CISAL CONSTRUÇÕES

ALOÍSIO ZIMMER advogados associados

Compliance SISTEMAS DE INTEGRIDADE

PROGRAMA DE INTEGRIDADE

RISK ASSESSMENT

ATUALIZADO ATÉ AGOSTO 2024

PROGRAMA DE INTEGRIDADE

O **PROGRAMA DE INTEGRIDADE**, ou como comumente chamado de ***compliance***, está relacionado à noção de conformidade, a aderir a um determinado sistema legal, a regras internas e contratuais. O aparecimento desta figura no campo do direito anticorrupção se deve à necessidade de somar às medidas de repressão precauções de prevenção, de forma a criar um sistema de incentivos capaz de fortalecer uma cultura de integridade.

A Lei n. 12.846/2013, de forma ampla, aproximou o tema das pessoas jurídicas de direito privado em geral, enquanto a Lei n. 13.303/2016 exigiu a implementação de programas de integridade para as empresas públicas e as sociedades de economia mista.

O investimento em mecanismos preventivos de corrupção, de fraude e de condutas antiéticas é essencial para evitar a responsabilização da pessoa jurídica por ações ou omissões de terceiros. Isso porque a prática de atos ilícitos tipificados na lei por pessoas físicas que, não sendo da diretoria ou da administração, ajam em nome ou a serviço da empresa, produzirá a responsabilização objetiva da pessoa jurídica em cujo interesse ou benefício o ato foi praticado.

Os programas de integridade aparecem, nesse sentido, como importantes aliados no aumento do controle de dirigentes e administradores sobre atos praticados em interesse ou benefício da pessoa jurídica, de modo a mitigar riscos de infringência à Lei n. 12.846/2013 e de atração de suas sanções.

Nesse sentido, o escritório **ALOÍSIO ZIMMER ADVOGADOS** foi contratado para implementar o Programa de Compliance da **CISAL CONSTRUÇÕES LTDA** a fim de adequar-se às normas anticorrupção e ao que há de mais moderno em governança pública.

Segundo o inciso I art. 2º do Decreto Federal n. 9.203/2017, a governança pública consiste *no conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.*

Por sua vez, o inciso IV art. 2º do Decreto Federal n. 9.203/2017 define gestão de riscos como *processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos*.

Os programas de compliance não têm, por certo, a pretensão de eliminar atos ilícitos, mas, sim, de mitigar riscos quanto à prática de ações da espécie. Isso porque, por meio deles, criam-se ferramentas para identificação célere da iminência ou ocorrência de ilícitos, facilitando a resolução dos problemas daí derivados.

Para tanto, esses programas estruturam-se a partir de **CINCOS ELEMENTOS FUNDAMENTAIS**[1]:

- ✓ **desenvolvimento do ambiente de gestão do programa de integridade;**
- ✓ **detecção, avaliação e tratamento de riscos;**
- ✓ **estruturação e implantação das políticas e dos procedimentos;**
- ✓ **comunicação e treinamento; e**
- ✓ **monitoramento do programa, medidas de remediação e aplicação de penalidades.**

Como se nota, o mapeamento de riscos de compliance – ou **COMPLIANCE RISK ASSESSMENT** – é um dos mecanismos do programa de integridade.

Essa avaliação é realizada a partir de uma dupla perspectiva, relativamente à organização: **1)** a perspectiva interna, já que cada um possui especificidades tanto em sua estrutura interna quanto no relacionamento com terceiros – outras empresas, colaboradores, órgãos e agentes públicos etc.; e **2)** a perspectiva externa, dado que cada setor apresenta características diferentes.

[1] BRASIL. Controladoria-Geral da União. **Guia de implantação de programa de integridade nas empresas estatais**: orientações para a gestão da integridade nas empresas estatais federais. Brasília: CGU, dez. 2015. Disponível em: <*www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/guia_estatais_final.pdf*>. Acesso em dez 2022.

Em termos procedimentais, a organização precisa considerar as seguintes etapas: conhecimento da própria instituição; conhecimento do ordenamento jurídico incidente sobre a atividade desenvolvida e sobre seus agentes; identificação dos fatores e das atividades da empresa mais expostos a risco; criação de uma classificação de risco das atividades; apresentação das ferramentas de mitigação dos riscos encontrados e recomendação de utilização de novos instrumentos; estabelecimento de um grau de risco desejado para o desenvolvimento das atividades da entidade; e acompanhamento e implementação dos instrumentos de mitigação.

Para tanto, na reunião inaugural, Dr. Aloísio Zimmer detalhou o passo-a-passo da implantação de um Programa de Compliance efetivo:

1 REUNIÃO INAUGURAL: Nesta etapa, é tratado junto aos diretores da instituição sobre quais serão os passos de implementação do Programa de Compliance.

2 COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO: O comprometimento da alta administração da instituição com a integridade nas relações público-privadas e, consequentemente, com o Programa de Compliance é a base para a criação de uma cultura organizacional em que funcionários e terceiros efetivamente prezem por uma conduta ética. Possui pouco ou nenhum valor prático um Programa que não seja respaldado pela alta direção. A falta de compromisso da alta direção resulta no descompromisso dos demais funcionários, fazendo o Programa de Integridade existir apenas "no papel".

3 ENTREVISTAS: Os diretores e principais colaboradores serão entrevistados para que se tenha pleno entendimento do funcionamento da instituição. Além disso, estas entrevistas têm por finalidade o mapeamento dos riscos que a instituição está exposta em todos os setores.

4 ANÁLISE DE RISCOS: Efetuadas as entrevistas, é o momento de realizar a listagem dos riscos identificados na instituição. A partir desta lista, será efetivada a análise dos riscos inerente e residual, a partir da matriz probabilidade x impacto. Realizada tal etapa, a Alta Administração deverá validar a matriz de riscos, com o encaminhamento da gestão destes riscos (aceitar, transferir, mitigar ou eliminar).

5 CÓDIGO DE ÉTICA: Mapeada a instituição e identificados os riscos, será elaborado o código de ética e conduta da empresa que, obrigatoriamente, conterá os seguintes pontos: a) princípios, missões e valores; b) conflito de interesses; c) vedação de atos de corrupção e fraude; d) sanções aplicáveis.

6 COMITÊ DE ÉTICA: Serão eleitas as pessoas que formarão um comitê de ética (o código de ética deverá prever a existência) para deliberar sobre assuntos do compliance, bem como para a apuração das denúncias recebidas.

7 CANAL DE DENÚNCIAS: Estruturação de um canal de denúncias que assegurará a anonimidade do denunciante, caso requisitado. Este canal de denúncias deverá ser físico (na sede da empresa) e on-line (através de seu site e/ou e-mail indicado).

8 POLÍTICAS: Criação de políticas de brindes e presentes, contratos padrões com cláusula anticorrupção, formulário de pessoa politicamente exposta etc.

9 TREINAMENTO: A partir de toda a documentação gerada na instituição, será realizado o treinamento dos diretores e funcionários

para o entendimento do código de conduta, o canal de denúncias e as políticas criadas. Estