenar a comunicação de informações relativas as boas práticas de gestão de riscos e controles internos;

V. Gerenciar e monitorar o sistema de controles internos que tem por objetivo salvaguardar os ativos, verificar a exatidão e fidelidade dos dados contábeis, desenvolver a eficiência nas operações e estimular o seguimento das políticas institucionais;

VI. Propor revisão e alteração da Política de Gestão de Riscos e de Controles Internos;

VII. Gerenciar a elaboração e aplicação da metodologia e dos procedimentos para a gestão de riscos e controles internos, monitorando a sua eficiência e eficácia; e

VIII. Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria Estatutário.

Trimestralmente, a SUINT elabora o relatório acerca da gestão de riscos e controles internos, para envio à Diretoria Executiva, para posterior análise e deliberação do Conselho de Administração.

### 4.3 Terceira Linha

Composta pela Auditoria Interna. As atribuições da Auditoria Interna constam no Regimento Interno da Auditoria Interna, Resolução Valec n° 7/2020/CONSAD-Valec. São as atribuições:

I. Fornecer asseguração aos órgãos de governança e de gestão de que os processos de gestão de riscos operam de maneira eficaz e os maiores riscos do negócio são gerenciados adequadamente em todos os níveis da organização; e

II. Apoiar a estruturação e o funcionamento da primeira e da segunda linhas de defesa da gestão, por meio da prestação de serviços de avaliação ou de consultoria.

## 5. Processo de Gestão de Riscos

O processo de gestão de riscos, com base na ABNT NBR ISO 31000:2018, compreende as seguintes etapas: estabelecimento do contexto, identificação, análise, avaliação e tratamento dos riscos, comunicação e consulta e monitoramento e melhoria contínua.

### 5.1 Estabelecimento do Contexto

Esta etapa consiste em compreender o ambiente externo e interno no qual o objeto da gestão de riscos se encontra inserido e identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

Esta etapa é conduzida pela SUINT e é realizada a partir de oficinas de instrução com as diretorias.

O objetivo desta etapa é definir: quais são os objetos da gestão de riscos mais importantes na Valec; quais são os objetivos, metas e iniciativas relacionadas com esses objetos de gestão de riscos; quais são os fatores externos e internos que podem afetar no alcance desses objetivos e resultados; e, quais são os processos de trabalho relevantes para alcance desses objetivos e resultados.

O estabelecimento do contexto para o processo de gestão de riscos deve ser realizado com base no Planejamento Estratégico Institucional-PEI e no Plano de Negócios.

Portanto, o estabelecimento do contexto deve considerar os seguintes elementos:

- políticas públicas e legislação correlacionada;

- ambiente externo (cenário político, institucional, social, financeiro, legal, tecnológico, econômico etc.);
- ambiente interno (sistemas, estrutura organizacional, recursos e partes interessadas);
- modelo de negócios;
- os objetivos e resultados esperados constantes no planejamento estratégico;
- principais objetos (empreendimentos, programas, negócios) do planejamento estratégico;
- processos de trabalhos; e
- pessoas envolvidas nesses processos e especialistas nas áreas.

### 5.2 Identificação dos Riscos

A partir da instrução do processo, realizada com base nos elementos da etapa de estabelecimento do contexto, esta etapa consiste na identificação dos eventos de riscos que podem impedir, prejudicar ou atrasar o alcance dos principais objetivos organizacionais.

Esta etapa é conduzida pela SUINT e é realizada a partir de oficinas de instrução com as diretorias, superintendências e gerências. No nível estratégico, as oficinas de instrução para identificação dos eventos de riscos são realizadas com as diretorias. No nível tático e operacional, as oficinas de instrução para identificação dos eventos de riscos são realizadas com as superintendências e gerências e, posteriormente aprovadas pela diretoria.

Nesta etapa também devem ser relacionadas as seguintes informações referentes aos eventos de riscos: objeto relacionado (empreendimentos, programas, negócios, dentre outros); objetivos, metas e iniciativas; causas e consequências; e, nível da organização no qual o evento de risco abrange (estratégico, tático ou operacional), tipo e categoria.

### 5.3 Análise dos Riscos

Após as etapas de estabelecimento do contexto e identificação de riscos, devem ser realizadas as oficinas para as etapas de análise, avaliação e tratamento dos riscos. Estas oficinas são conduzidas pela SUINT e realizadas com as diretorias, superintendências e gerências, de acordo com o nível da organização que o risco abrange. No nível estratégico, as oficinas são realizadas com as diretorias. No nível tático e operacional as oficinas são realizadas com as superintendências e gerências e, posteriormente aprovadas pela diretoria.

Esta etapa compreende o cálculo do grau de exposição da empresa ao evento de risco identificado. O grau de exposição (nível de risco) é calculado a partir de critérios de probabilidade e impacto. Destarte, para cada evento de risco são atribuídos valores a partir de uma escala de probabilidade e de impacto, conforme os quadros constantes no Tutorial de Gestão de Riscos, anexo II desta resolução.

A multiplicação entre os valores atribuídos para probabilidade e impacto define o grau de exposição ao evento de risco, nesta etapa definido como risco inerente, pois não são considerados neste cálculo quaisquer controles que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Uma vez analisado na superintendência ou gerência e aprovado pela respectiva diretoria, o grau de exposição somente pode ser alterado com a apresentação das razões de justificativas. As razões de justificativas são analisadas pela SUINT, no qual é responsável por emitir o parecer recomendativo à diretoria.

### 5.4 Avaliação dos Riscos

Na etapa de avaliação é verificado se o grau de exposição ao evento de risco está ou não, além do apetite a riscos definido pelo Conselho de Administração-CONSAD. Compete ao Conselho de Administração definir o apetite a riscos da empresa.

Com base na matriz de riscos, a partir do grau de exposição, o evento de risco pode ser classificado de acordo com quatro graus de criticidade: baixo, médio, alto ou extremo.

Após a avaliação, deve ser apresentada uma resposta ao evento de risco de acordo com o grau de exposição. Esta resposta é apresentada na etapa de tratamentos dos riscos.

### 5.5 Tratamento dos Riscos

Esta etapa compreende a implementação das soluções aos eventos de riscos. Na descrição dessas soluções, podem ser estabelecidas quatro possíveis respostas ao evento de risco: aceitar, mitigar, transferir ou evitar.

Caso já existam os controles, estes são analisados e verificados, para efeitos de cálculo do risco residual. Caso não existam os controles, o evento de risco é caracterizado como inerente.

Os eventos de riscos que devem ser objeto de mitigação e priorização na etapa de tratamento, são aqueles classificados com grau de criticidade alto ou extremo, pois conforme limite de exposição na matriz de riscos, estão além do apetite a riscos da Valec.

Caso a resposta seja mitigar o evento de risco, devem ser elaborados os planos de tratamento (planos de ação) com a implementação de novos controles ou aprimoramento dos controles internos existentes, com as ações no sentido de reduzir a probabilidade de sua ocorrência ou seu impacto.

Após a conclusão do plano de tratamento, com base nas ações implementadas é realizado o cálculo do risco residual, de forma a verificar se o evento de risco foi mitigado, ou seja, se está abaixo do limite de exposição na matriz de riscos.

As informações constantes nas etapas de análise, avaliação e tratamento, devem ser enviadas para as respectivas diretorias para a análise, aprovação e posterior envio à SUINT.

As informações do processo de gestão de riscos integram o relatório trimestral referente a gestão de riscos e controles internos, elaborados pela SUINT, que são enviados para a Diretoria Executiva, para posterior análise e deliberação do Conselho de Administração.

### 5.6 Comunicação e Consulta

Esta etapa permeia todo o processo de gestão de riscos e consiste no fornecimento de informações relativas ao evento de risco e ao seu tratamento para todos que possam diretamente influenciar ou ser influenciados por esse evento de risco, sob pena de ele se materializar plenamente.

O propósito desta etapa é prestar assistência e apoio metodológico às partes interessadas, a respeito da compreensão dos riscos e de todas as etapas do processo de gestão de riscos, de forma a fornecer bases e subsídios para tomada de decisões e as razões pelas quais ações específicas são exigidas no processo. A assistência e apoio metodológico é de responsabilidade da SUINT.

O fluxo de comunicação das informações da gestão de riscos pode ser horizontal ou vertical.

A comunicação horizontal, quando envolve diversas unidades de diferentes diretorias, é feita a partir da interlocução da SUINT com as diretorias e superintendências, no intuito de integrar as informações e instruir o processo de gestão de riscos.

A comunicação vertical é no sentido da unidade organizacional para o órgão máximo de governança da estatal, o Conselho de Administração, ou vice-versa. É quando o processo e o evento de risco envolvem especificamente uma unidade.

No que tange ao fluxo de comunicação horizontal e vertical, trimestralmente a SUINT elabora o relatório acerca da gestão de riscos e controles internos, para envio à Diretoria Executiva, para posterior análise e deliberação do Conselho de Administração.

A comunicação visa a promover a ciência e a compreensão dos eventos de riscos e, a consulta, envolve a obtenção de *feedbacks* e informações necessárias para o apoio à tomada de decisão. A coordenação adequada entre a comunicação e a consulta favorece a troca de informações precisas, relevantes, oportunas e baseadas em evidências factuais, levando em consideração a confidencialidade e a integridade da informação.

### 5.7 Monitoramento e melhoria contínua

Esta etapa permeia todo o processo de gestão de riscos e consiste em detectar mudanças no ambiente externo e interno, que podem alterar as informações relacionadas aos eventos de riscos identificados ou a identificação de novos riscos.

O monitoramento também compreende o acompanhamento e a verificação do desempenho ou da situação dos elementos da gestão de risco, bem como a revisão da política, do manual, dos eventos de riscos, dos controles internos e dos planos de tratamento. O monitoramento é realizado pela Superintendência de Integridade-SUINT e pelo Comitê de Governança, Riscos e Controle - CGRC.

Os planos de tratamento (planos de ação) são objeto de constante monitoramento pela segunda linha e comitê correlato ao tema. Este monitoramento envolve o acompanhamento dos prazos das ações e controles propostos, relacionadas com os eventos de riscos.

As ações de implementação estão associadas ao evento de risco em específico que, por sua vez, está relacionado com um ou mais objetivos e metas estratégicas. Portanto, os prazos das ações e controles propostos devem estar compatíveis, de forma a convergir com o prazo para a conclusão das metas estratégicas.

O acompanhamento e verificação podem resultar na melhoraria contínua do processo, com aperfeiçoamento ou ajustes nos elementos da gestão de riscos avaliados no processo de gerenciamento de riscos.

Devido à abrangência e à complexidade do tema, o Manual e Tutorial de Gestão de Riscos da Valec serão implantados de forma gradual e continuada, com o monitoramento a partir de relatórios trimestrais.

O Manual e Tutorial de Gestão de Riscos devem ser atualizados ou ratificados em intervalos não superiores a 2 (dois) anos ou quando mudanças significativas ocorrerem, para a assegurar a sua contínua pertinência, adequação e eficácia.

## 6. Níveis da Organização

**Nível Estratégico** - Nível relacionado com as políticas públicas da empresa, objetivos estratégicos do Planejamento Estratégico Institucional e atividades fim da estatal, com maior grau de relevância e priorização pela Alta Administração, a fim de garantir a continuidade e perenização da organização.

**Nível Tático** - Nível relacionado com programas, planos, iniciativas e atividades essenciais para apoio e consecução dos objetivos estratégicos.

**Nível Operacional** - Nível relacionado com a implementação de projetos e execução dos trabalhos das unidades organizacionais.

## 7. Tipos e Categorias de riscos

Com base nas informações do Estatuto Social, do Planejamento Estratégico Institucional, do Plano de Negócios e da estrutura organizacional, foram definidas os seguintes tipos e categorias de riscos para objeto de classificação dos eventos de riscos, aplicáveis para a Valec.

### 7.1 Riscos Operacionais

Os riscos operacionais compreendem os eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Contratação e Aquisições; Execução Operacional; Infraestrutura; Pessoal; Processos; Segurança da Informação; Sistemas; e, Terceiro.

**Risco de Contratação e Aquisições -** Eventos relacionados com inconsistências, desvios ou erros nos processos de contratação de obras, prestação de serviços, bens e materiais.

**Risco de Execução Operacional -** Eventos relacionados com descumprimento ou falha na observância de norma e procedimentos definidos pela empresa, falhas na execução de atividades, tarefas, geração de dados e informações inconsistentes, pendências de caminho crítico de obras e não adoção de medidas com vista à correção dos atos administrativos falhos e incorretos.

**Risco de Infraestrutura -** Eventos relacionados com inadequação ou comprometimento da estrutura física, de logística ou tecnológica da empresa.

**Risco de Pessoal -** Eventos que podem comprometer a capacidade da força de trabalho dos setores da Valec abaixo da lotação mínima necessária para consecução das atividades. Nesta categoria também está incluso eventos relacionados a falta de capacitação e gestão por competências inadequada.

**Risco de Processos -** Eventos que podem comprometer o fluxo de atividades dos macroprocessos constantes na Cadeia de Valor do Planejamento Estratégico Institucional.

**Risco de Segurança da Informação -** Eventos relacionados com a quebra de confidencialidade, integridade, disponibilidade e autenticidade da informação.

**Risco de Sistemas -** Eventos relacionados com sistemas com programações tecnológicas que resultem em registro, processamento ou reporte de dados inválidos, incompletos ou em desacordo com as necessidades da gestão.

**Risco de Terceiro -** Eventos de riscos relacionados com serviços prestados por terceiros/fornecedores, empresas contratadas, obras ou produtos adquiridos sem os requisitos de qualidade contratados e esperados ou não entregues nas datas previstas.

### 7.2 Riscos de Imagem

**Risco de Imagem Institucional -** Eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) e da Administração Pública em relação à capacidade da entidade cumprir sua missão institucional.

### 7.3 Riscos Legais

Os riscos legais compreendem os eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da Valec. Este tipo de risco também envolve as ações que podem resultar em descumprimento de dispositivos legais ou normativos.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Conformidade Legal; Contábil; Contencioso; Legal e Regulamentar; Patrimonial; Trabalhista; Tratamento de Dados Pessoais; e, Tributário.

**Risco de Conformidade Legal -** Eventos relacionados com descumprimento de dispositivos legais e regulamentares.

**Risco Contábil -** Eventos relacionados com inobservância de normas, princípios, pronunciamentos técnicos ou melhores práticas contábeis.

**Risco de Contencioso -** Eventos decorrentes de transações contratuais malsucedidas, judicializações contra a empresa, ou de outras eventualidades legais que resultam em um passivo ou em outras perdas. Litígio judicial ou extrajudicial.

**Risco Legal e Regulamentar** - Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da entidade.

**Risco Patrimonial -** Eventos que podem comprometer a devida valorização dos ativos da companhia e benefícios futuros esperados. Nesta categoria também está incluso eventos relacionados com inconsistências ou cálculos inadequados nos respectivos laudos de avaliação.

**Risco Trabalhista -** Eventos de riscos que podem resultar na inobservância ou descumprimento de legislação e regulamentação trabalhista.

**Riscos de Tratamento de Dados Pessoais -** Eventos de riscos relacionados com a eventual exposição e tratamento indevido de dados pessoais.

**Risco Tributário -** Qualquer evento, ação ou falta de ação relacionada com estratégia fiscal, operações tributárias, emissão de relatórios contábeis de impostos ou conformidade fiscal.

### 7.4 Riscos Financeiros/Orçamentários

Os riscos financeiros/orçamentários compreendem os eventos que podem comprometer a capacidade da Valec de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Mercado e Orçamentário/Financeiro.

**Risco de Mercado -** Eventos relacionados com mudança nos preços de mercado, variação cambial, de taxas de juros e de preços ou variações no ambiente de negócios sob o ponto de vista de oferta e demanda.

**Risco Orçamentário/Financeiro -** Eventos que podem comprometer a capacidade da entidade em contar com os recursos orçamentários e financeiros para a consecução do plano de negócios, função social e atividades. Nesta categoria também se enquadram eventos que podem comprometer na execução orçamentária, como atraso nas licitações, e, eventos que podem ocasionar redução de orçamento, perda de orçamento nas janelas trimestrais, dentre outros.

### 7.5 Riscos de Governança

Os riscos de governança compreendem os eventos relacionados com a elaboração ou implementação inadequada do modelo de negócios, objetivos e metas, considerando as políticas públicas da empresa. Este tipo de risco também envolve as mudanças e questões externas que podem comprometer as atividades da empresa. Considerando a relevância do tema, este tipo de risco também compreende os riscos de integridade e riscos de pessoal com ênfase nas lideranças.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Conjuntura; Estratégia; Integridade; Liderança e Pessoas; e, Negócios.

**Risco de Conjuntura -** Eventos relacionados com mudanças nas condições políticas, culturais, sociais, econômicas, regulatórias, financeiras do Brasil ou de outros países que possam comprometer as atividades da empresa.

**Risco de Estratégia** - Eventos relacionados com a definição de estrutura, objetivos, processos, metas e iniciativas inadequadas para a consecução das políticas públicas da empresa.

**Risco de Integridade -** Eventos relacionados com desvio ético, fraude ou corrupção, assim como qualquer ato ou procedimento irregular em desacordo com os princípios da Administração Pública, boas práticas de governança, normas, regulamentos e legislação correlata.

**Risco de Liderança e Pessoas -** Eventos que podem comprometer o mecanismo de liderança no qual é composto pelo conjunto de práticas de natureza humana ou comportamental que asseguram que pessoas probas, capacitadas, competentes, responsáveis e motivadas ocupem a alta administração e as principais posições gerenciais da Valec, liderando as pessoas e as funções organizacionais para o alcance dos resultados esperados pelas partes interessadas.

**Risco de Negócios -** Eventos relacionados com modelo de negócios inadequado e divergente do ambiente interno e externo da empresa, não relação com o planejamento estratégico, definição inadequada, inexistente ou subjetiva dos programas, projetos, clientes, produtos, serviços, análise competitiva e inteligência de mercado.

## 8. Tutorial de Gestão de Riscos

No intuito de detalhar o Processo de Gestão de Riscos, bem como apresentar as figuras, quadros, tabelas e referências normativas, segue o Tutorial de Gestão de Riscos, Anexo II desta resolução.

**ANEXO II DA RESOLUÇÃO NORMATIVA VALEC Nº 12/2022/CONSAD, DE 23 DE MAIO DE 2022**

# TUTORIAL DE GESTÃO DE RISCOS DA VALEC

VALEC Engenharia, Construções e Ferrovias S.A.

MINISTÉRIO DA INFRAESTRUTURA

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

**TUTORIAL DE GESTÃO DE RISCOS**

**VALEC - ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A.**
Edifício Sede - SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5 - Asa Sul - 70.070-010 –
Brasília – DF - tel: +61 2029 6100
https://www.valec.gov.br
**Diretor-Presidente**
André Kuhn
**Superintendente de Integridade**
Nelbe Ferraz de Freitas
**Gerente de Riscos e Controles Internos**
Paulo Cézar Rabelo
**Equipe da Gerência de Riscos e Controles Internos**
Pablo Anderson Alves

**SUMÁRIO**

**LISTA DE FIGURAS**



**LISTA DE QUADROS**



**LISTA DE TABELAS**

## 1. Introdução

O Tutorial de Gestão de Riscos, apresenta os fundamentos, a estrutura e a metodologia detalhada do Processo Gestão de Riscos no âmbito da Valec Engenharia Construções e Ferrovias S.A., considerando o Estatuto Social e a Política de Gestão de Riscos, Controle e Conformidade, aprovada pelo Conselho de Administração-CONSAD, conforme Resolução Normativa Valec n° 9/2021/CONSAD-Valec.

O Manual e Tutorial de Gestão de Riscos têm como objetivo estabelecer as diretrizes a serem observadas no processo de Gestão de Riscos da Valec Engenharia Construções e Ferrovias S.A., com vistas à definição de estratégias, ao alcance de objetivos e na tomada de decisões fundamentadas, tendo como pressupostos:

I. Apoiar a governança da Valec;
II. Aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas;
III. Aprimorar os controles internos;
IV. Resguardar a Administração da Valec e os demais gestores quanto à tomada de decisão e à prestação de contas;
V. Explicitar o apetite de risco da Valec;
VI. Manter a estrutura apropriada de governança de risco;
VII. Estabelecer critérios e parâmetros para identificação, avaliação, monitoramento e controle dos riscos relevantes da empresa;
VIII. Disseminar a cultura de Gestão de Riscos, especificando o perfil de risco adotado, introduzindo uma linguagem comum para o assunto "riscos" em todos os níveis da organização;
IX. Garantir que os processos e procedimentos relacionados a Gestão de Riscos da Valec atendam aos requerimentos regulatórios vigentes, bem como às melhores práticas nacionais e internacionais; e
X. Integrar as informações relacionadas a riscos e controles de gestão ao processo de Planejamento Estratégico da Valec, para a consecução dos objetivos institucionais.

A Gestão de Riscos Corporativos tem como principal objetivo o cumprimento dos objetivos e metas constantes no Planejamento Estratégico Institucional. Dessa forma, a gestão de riscos e o planejamento estratégico são realizadas de forma integrada, com a apresentação trimestral dos resultados à Diretoria Executiva-DIREX, para posterior análise e deliberação do Conselho de Administração-CONSAD.

Este tutorial foi elaborado em consonância com a regulamentação correlata. No que tange a regulamentação no âmbito do Poder Executivo Federal, destacam-se a Instrução Normativa MP/CGU n° 1/2016 e o Decreto n° 8945, de 27 de dezembro de 2016. A Instrução Normativa MP/CGU n° 1/2016, foi elaborada de forma a orientar os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança. O Decreto n° 8945/1016, especificamente na Seção II, está relacionado com as regras de estrutura e práticas de gestão de riscos a serem adotadas pelas empresas estatais.

Conforme inciso II, art. 18 da Lei 13303, de 30 de junho de 2016, compete ao Conselho de Administração implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a empresa pública, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os riscos relacionados à ocorrência de fraude e corrupção.

Portanto, deve ser estruturado pela diretoria o sistema de gestão de riscos corporativos adequados à empresa, assim como a verificação da eficácia dessa gestão de riscos na respectiva área de atuação e comunicação trimestral ao Conselho de Administração. Além disso, os sistemas de controles internos devem estar adequados para monitorar e mitigar os riscos e proteger os ativos da empresa, garantindo a precisão e qualidade das informações prestadas pela gestão.

A gestão de riscos corporativos e controles internos compõem alguns dos critérios que são considerados na avaliação anual dos membros da Diretoria Executiva pelo Conselho de Administração.

Destaca-se que a importância do processo de gerenciamento de risco é em função da necessidade de assegurar melhores resultados para a gestão e governança, com os riscos mitigados e controles implantados, bem como transparência aos processos, para que os empreendimentos e serviços sejam concluídos e a Valec cumpra a sua função social que justificou a autorização da sua respectiva criação.

## 2. Princípios

A Gestão de Riscos da Valec, tendo como referências as melhores práticas internacionais de gestão de riscos, focando a criação e proteção de valor para a empresa, observará princípios, que servem de orientação para que a gestão de riscos seja eficiente e eficaz. A Gestão de Riscos eficaz requer (precisa ser/ter) os seguintes elementos:

I. Integrada. A gestão de riscos é parte integrante de todas as atividades organizacionais;
II. Estruturada e abrangente. Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis;
III. Personalizada. A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos;
IV. Inclusiva. O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada;
V. Dinâmica. Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna;
VI. Melhor informação disponível. As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes;
VII. Fatores humanos e culturais. O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio; e
VIII. Melhoria contínua. A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

As diretrizes e princípios estabelecidos no Manual de Gestão de Riscos se aplicam aos órgãos sociais e estatutários; aos colaboradores e aos prestadores de serviços diretos e indiretos naquilo que couber.

## 3. Conceitos

**Apetite a risco -** Grau de exposição (nível de risco) que uma organização está disposta a aceitar na busca dos seus objetivos.

**Causas -** Elementos, situações ou condições que têm o potencial de dar origem aos eventos de riscos.

**Consequência -** Resultado e impacto no cumprimento dos objetivos da organização no caso de materialização do risco.

**Controles internos -** Conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de empregados, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:

a - Execução ordenada, ética, econômica, eficiente e eficaz das operações;

b - Cumprimento das obrigações de *accountability*;

c - Cumprimento das leis e regulamentos aplicáveis; e

d - Salvaguarda dos recursos para evitar perdas, mau uso e danos.

O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.

**Evento -** Um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.

**Gerenciamento de riscos -** Processo com estrutura orientada com vistas à identificação, análise, avaliação e tratamento dos eventos de riscos, de forma a fornecer razoável certeza quanto ao alcance dos objetivos da organização.

**Grau de exposição (nível de risco) -** Valor numérico obtido a partir multiplicação entre a pontuação atribuída à probabilidade e a pontuação atribuída ao impacto, de acordo com as escalas de probabilidade e impacto da empresa.

**Incerteza -** Incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

**Matriz de riscos** - Matriz gráfica composta pelo conjunto de combinações de probabilidade e impacto, de forma a apresentar o grau de criticidade dos eventos de riscos com base no grau de exposição (nível de risco).

**Mensuração de risco -** Significa estimar a importância de um evento de risco, bem como a probabilidade e o impacto de sua ocorrência.

**Modelo das três linhas -** Modelo que apresenta a estrutura da gestão de riscos e controles internos de uma organização, no intuito de definir os papéis e responsabilidades dos diversos setores, considerando os órgãos de governança, a gestão e a auditoria interna.

**Risco -** Possibilidade de ocorrência de um evento que venha a ter resultado e impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e probabilidade.

**Risco inerente -** Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

**Risco residual -** Risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento dos riscos.

**Tolerância a risco (limite de exposição) -** Grau de exposição (nível de risco) acima do qual o evento de risco passa a ser objeto de priorização no processo de gestão de riscos, em função de estar além do apetite a riscos da organização.

## 4. Estrutura da Gestão de Riscos e Controles Internos

De acordo com o Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020) e, Instrução Normativa Conjunta CGU/MP (Controladoria-Geral da União e Ministério do Planejamento, Orçamento e Gestão) n° 01, de 10 de maio de 2016, a estrutura de gestão de riscos e controles internos em uma organização é formada por três linhas.

Esta estrutura tem como objetivo principal o gerenciamento eficaz de riscos e controles internos de forma a assegurar que a organização atinja os seus objetivos. Antes de apresentar o Modelo das Linhas é essencial compreender cada uma das responsabilidades de cada linha e as áreas da Valec que compõe cada linha.

### 4.1 Responsabilidades

#### 4.1.1 Primeira Linha

Conforme Política de Gestão de Riscos, Controle e Conformidade, a primeira linha é composta pelas unidades organizacionais responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio da Valec. São as unidades organizacionais que executam as ações referentes a implementação da gestão de riscos e respectivos controles.

Considerando o Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020) e, Instrução Normativa Conjunta CGU/MP (Controladoria-Geral da União e Ministério do Planejamento, Orçamento e Gestão) n° 01, de 10 de maio de 2016, são papéis da primeira linha:

I. Identificar, analisar, avaliar e gerir os eventos de riscos, de forma a atingir os objetivos organizacionais;
II. Elaborar os planos de tratamento, bem como implementar e manter mecanismos de controles internos;
III. Implementar as ações efetivas para aprimorar os controles e solucionar inconsistências ou erros eventualmente identificados;
IV. Assegurar que os procedimentos efetivos de implementação de controles internos integrem as suas práticas de gerenciamento de riscos; e
V. Comunicar à segunda linha (Superintendência de Integridade-SUINT) as situações relevantes ou críticas do processo de gerenciamento de riscos, assim como os novos eventos de riscos, eventos de riscos com aumento do grau de exposição, iminência ou materialização do risco e situações com necessidades imediatas de implementação de controles.

#### 4.1.2 Segunda Linha

Composta pela Superintendência de Integridade-SUINT, unidade organizacional de gestão de riscos vinculada à Presidência. Conforme Estatuto Social e Regimento Interno, são as atribuições:

I. Prestar apoio e suporte metodológico para a gestão de riscos e controles internos nas unidades organizacionais;
II. Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a empresa;

III. Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;
IV. Coordenar a comunicação de informações relativas as boas práticas de gestão de riscos e controles internos;
V. Gerenciar e monitorar o sistema de controles internos que tem por objetivo salvaguardar os ativos, verificar a exatidão e fidelidade dos dados contábeis, desenvolver a eficiência nas operações e estimular o seguimento das políticas institucionais;
VI. Propor revisão e alteração da Política de Gestão de Riscos e de Controles Internos;
VII. Gerenciar a elaboração e aplicação da metodologia e dos procedimentos para a gestão de riscos e controles internos, monitorando a sua eficiência e eficácia; e
VIII. Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria Estatutário.

Trimestralmente, a SUINT elabora o relatório acerca da gestão de riscos e controles internos, para envio à Diretoria Executiva, para posterior análise e deliberação do Conselho de Administração.

#### 4.1.3 Terceira Linha

Composta pela Auditoria Interna. As atribuições da Auditoria Interna constam no Regimento Interno da Auditoria Interna, Resolução Valec n° 7/2020/CONSAD-Valec. São as atribuições:

I. Fornecer asseguração aos órgãos de governança e de gestão de que os processos de gestão de riscos operam de maneira eficaz e os maiores riscos do negócio são gerenciados adequadamente em todos os níveis da organização; e
II. Apoiar a estruturação e o funcionamento da primeira e da segunda linhas de defesa da gestão, por meio da prestação de serviços de avaliação ou de consultoria.

### 4.2 Modelo das Três Linhas

O Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020) apresenta a estrutura no intuito de definir os papéis e responsabilidades dos diversos setores da organização. O Instituto de Auditores Internos representado no Brasil pelo IIA Brasil, é referência internacional para as empresas e organizações.

Este modelo é de extrema relevância, pois apresenta como as três linhas estão dispostas no contexto de toda a organização, considerando os órgãos de governança, a gestão e a auditoria interna. Depreende-se que o modelo foi atualizado em 2020, com o título *Modelo das Três Linhas do The IIA*, conforme segue na Figura 1.

**FIGURA 1 - O MODELO DAS TRÊS LINHAS DO INSTITUTO DE AUDITORES INTERNOS**


Fonte: Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020)

A Figura 1 apresenta o reporte da primeira e segunda linha, como unidades de gestão, aos Órgãos de Governança, neste caso ao Conselho de Administração-CONSAD, assessorado pelo Comitê de Auditoria-COAUD.

Os prestadores externos, é a auditoria externa, no qual realiza uma avaliação acerca do cumprimento da legislação e regulação.

Neste tutorial é também relevante citar os Princípios 3 e 4 do Modelo do *IIA*, pois apresentam de forma resumida os papéis e responsabilidades da primeira, segunda e terceira linhas.

- *Princípio 3: Gestão e os papéis da primeira e segunda linhas*

  *"A responsabilidade da gestão de atingir os objetivos organizacionais compreende os papéis da primeira e segunda linhas. Os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio. Os papéis de segunda linha fornecem assistência no gerenciamento de riscos."*

- *Princípio 4: Papéis da Terceira Linha*

  *"A auditoria interna presta avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Isso é feito através da aplicação competente de processos sistemáticos e disciplinados, expertise e conhecimentos. Ela 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."*

Com destaque ao *Princípio 3: Gestão e os papéis da primeira e segunda linhas* o modelo relata que a responsabilidade de atingir os objetivos organizacionais é da primeira linha e, também, da segunda linha. Outro ponto importante reforçado no modelo, é que a avaliação e assessoria da Auditoria Interna são independentes da gestão.

A título de informação, a Instrução Normativa CGU/MP nº 01/2016, também apresenta disposições relevantes acerca das três linhas, no *Capítulo II - Dos Controles Internos da Gestão*, em suma:

- Primeiro Linha (art. 3° da Instrução Normativa CGU/MP nº 01/2016)

  *"Art. 3° Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público. Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos. Esses controles são operados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo federal. A definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos das organizações públicas. Assim, tendo em vista os objetivos estabelecidos pelos órgãos e entidades da administração pública, e os riscos decorrentes de eventos internos ou externos que possam obstaculizar o alcance desses objetivos, devem ser posicionados os controles internos mais adequados para mitigar a probabilidade de ocorrência dos riscos, ou o seu impacto sobre os objetivos organizacionais."*

- Segunda Linha (art. 6° da Instrução Normativa CGU/MP nº 01/2016)

  *"Art. 6° Além dos controles internos da gestão, os órgãos e entidades do Poder Executivo federal podem estabelecer instâncias de segunda linha (ou camada) de defesa, para supervisão e monitoramento desses controles internos. Assim, comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance, por exemplo, podem se constituir em instâncias de supervisão de controles internos."*

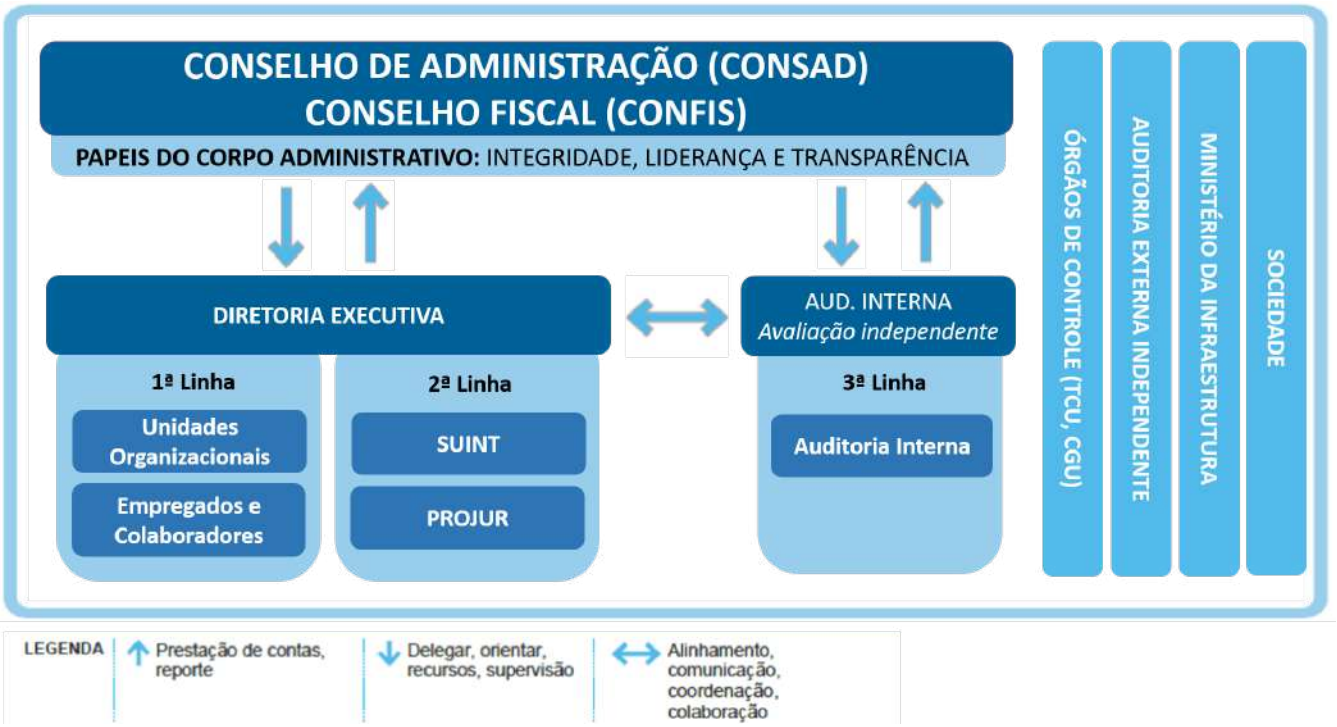
- Terceira Linha (inciso III, art. 2° da Instrução Normativa CGU/MP nº 01/2016)

  *III - auditoria interna: atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhoraras operações de uma organização. Ela auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança. As auditorias internas no âmbito da Administração Públicas e constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos). Compete às auditorias internas oferecer avaliações e assessoramento às organizações públicas, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes e eficazes mitiguem os principais riscos de que os órgãos e entidades não alcancem seus objetivos;*

Portanto, verifica-se que as responsabilidades das três linhas constantes no manual e tutorial estão convergentes aos princípios do Modelo das Três Linhas do Instituto de Auditores Internos e às disposições constantes na Instrução Normativa Conjunta CGU/MP nº 01/2016.

De forma adaptada à estrutura da Valec, apenas a título instrutivo, apresentamos na Figura 2 os setores da empresa que compõem as 1°, 2° e 3° linhas.

**FIGURA 2 - O MODELO DAS TRÊS LINHAS - SETORES DA VALEC (ADAPTADO)**



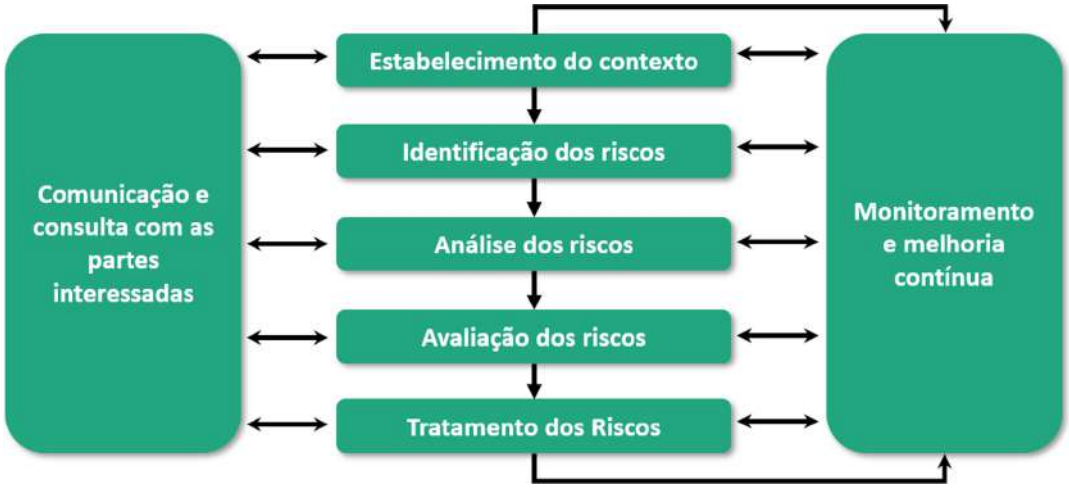

Fonte: Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020)

## 5. Processo de Gestão de Riscos

O processo de gestão de riscos na Valec, com base na ABNT NBR ISO 31000:2018, compreende as seguintes etapas:

I - estabelecimento do contexto;
II - identificação dos riscos;
III - análise dos riscos;
IV - avaliação dos riscos;
V - tratamento dos riscos;
VI - comunicação e consulta; e
VII - monitoramento e melhoria contínua.

**FIGURA 3 - ETAPAS DO PROCESSO DE GESTÃO DE RISCOS**




Fonte: Manual de Gestão de Riscos do TCU (TCU, 2020, adaptado da ISO 31000:2018)

Este tutorial tem como objetivo detalhar as etapas do processo de gestão de riscos, com os quadros, figuras e tabelas, e relacionar a utilização de diversos normativos de órgãos da Administração Pública consolidados sobre o tema.

Em específico para a elaboração dos quadros do tutorial, de forma a ter uniformidade nos valores, foram utilizados os parâmetros do Referencial Básico de Gestão de Riscos do Tribunal de Contas da União-TCU, 2018.

Para fins instrutivos e de forma resumida, o Referencial básico de Gestão de Riscos do TCU (2018), apresenta um roteiro básico para a gestão de riscos de uma organização, com 11 questões:

1. Que empreendimento você deseja proteger ou ver bem-sucedido? Pode ser um projeto, um processo, uma organização, uma política.
2. Quais são os objetivos desse empreendimento?
3. Que fatores (fraquezas, ameaças, erros, falhas) podem afetar o alcance desses objetivos?
4. Que riscos podem se originar da ocorrência desses fatores?
5. Qual seria a probabilidade e o impacto da ocorrência de cada um desses eventos de riscos se nada tivesse sido feito para mitigá-los até o momento? Calcule o risco inerente (probabilidade inicial × impacto inicial).
6. Qual é o seu apetite e a sua tolerância a risco? Qual nível de riscos você considera aceitável?
7. Quais medidas mitigadoras já foram adotadas e que controles internos já estão implantados? Qual a eficácia dessas medidas e controles? Algum deles pode ser eliminado?
8. Que outras medidas mitigadoras e controles internos podem ser adotados para adequar o nível de risco ao apetite e à tolerância a risco?
9. Qual é a probabilidade e o impacto esperado da ocorrência desses riscos após a avaliação de eficácia e adequação das medidas mitigadoras e controles internos? Calcule o risco residual (risco inerente × risco de controle);
10. Com que frequência esses riscos devem ser monitorados?
11. Quais são os responsáveis por monitorar os riscos? Quem deve ser comunicado acerca desses? Com que frequência isso deve ser feito e por quais mecanismos?

A seguir apresentamos de forma detalhada cada uma das etapas do processo de gestão de riscos, de forma a instruir e auxiliar as unidades organizacionais da Valec no gerenciamento dos riscos corporativos.

## 5.1 Estabelecimento do Contexto

Esta etapa consiste em compreender o ambiente externo e interno no qual o objeto da gestão de riscos se encontra inserido e identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

Esta etapa é conduzida pela SUINT e é realizada a partir de oficinas de instrução com as diretorias.

O objetivo desta etapa é definir: quais são os objetos de gestão da riscos mais importantes na Valec; quais são os objetivos, metas e iniciativas relacionadas com esses objetos de gestão de riscos; quais são os fatores externos e internos que podem afetar no alcance desses objetivos e resultados; e, quais são os processos de trabalho relevantes para alcance desses objetivos e resultados.

O estabelecimento do contexto para o processo de gestão de riscos deve ser realizado com base no Planejamento Estratégico Institucional e no Plano de Negócios.

O Planejamento Estratégico Institucional-PEI apresenta os objetivos e resultados esperados da empresa nos próximos anos. Além disso, conforme Resolução Valec nº 6/2021/CONSAD-Valec, a Matriz SWOT (forças, fraquezas, oportunidades, ameaças), um essencial mecanismo para estabelecimento do contexto, também compõe o PEI.

Segue a Figura 4 atinente ao Mapa Estratégico, com os objetivos estratégicos do Planejamento Estratégico Institucional 2020-2024.

**FIGURA 4 - MAPA ESTRATÉGICO DA VALEC 2020-2024**


O Plano de Negócios elaborado anualmente também é uma relevante peça para instrução na etapa de estabelecimento do contexto, pois apresenta o Modelo de Negócios da empresa. No Modelo de Negócios, são apresentadas as informações relacionadas com a análise competitiva de mercado, clientes, produtos e serviços, fornecedores e parcerias e imagem corporativa.

Portanto, o estabelecimento do contexto deve considerar os seguintes elementos:

- políticas públicas e legislação correlacionada;
- ambiente externo (cenário político, institucional, social, financeiro, legal, tecnológico, econômico etc.)
- ambiente interno (sistemas, estrutura organizacional, recursos e partes interessadas)
- modelo de negócios;
- os objetivos e resultados esperados constantes no planejamento estratégico;
- principais objetos (empreendimentos, programas, negócios) do planejamento estratégico;
- processos de trabalhos; e
- pessoas envolvidas nesses processos e especialistas nas áreas.

## 5.2 Identificação dos riscos

A partir da instrução do processo, realizada com base nos elementos da etapa de estabelecimento do contexto, esta etapa consiste na identificação dos eventos de riscos que podem impedir, prejudicar ou atrasar o alcance dos principais objetivos organizacionais.

Esta etapa é conduzida pela SUINT e é realizada a partir de oficinas de instrução com as diretorias, superintendências e gerências. No nível estratégico, as oficinas de instrução para identificação dos eventos de riscos são realizadas com as diretorias. No nível tático e operacional, as oficinas de instrução para identificação dos eventos de riscos são realizadas com as superintendências e gerências e, posteriormente aprovadas pela diretoria.

Nesta etapa, também devem ser relacionadas as informações referentes ao evento de riscos. Portanto, deve ser realizado o preenchimento da Tabela 1, de forma a correlacionar os objetos da gestão de riscos (empreendimentos, programas, negócios) aos objetivos, metas e iniciativas previstas no PEI.

Nesta etapa também devem ser relacionadas as seguintes informações referentes aos eventos de riscos: objeto relacionado (empreendimentos, programas, negócios, dentre outros); objetivos, metas e iniciativas; causas e consequências; e, nível da organização no qual o evento de risco abrange (estratégico, tático ou operacional), tipo e categoria.

Portanto, as informações que devem ser correlacionadas conforme Tabela 1 são:

- evento de risco;
- objeto relacionado (empreendimentos, programas, negócios, dentre outros);
- objetivos, metas e iniciativas;
- causas e consequências; e
- nível da organização, tipo e categoria.

**TABELA 1 - Identificação dos riscos**

| Evento de Risco | Objeto | Causa(s) | Consequência(s) | Objetivo(s) | Meta(s) | Iniciativa(s) | Nível | Tipo | Categoria |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Nos itens 5.2.1 e 5.2.2, seguem a descrição dos níveis da organização, tipos e categorias de riscos e, no item 5.2.3, os conceitos detalhados sobre causa e consequência de forma a auxiliar os gestores no preenchimento da tabela.

Cabe destacar que o preenchimento das tabelas deste tutorial deve ser realizado com o apoio metodológico da segunda linha.

### 5.2.1 Níveis da Organização

A Valec se encaixa no modelo de uma organização no qual o arranjo hierárquico para as decisões pode ser dividido em três camadas: nível operacional, nível tático e nível estratégico.

A Figura 5, relacionada no Livro Laranja: Gestão de Riscos - Princípios e Conceitos (*Orange Book: Management of risk - Principles and Concepts,* 2004) do Reino Unido, apresenta uma ilustração esquemática da hierarquia de riscos em uma organização.

De acordo com o Livro Laranja, a gestão de riscos a nível estratégico, tático e operacional deve ser integrada para que os níveis se apoiem mutualmente. Conforme Figura 5, quanto maior o nível da organização, maior o nível de incerteza.

**FIGURA 5 - HIERARQUIA DO RISCO - HIERARCHY OF RISK**


Fonte: Traduzido do Livro Laranja: Gestão de Riscos - Princípios e Conceitos (*Orange Book: Management of risk - Principles and Concepts,* 2004)

A gestão de riscos é liderada no topo com base em decisões estratégicas que determinam a direção e sustentabilidade da organização. No nível tático, as decisões tomadas envolvem a escolha de métodos ou mecanismos alternativos que podem ser usados para alcançar as decisões estratégicas. Por fim, no nível operacional, com menor grau de incerteza, considerando que as diretrizes já foram estabelecidas pelos níveis

superiores, as decisões de implementação são bastantes operacionais (relativo a procedimentos rotineiros executados). Com base no Livro Laranja apresentamos as definições abaixo.

**Nível Estratégico** - Nível relacionado com as políticas públicas da empresa, objetivos estratégicos do Planejamento Estratégico Institucional e atividades fim da estatal, com maior grau de relevância e priorização pela Alta Administração, a fim de garantir a continuidade e perenização da organização.

**Nível Tático** - Nível relacionado com programas, planos, iniciativas e atividades essenciais para apoio e consecução dos objetivos estratégicos.

**Nível Operacional** - Nível relacionado com a implementação de projetos e execução dos trabalhos das unidades organizacionais.

#### 5.2.2 Tipos e Categorias de riscos

Com base nas informações do Estatuto Social, do Planejamento Estratégico Institucional, do Plano de Negócios e da estrutura organizacional, foram definidas os seguintes tipos e categorias de riscos para objeto de classificação dos eventos de riscos, aplicáveis para a Valec.

### a) Riscos Operacionais

Os riscos operacionais compreendem os eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Contratação e Aquisições; Execução Operacional; Infraestrutura; Pessoal; Processos; Segurança da Informação; Sistemas; e, Terceiro.

**Risco de Contratação e Aquisições -** Eventos relacionados com inconsistências, desvios ou erros nos processos de contratação de obras, prestação de serviços, bens e materiais.

**Risco de Execução Operacional -** Eventos relacionados com descumprimento ou falha na observância de norma e procedimentos definidos pela empresa, falhas na execução de atividades, tarefas, geração de dados e informações inconsistentes, pendências de caminho crítico de obras e não adoção de medidas com vista à correção dos atos administrativos falhos e incorretos.

**Risco de Infraestrutura -** Eventos relacionados com inadequação ou comprometimento da estrutura física, de logística ou tecnológica da empresa.

**Risco de Pessoal -** Eventos que podem comprometer a capacidade da força de trabalho dos setores da Valec abaixo da lotação mínima necessária para consecução das atividades. Nesta categoria também está incluso eventos relacionados a falta de capacitação e gestão por competências inadequada.

**Risco de Processos -** Eventos que podem comprometer o fluxo de atividades dos macroprocessos constantes na Cadeia de Valor do Planejamento Estratégico Institucional.

**Risco de Segurança da Informação -** Eventos relacionados com a quebra de confidencialidade, integridade, disponibilidade e autenticidade da informação.

**Risco de Sistemas -** Eventos relacionados com sistemas com programações tecnológicas que resultem em registro, processamento ou reporte de dados inválidos, incompletos ou em desacordo com as necessidades da gestão.

**Risco de Terceiro -** Eventos de riscos relacionados com serviços prestados por terceiros/fornecedores, empresas contratadas, obras ou produtos adquiridos sem os requisitos de qualidade contratados e esperados ou não entregues nas datas previstas.

### b) Riscos de Imagem

**Risco de Imagem Institucional -** Eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) e da Administração Pública em relação à capacidade da entidade cumprir sua missão institucional.

### c) Riscos Legais

Os riscos legais compreendem os eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da Valec. Este tipo de risco também envolve as ações que podem resultar em descumprimento de dispositivos legais ou normativos.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Conformidade Legal; Contábil; Contencioso; Legal e Regulamentar; Patrimonial; Trabalhista; Tratamento de Dados Pessoais; e, Tributário.

**Risco de Conformidade Legal -** Eventos relacionados com descumprimento de dispositivos legais e regulamentares.

**Risco Contábil -** Eventos relacionados com inobservância de normas, princípios, pronunciamentos técnicos ou melhores práticas contábeis.

**Risco de Contencioso -** Eventos decorrentes de transações contratuais malsucedidas, judicializações contra a empresa, ou de outras eventualidades legais que resultam em um passivo ou em outras perdas. Litígio judicial ou extrajudicial.

**Risco Legal e Regulamentar** - Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da entidade.

**Risco Patrimonial -** Eventos que podem comprometer a devida valorização dos ativos da companhia e benefícios futuros esperados. Nesta categoria também está incluso eventos relacionados com inconsistências ou cálculos inadequados nos respectivos laudos de avaliação.

**Risco Trabalhista -** Eventos de riscos que podem resultar na inobservância ou descumprimento de legislação e regulamentação trabalhista.

**Riscos de Tratamento de Dados Pessoais -** Eventos de riscos relacionados com a eventual exposição e tratamento indevido de dados pessoais.

**Risco Tributário -** Qualquer evento, ação ou falta de ação relacionada com estratégia fiscal, operações tributárias, emissão de relatórios contábeis de impostos ou conformidade fiscal.

### d) Riscos financeiros/orçamentários

Os riscos financeiros/orçamentários compreendem os eventos que podem comprometer a capacidade da Valec de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Mercado e Orçamentário/Financeiro.

**Risco de Mercado -** Eventos relacionados com mudança nos preços de mercado, variação cambial, de taxas de juros e de preços ou variações no ambiente de negócios sob o ponto de vista de oferta e demanda.

**Risco Orçamentário/Financeiro -** Eventos que podem comprometer a capacidade da entidade em contar com os recursos orçamentários e financeiros para a consecução do plano de negócios, função social e atividades. Nesta categoria também se enquadram eventos que podem comprometer na execução orçamentária, como atraso nas licitações, e, eventos que podem ocasionar redução de orçamento, perda de orçamento nas janelas trimestrais, dentre outros.

### e) Riscos de Governança

Os riscos de governança compreendem os eventos relacionados com a elaboração ou implementação inadequada do modelo de negócios, objetivos e metas, considerando as políticas públicas da empresa. Este tipo de risco também envolve as mudanças e questões externas que podem comprometer as atividades da empresa. Considerando a relevância do tema, este tipo de risco também compreende os riscos de integridade.

Neste tipo de risco estão enquadradas as seguintes categorias de riscos: Conjuntura; Estratégia; Integridade; Liderança e Pessoas; e, Negócios.

**Risco de Conjuntura -** Eventos relacionados com mudanças nas condições políticas, culturais, sociais, econômicas, regulatórias, financeiras do Brasil ou de outros países que possam comprometer as atividades da empresa.

**Risco de Estratégia** - Eventos relacionados com a definição de estrutura, objetivos, processos, metas e iniciativas inadequadas para a consecução das políticas públicas da empresa.

**Risco de Integridade -** Eventos relacionados com desvio ético, fraude ou corrupção, assim como qualquer ato ou procedimento irregular em desacordo com os princípios da Administração Pública, boas práticas de governança, normas, regulamentos e legislação correlata.

**Risco de Liderança e Pessoas -** Eventos que podem comprometer o mecanismo de liderança no qual é composto pelo conjunto de práticas de natureza humana ou comportamental que asseguram que pessoas probas, capacitadas, competentes, responsáveis e motivadas ocupem a alta

administração e as principais posições gerenciais da Valec, liderando as pessoas e as funções organizacionais para o alcance dos resultados esperados pelas partes interessadas.

**Risco de Negócios -** Eventos relacionados com modelo de negócios inadequado e divergente do ambiente interno e externo da empresa, não relação com o planejamento estratégico, definição inadequada, inexistente ou subjetiva dos programas, projetos, clientes, produtos, serviços, análise competitiva e inteligência de mercado.

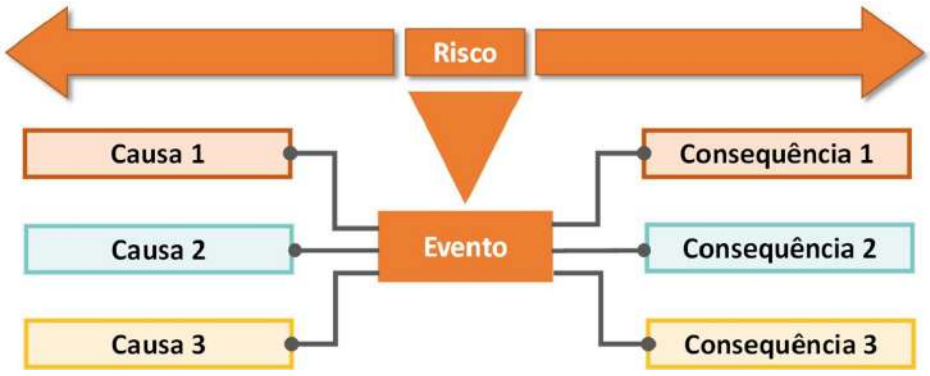
**QUADRO 1 - TIPOS E CATEGORIAS DE RISCOS**

| Tipos de Riscos | Categorias de Riscos |
|---|---|
| Riscos Operacionais | Risco de Contratação e Aquisições |
| | Risco de Execução Operacional |
| | Risco de Infraestrutura |
| | Risco de Pessoal |
| | Risco de Processos |
| | Risco de Segurança da Informação |
| | Risco de Sistemas |
| | Risco de Terceiro |
| Riscos de Imagem | Risco de Imagem Institucional |
| Riscos Legais | Risco de Conformidade Legal |
| | Risco Contábil |
| | Risco de Contencioso |
| | Risco Legal e Regulamentar |
| | Risco Patrimonial |
| | Risco Trabalhista |
| | Riscos de Tratamento de Dados Pessoais |
| | Risco Tributário |
| Riscos Financeiros/Orçamentários | Risco de Mercado |
| | Risco Orçamentário/Financeiro |
| Riscos de Governança | Risco de Conjuntura |
| | Risco de Estratégia |
| | Risco de Integridade |
| | Risco de Liderança e Pessoas |
| | Risco de Negócios |

### 5.2.3 Causa e consequência

Para a verificação da causa e consequência associadas aos eventos de riscos, segue a Figura 6, constante do Livro Laranja: Gestão de Riscos - Princípios e Conceitos (*Orange Book: Management of risk - Principles and Concepts,* 2020) do Reino Unido.

**FIGURA 6 - DETALHAMENTO ESQUEMÁTICO DA IDENTIFICAÇÃO DOS RISCOS**




Fonte: Livro Laranja: Gestão de Riscos - Princípios e Conceitos (*Orange Book: Management of risk - Principles and Concepts,* 2020)

Em que:

- **Causa** é um elemento que isolado ou combinado tem o potencial de dar origem ao evento de risco. No âmbito interno da organização, os elementos da causa assumem as formas de fragilidades e vulnerabilidades que tornam a organização suscetível a ocorrências e incidentes que materializam o risco. No âmbito externo, o ambiente no qual a organização explora seu modelo de negócios, os elementos da causa estão mais associados às oscilações, reviravoltas, instabilidade econômica ou política, ou seja, eventos adversos de grande repercussão capazes de desencadear riscos que podem comprometer o alcance dos objetivos da organização. As causas antecedem os eventos de riscos.

- **Consequência** constitui o resultado e impacto no cumprimento dos objetivos da organização em função da materialização do risco. Podem ser certas ou incertas, diretas ou indiretas, positivas ou negativas, ser expressas qualitativa ou quantitativamente e podem exibir efeitos cumulativos em cadeia. As consequências sucedem a materialização do risco.

## 5.3 Análise dos Riscos

Após as etapas de estabelecimento do contexto e identificação de riscos, devem ser realizadas as oficinas para as etapas de análise, avaliação e tratamento dos riscos. Estas oficinas são conduzidas pela SUINT e realizadas com as diretorias, superintendências e gerências, de acordo com o nível da organização que o risco abrange. No nível estratégico, as oficinas são realizadas com as diretorias. No nível tático e operacional as oficinas são realizadas com as superintendências e gerências e, posteriormente aprovadas pela diretoria.

Esta etapa compreende o cálculo do grau de exposição da empresa ao evento de risco identificado. O grau de exposição é calculado a partir de critérios de probabilidade e impacto. Destarte, para cada evento de risco são atribuídos valores a partir de uma escala de probabilidade e de impacto.

A multiplicação entre os valores atribuídos para probabilidade e impacto define o grau de exposição ao evento de risco, nesta etapa definido como risco inerente, pois não são considerados neste cálculo quaisquer controles que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Os Quadros 2 e 3 apresentam os valores associados à escala de probabilidade e impacto. Estes valores são definidos de acordo com as informações associadas ao evento de risco.

Portanto, apresentamos abaixo a fórmula para o cálculo do grau de exposição (nível de risco inerente) ao evento de risco:

**NRI = P x I**

*em que:*

- **NRI** = nível de risco inerente (grau de exposição)
- **P** = probabilidade do risco
- **I** = impacto do risco

Uma vez analisado na superintendência ou gerência e aprovado pela respectiva diretoria, o grau de exposição somente pode ser alterado com a apresentação das razões de justificativas. As razões de justificativas devem ser apresentadas à SUINT/PRESI.

**QUADRO 2 - GESTÃO DE RISCOS - ESCALA DE PROBABILIDADE**

| PROBABILIDADE | DESCRIÇÃO DA PROBABILIDADE, DECONSIDERNADO OS CONTROLES | PESO |
|---|---|---|
| **Muito baixa** | **Improvável**. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade. | **1** |
| **Baixa** | **Rara**. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. | **2** |
| **Média** | **Possível**. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. | **5** |
| **Alta** | **Provável**. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. | **8** |
| **Muito alta** | **Praticamente certa**. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade. | **10** |

Fonte: Referencial básico de gestão de riscos (TCU, 2018)

**QUADRO 3 - GESTÃO DE RISCOS - ESCALA DE IMPACTO**

| IMPACTO | DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA | PESO |
|---|---|---|
| **Muito baixo** | **Mínimo** impacto nos objetivos (estratégicos, operacionais, de informação/ comunicação/divulgação ou de conformidade). | **1** |
| **Baixo** | **Pequeno** impacto nos objetivos (idem). | **2** |
| **Médio** | **Moderado** impacto nos objetivos (idem), porém recuperável. | **5** |
| **Alto** | **Significativo** impacto nos objetivos (idem), de difícil reversão. | **8** |
| **Muito alto** | **Catastrófico** impacto nos objetivos (idem), de forma irreversível. | **10** |

Fonte: Referencial básico de gestão de riscos (TCU, 2018)

## 5.4 Avaliação dos riscos

Na etapa de avaliação é verificado se o grau de exposição ao evento de risco está ou não, além do apetite a riscos definido pelo Conselho de Administração-CONSAD. Compete ao Conselho de Administração definir o apetite a riscos da empresa.

Com base na matriz de riscos, a partir do grau de exposição, o evento de risco pode ser classificado de acordo com quatro graus de criticidade: baixo, médio, alto ou extremo.

A Matriz de Riscos é a matriz gráfica composta pelo conjunto de combinações de probabilidade e impacto, de forma a apresentar a criticidade dos eventos de riscos com base no grau de exposição (nível de risco). Com vistas a facilitar visualização da exposição da empresa aos eventos de riscos, a Matriz de Risco deve ser apresentada conforme Figura 7.

**FIGURA 7 - MATRIZ DE RISCOS**

| IMPACTO | | | | | | |
|---|---|---|---|---|---|---|
| | Catastrófico 10 | 10 RM | 20 RM | 50 RA | 80 RE | 100 RE |
| | Significativo 8 | 8 RB | 16 RM | 40 RA | 64 RA | 80 RE |
| | Moderado 5 | 5 RB | 10 RM | 25 RM | 40 RA | 50 RA |
| | Pequeno 2 | 2 RB | 4 RB | 10 RM | 16 RM | 20 RM |
| | Mínimo 1 | 1 RB | 2 RB | 5 RB | 8 RB | 10 RM |
| | | Muito Baixa 1 | Baixa 2 | Média 5 | Alta 8 | Muito Alta 10 |
| | | PROBABILIDADE | | | | |

Fonte: Referencial básico de gestão de riscos (TCU, 2018)

***Matriz de Riscos - Limite de exposição aos eventos de riscos***

*Área vermelha e área laranja - acima da faixa de delimitação (limite de exposição) da Matriz de Riscos, além do apetite a riscos;*

*Área amarela - abaixo da faixa de delimitação (limite de exposição) da Matriz de Riscos, com necessidade de monitoramento;*

*Área verde - eventos de riscos que podem ser aceitos.*

Para a avaliação do evento de risco é utilizado o Quadro 4, no qual apresenta os intervalos de valores associados ao grau de exposição, correlacionados com o grau de criticidade.

**QUADRO 4 - ESCALA DE AVALIAÇÃO DOS EVENTOS DE RISCOS**

| **RB** (Risco Baixo) | **RM** (Risco Médio) | **RA** (Risco Alto) | **RE** (Risco Extremo) |
|---|---|---|---|
| $1 \leq$ Risco $< 10$ | $10 \leq$ Risco $< 40$ | $40 \leq$ Risco $< 80$ | $80 \leq$ Risco $\leq 100$ |

Fonte: Referencial básico de gestão de riscos (TCU, 2018)

O Quadro 4 também apresenta os intervalos de valores e respectivas cores na Matriz de Riscos.

Após a avaliação, deve ser apresentada uma resposta ao evento de riscos de acordo com o grau de exposição. Esta resposta é apresentada na etapa de tratamentos dos riscos

O grau de criticidade do evento de risco (extremo, alto, médio ou baixo) especifica a sua localização ao longo da matriz de riscos. O canto inferior esquerdo da matriz de risco indica a criticidade mais baixa que um dado evento de risco pode assumir. Por outro lado, o canto superior direito da matriz de riscos, indica a criticidade mais elevada que um determinado evento de risco pode representar à empresa.

**5.4.1 Apetite a riscos**

O apetite a riscos da Valec definido pelo Conselho de Administração correspondente à área verde e amarela da Matriz de Riscos. Portanto, eventos de riscos com o grau de criticidade inferior ao valor de 40, estão dentro do apetite a riscos da Valec.

Por conseguinte, todo evento de risco com o grau de exposição (nível de risco) igual ou superior ao valor de 40, ou seja, localizado na área laranja ou vermelha da Matriz de Riscos, está além do apetite a riscos da empresa e necessariamente devem ser apresentadas pelos gestores soluções com vistas ao tratamento dos riscos.

**5.4.2 Priorização dos Riscos**

No processo de gestão de riscos, para efeitos de priorização na etapa de tratamento dos riscos, deve ser considerado o grau de criticidade (extremo, alto, médio ou baixo).

Os eventos de riscos que devem ser objeto de mitigação e priorização na etapa de tratamento, são aqueles classificados com grau de criticidade alto ou extremo, pois conforme limite de exposição na matriz de riscos, estão além do apetite a riscos da Valec.

A prioridade no tratamento dos eventos de riscos, que incorpora o grau de criticidade como fator preponderante, consiste com base nos critérios descritos no Quadro 5.

**QUADRO 5 - DIRETRIZES PARA A PRIORIZAÇÃO E TRATAMENTO DOS RISCOS**

| GRAU DE CRITICIDADE | CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS |
|---|---|
| RE | Grau de exposição **muito além do apetite a risco**. Qualquer risco nesse nível deve ser co municado à governança e alta administração e ter uma respost imediata. Postergação de medidas só com autorização do dirigente máximo |
| RA | Grau de exposição **além do apetite a risco**. Qualquer risco nesse nível dever ser comunica do a alta administração e ter uma ação tomada em período determinado Postergação de medidas só com autorização do dirigente de área. |
| RM | Grau de exposição **dentro do apetite a risco**. Geralmente nenhuma medida especial é ne cessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais. |
| RB | Grau de exposição **dentro do apetite a risco**, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles. |

Fonte: Referencial básico de gestão de riscos (TCU, 2018)

A Tabela 2 apresenta as informações que são obtidas na etapa de avaliação dos eventos de riscos.

**TABELA 2 - AVALIAÇÃO DOS RISCOS**

| Avaliação dos Riscos | | | | |
|---|---|---|---|---|
| Evento de Risco | Impacto - I (escala de impacto) | Probabilidade - P (escala de probabilidade) | Nível de Risco (PxI) | Prioridade do Risco |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Fonte: Manual de Gerenciamento de Riscos e Controles Internos (MJSP, 2020)

## 5.5 Tratamento dos Riscos

Esta etapa compreende a implementação das soluções aos eventos de riscos. Na descrição dessas soluções, podem ser estabelecidas quatro possíveis respostas ao evento de risco: aceitar, mitigar, transferir ou evitar.

Segue a descrição das respostas ao evento de riscos

- **Mitigar**: neste caso elabora-se um plano de ação, ou plano de mitigação, no qual devem ser descritas as ações gerenciais destinadas a reduzir a probabilidade e/ou impacto.
- **Aceitar**: esta opção de tratamento deve ser utilizada quando um risco não aceitável está fora do alcance de influência da organização, permanecendo inalterado ou ainda mantendo sua elevada criticidade apesar dos esforços de tratamento da organização. Esta opção também pode ser utilizada no caso em que a organização tem controle sobre o risco, mas o tratamento envolve custos proibitivos. Nesses casos, a organização pode considerar vantajoso criar planos de contingência para atenuar os efeitos das consequências advindas da materialização de um risco crítico.
- **Transferir**: é possível transferir parcial ou totalmente a responsabilidade por um risco, seja por meio de contratos, parceiras, seguros ou mesmo compartilhando a responsabilidade pelo risco, para garantir maior segurança no atingimento dos objetivos da empresa.
- **Evitar**: pode envolver deixar de perseguir determinado objetivo, empreendimento, projeto, processo ou descontinuar atividades, ou ainda mudar o caminho traçado rumo a um determinado objetivo, à realização de um

empreendimento, projeto ou atividade, deixando se expor a riscos que a organização julgue não poder suportar**.**

As opções de tratamento não são necessariamente exclusivas, podendo ser combinadas.

Antes de abordar o tópico relativo aos planos de tratamento (item 5.5.3), é essencial entender a relevância dos controles internos (item 5.5.1) e o cálculo do risco residual (item 5.5.2).

### 5.5.1 Controles Internos

Os controles internos constituem a ação de implementação para mitigação dos eventos de riscos, e são especialmente importantes em razão da capacidade reduzir o grau de exposição ao evento de riscos. É relevante citar que recorrentemente as unidades podem ter dificuldade na identificação ou institucionalização dos controles internos.

A título de exemplo, as unidades organizacionais podem ter desenvolvido ações, práticas e rotinas que são de extrema relevância para o processo, mas não estão institucionalizadas ou formalizadas de forma a garantir e eficácia, eficiência e perenização. Na ausência de formalização, na eventual substituição do gestor responsável, as boas práticas de governança e gestão podem ser abandonadas, descontinuadas ou esquecidas.

Outro conceito que pode ser aproveitado na identificação dos controles é a definição de controle interno fornecida pelo Livro Laranja: Gestão de Riscos - Princípios e Conceitos (*Orange Book: Management of risk - Principles and Concepts,* 2020) do Reino Unido. Para a estrutura metodológica desenvolvida pelo Livro Laranja, controle interno é: "*a estrutura dinâmica e iterativa de processos, políticas, procedimentos, atividades, dispositivos, práticas, ou outras condições e/ou ações que mantém ou modificam o risco. Os controles internos permeiam e são inerentes à maneira como a organização opera e são afetados pela cultura e por fatores ambientais.*".

**Caso já existam os controles, estes são analisados e verificados, para efeitos de cálculo do risco residual, conforme fórmula constante no tópico 5.5.2. Caso não existam os controles, o evento de risco é caracterizado como inerente.**

#### 5.5.2 Cálculo do risco residual

Para análise da efetividade dos controles deve ser utilizado o Quadro 6. A relação de controles internos indicados e estabelecidos para mitigar determinado evento de risco é avaliada segundo uma escala que relaciona um fator, denominado Risco de Controle, à uma descrição que indica a consistência do controle.

**QUADRO 6 - ESCALA PARA AVALIAÇÃO DE CONTROLES**

| NÍVEL DE CONFIANÇA (NC) | AVALIAÇÃO DO DESENHO E IMPLEMENTAÇÃO DOS CONTROLES (ATRIBUTOS DO CONTROLE) | RISCO DE CONTROLE (RC) |
|---|---|---|
| **Inexistente** | Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais. | **Muito Alto 1,0** |
| **Fraco** | Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas. | **Alto 0,8** |
| **Mediano** | Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas. | **Médio 0,6** |
| **Satisfatório** | Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente. | **Baixo 0,4** |
| **Forte** | Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco. | **Muito Baixo 0,2** |

Fonte: Referencial básico de gestão de riscos (TCU, 2018)

Portanto, os controles internos devem ser criteriosamente avaliados de forma a verificar em qual nível de confiança e Risco de Controle (RC) estes se enquadram.

Por conseguinte, o valor do grau de exposição (nível de risco) do risco residual é calculado a partir da multiplicação entre o valor do grau de exposição do risco inerente e o fator de avaliação dos controles, denominado Risco de Controle (RC), conforme fórmula:

**NRR = NRI x RC**

*em que:*

- **NRR** = nível de risco residual (grau de exposição)
- **NRI** = nível de riscos inerente (grau de exposição)
- **RC** = Risco de Controle

**5.5.3 Planos de Tratamento**

Os eventos de riscos que devem ser objeto de mitigação e priorização na etapa de tratamento, são aqueles classificados com grau de criticidade alto ou extremo, pois conforme limite de exposição na matriz de riscos, estão além do apetite a riscos da Valec.

Caso a resposta seja mitigar o evento de risco, devem ser elaborados os planos de tratamento (planos de ação) com a implementação de novos controles ou aprimoramento dos controles internos existentes, com as ações no sentido de reduzir a probabilidade de sua ocorrência ou seu impacto.

Estes planos de tratamento devem conter as informações constantes na Tabela 3: evento de risco, objeto (empreendimentos, programas, negócios, dentre outros), causas, unidade organizacional, grau de exposição (nível de risco) e grau de criticidade (baixo, médio, alto ou extremo), ações e controles internos propostos, tipo de controle (preventivos, detectivos ou mitigatórios), responsável e prazo (início e fim).

**TABELA 3 - PLANOS DE TRATAMENTO (PLANOS DE AÇÃO)**

| **Evento de Risco** | Objeto | Causas | Unidade organizacional | Nível de Risco | **Tratamento do evento de risco** | | |
|---|---|---|---|---|---|---|---|
| | | | | | Controles internos | Prazos | |
| | | | | | Ação de implementação | Início | Fim |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Os controles internos podem ser de três tipos: preventivos (quando atuam na causa); detectivos (quando estão relacionados com a detecção do evento de risco); ou, mitigatórios (quando atuam no impacto).

Os planos de tratamento são constituídos de ações de implementação, como resposta ao evento de risco. As medidas mitigadoras podem envolver a adoção de controles, redesenho de processos, realocação de pessoas, ações de capacitação, desenvolvimento ou aperfeiçoamento de soluções de TI, adequação da estrutura organizacional, dentre outros.

As ações de implementação devem ser analisadas e estabelecidas através das oficinas entre a SUINT e a superintendência responsável. Portanto, os planos de tratamento são elaborados pela superintendência responsável pelo evento de risco, com o apoio metodológico da SUINT.

Após a conclusão do plano de tratamento, com base nas ações implementadas é realizado o cálculo do risco residual, de forma a verificar se o evento de risco foi mitigado, ou seja, se está abaixo do limite de exposição na matriz de riscos.

As informações constantes nas etapas de análise, avaliação e tratamento, devem ser enviadas para as respectivas diretorias para a análise, aprovação e posterior envio à SUINT.

As informações do processo de gestão de riscos integram o relatório trimestral referente a gestão de riscos e controles internos, elaborados pela SUINT, que são enviados para a Diretoria Executiva, para posterior análise e deliberação do Conselho de Administração.

No intuito de apresentar as informações do evento de risco de forma consolidada, segue abaixo a Tabela 4 com o Mapa de Gestão de Riscos.

**TABELA 4 - MAPA DE GESTÃO DE RISCOS**

| MAPA DE GESTÃO DE RISCOS | TRIMESTRE/ANO: |
|---|---|
| **RISCO:** | |
| **DESCRIÇÃO:** | |

| CAUSAS |
|---|
| **1..** |
| **2..** |
| **3..** |
| **UNIDADES ORGANIZACIONAIS ENVOLVIDAS:** |

| PROBABILIDADE | | | IMPACTO | | | NÍVEL DE RISCO | |
|---|---|---|---|---|---|---|---|
| | 1 | Muito baixa | | 1 | Mínimo | | RE - Risco Extremo<br>80 ≤ Risco ≤ 100 |
| | 2 | Baixa | | 2 | Pequeno | | RA - Risco Alto<br>40 ≤ Risco < 80 |
| | 5 | Média | | 5 | Moderado | | RM - Risco Médio<br>10 ≤ Risco < 40 |
| | 8 | Alta | | 8 | Significativo | | RB - Risco Baixo<br>1 ≤ Risco < 10 |
| | 10 | Muito alta | | 10 | Catastrófico | | |

| CONTROLES INTERNOS |
|---|
| **1..** |
| **2..** |
| **3..** |

| NÍVEL DE CONFIANÇA | | NÍVEL DE RISCO RESIDUAL | | CONSIDERAÇÕES |
|---|---|---|---|---|
| Inexistente (RC = 1,0) | | | RE - Risco Extremo | |
| Fraco (RC = 0,8) | | | RA - Risco Alto | |
| Mediano (RC = 0,6) | | | RM - Risco Médio | |
| Satisfatório (RC = 0,4) | | | RB - Risco Baixo | |
| Forte (RC = 0,2) | | | | |

| AÇÃO (CONTROLE INTERNO) | RESP. | PRAZO | | STATUS | | CONSIDERAÇÕES |
|---|---|---|---|---|---|---|
| | | INÍCIO | FIM | ✔ | ✖ | |
| **1..** | | | | | | |
| **2..** | | | | | | |
| **3..** | | | | | | |
| **4..** | | | | | | |
| **5..** | | | | | | |

## 5.6 Comunicação e Consulta

Esta etapa permeia todo o processo de gestão de riscos e consiste no fornecimento de informações relativas ao evento de risco e ao seu tratamento para todos que possam diretamente influenciar ou ser influenciados por esse evento de risco, sob pena de ele se materializar plenamente.

De acordo com a ISO 31000:2018, o propósito desta etapa é prestar assistência e apoio metodológico às partes interessadas, a respeito da compreensão dos riscos e de todas as etapas do processo de gestão de riscos, de forma a fornecer bases e subsídios para tomada de decisões e as razões pelas quais ações específicas são exigidas no processo. A assistência e apoio metodológico é de responsabilidade da SUINT.

O fluxo de comunicação das informações da gestão de riscos pode ser horizontal ou vertical.

A comunicação horizontal, quando envolve diversas unidades de diretorias diferentes, é feita a partir da interlocução da SUINT com as diretorias e superintendências, no intuito de integrar as informações e instruir o processo de gestão de riscos.

A comunicação vertical é no sentido da unidade organizacional para o órgão máximo de governança da estatal, o Conselho de Administração, ou vice-versa. É quando o processo e o evento de risco envolvem especificamente uma unidade.

No que tange ao fluxo de comunicação horizontal e vertical, trimestralmente a SUINT elabora o relatório acerca da gestão de riscos, controles internos, para envio à Diretoria Executiva, para posterior análise e deliberação do Conselho de Administração.

A comunicação visa a promover a ciência e a compreensão dos eventos de riscos e, a consulta, envolve a obtenção de *feedbacks* e informações necessárias para o apoio à tomada de decisão. A coordenação adequada entre a comunicação e a consulta favorece a troca de informações precisas, relevantes, oportunas e baseadas em evidências factuais, levando em consideração a confidencialidade e a integridade da informação.

A título de informação sobre o relatório trimestral de riscos e controle internos, conforme recomendações do Comitê de Auditoria, a metodologia adotada na elaboração dos relatórios poderá ser complementada, gradativamente, com a implementação do COSO *(COSO ERM - Enterprise Risk Management,* 2017*).*

De acordo com a Figura 8, o *framework* é um conjunto de princípios organizados em cinco componentes principais interrelacionados: governança e cultura; estratégica e definição de objetivos; performance; análise e revisão; e, informação, comunicação e divulgação. Esta versão do COSO atualizada em 2017, potencializa a importância da gestão de riscos no processo de definição da estratégia da organização e na condução de seus resultados.

**FIGURA 8 - GERENCIAMENTO DE RISCOS - COSO ERM**


Fonte: COSO (*Committee of Sponsoring Organizations of the Treadway Commission*, 2017*)*

Conforme com a Figura 9, os cinco componentes do novo *framework* se combinam em um conjunto de princípios. Esses princípios abrangem desde a governança até o monitoramento. Esses descrevem práticas que podem ser aplicadas de diferentes formas nas organizações, independentemente do seu tamanho, tipo ou setor econômico.

**FIGURA 9 - PRINCÍPIOS DE GERENCIAMENTO DE RISCOS - COSO ERM**


Fonte: COSO (*Committee of Sponsoring Organizations of the Treadway Commission*, 2017*)*

## 5.7 Monitoramento e melhoria contínua

Esta etapa permeia todo o processo de gestão de riscos e consiste em detectar mudanças no ambiente externo e interno, que podem alterar as informações relacionadas aos eventos de riscos identificados ou a identificação de novos riscos.

O monitoramento também compreende o acompanhamento e a verificação do desempenho ou da situação dos elementos da gestão de risco, bem como a revisão da política, do manual, dos eventos de riscos, dos controles internos e dos planos de tratamento. O monitoramento é realizado pela Superintendência de Integridade-SUINT e pelo Comitê de Governança, Riscos e Controle - CGRC.

Os planos de tratamento (planos de ação) são objeto de constante monitoramento pela segunda linha e comitê correlato ao tema. Este monitoramento envolve o acompanhamento dos prazos das ações e controles propostos, relacionadas com os eventos de riscos.As ações de implementação estão associadas ao evento de risco em específico que, por sua vez, está relacionado com um ou mais objetivos e metas estratégicas. Portanto, os prazos das ações e controles propostos devem estar compatíveis, de forma a convergir com o prazo para a conclusão das metas estratégicas.

O ciclo institucional da gestão de riscos acompanha o ciclo institucional do planejamento estratégico. Nesta esteira, os relatórios relacionados com a gestão de riscos são apresentados para deliberação do CONSAD de forma integrada com os relatórios relacionados com o planejamento estratégico. O objetivo do procedimento é sempre garantir a integração da gestão de riscos e controles internos com o planejamento estratégico institucional.

O acompanhamento e verificação podem resultar na melhoraria contínua do processo, com aperfeiçoamento ou ajustes nos elementos da gestão de riscos avaliados no processo de gerenciamento de riscos. Ante o exposto, a Política de Gestão de Riscos, Controle e Conformidade, o manual e o presente tutorial, após a execução das etapas do processo de gestão de riscos, estão sujeitos a melhoria contínua, atualizações e aprimoramentos.

Devido à abrangência e à complexidade do tema, o Manual e Tutorial de Gestão de Riscos da Valec serão implantados de forma gradual e continuada, com o monitoramento a partir de relatórios trimestrais.

O Manual e Tutorial de Gestão de Riscos devem ser atualizados ou ratificados em intervalos não superiores a 2 (dois) anos ou quando mudanças significativas ocorrerem, para a assegurar a sua contínua pertinência, adequação e eficácia.

## 6. Considerações Finais

A Gestão de Riscos Corporativos tem como principal objetivo o cumprimento dos objetivos e metas constantes no Planejamento Estratégico Institucional-PEI 2020-2024. Além do PEI 2020-2024, foi aprovado pelo Conselho de Administração, o Relatório de Remuneração Variável Anual-RVA 2022 dos membros da Diretoria Executiva, com um conjunto de metas ao longo do ano que também são objeto de gerenciamento de riscos.

O gerenciamento de riscos e controles compõe uma das 3 dimensões que foram consideradas na avaliação das empresas estatais em 2021, através do Indicador de Governança - IG-SEST. No 5° Ciclo do Indicador de Governança - IG-SEST, da Secretaria de Coordenação e Governança das Empresas Estatais/SEST (Ministério da Economia), na avaliação das empresas estatais foram consideradas 3 dimensões:

- Dimensão 1 - Governança, Conselhos e Diretoria;
- Dimensão 2 - Transparência; e
- Dimensão 3 - Gerenciamento de Riscos e Controles.

Em 2022, o gerenciamento de riscos e controles também compõe uma das 3 dimensões do 6° Ciclo do IG-SEST. As dimensões são: Dimensão 1: Conselhos e Diretoria; Dimensão 2: Transparência; e, Dimensão 3: Gerenciamento de Riscos, Controles e Auditoria.

A gestão de riscos e controles internos das empresas públicas também é avaliada pelo Tribunal de Contas da União-TCU, para a composição do índice integrado de governança e gestão (iGG).

Portanto, o processo de gestão de riscos eficaz contribui de forma efetiva no alcance dos objetivos e metas do PEI 2020-2024 e RVA-2022, adoção das melhores práticas de governança, capacitação os gestores no tema e melhores pontuações da Valec nos índices de governança da Administração Pública.

Por fim, considerando que o processo de gerenciamento de riscos e controle está em aprimoramento contínuo, a Política de Gestão de Riscos, Controle e Conformidade, o Manual de Gestão de Riscos e o Tutorial de Gestão de Riscos, podem ser alterados e ajustados para adaptarem ao grau de maturidade alcançado pelas áreas da Valec às novas práticas utilizadas, assim como metodologias de destaque na Administração Pública Federal e referências internacionais.

## 7. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO 31.000:2018. **Gestão de Riscos**. 2018.

BRASIL. **Decreto 8945, de 27 de dezembro de 2016**. Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. 2016.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. **COSO Enterprise Risk Management - Integrating with Strategy and Performance - Executive Summary**. 2017.

GOV.UK. **Orange Book: Management of risk - Principles and Concepts**. Versões de 2004 e 2020.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Manual de Gerenciamento de Riscos e Controles Internos**. 2020.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO-CGU. **Metodologia de Gestão de Riscos**. 2018.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão**. 2017.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. **Resolução CGPAR N° 18**. 2016.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO e CONTROLADORIA-GERAL DA UNIÃO. **Instrução Normativa Conjunta n° 1/2016**. 2016.

THE INSTITUTE OF INTERNAL AUDITORS - IIA. **Modelo das Três Linhas**. 2020.

TRIBUNAL DE CONTAS DA UNIÃO. **Manual de Gestão de Riscos do TCU**. 2020.

TRIBUNAL DE CONTAS DA UNIÃO. **Referencial básico de Gestão de Riscos**. 2018.

VALEC ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A. **Política de Gestão de Riscos, Controle e Conformidade**, Resolução Normativa Valec n° 9/2021/CONSAD- Valec. 2021.

VALEC ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A. **Regimento Interno da Auditoria Interna**, Resolução Valec n° 7/2020/CONSAD-Valec. 2020.

Documento assinado eletronicamente por **MARCELLO DA COSTA VIEIRA**, **Presidente do Conselho de Administração**, em 31/05/2022, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.infraestrutura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5633180** e o código CRC **7D260614**.



SAUS Quadra 01, Bloco G, Lotes 3 e 5 - Bairro ASA SUL
Brasília/DF, CEP 70070010
Telefone: 2029-6100 - www.valec.gov.br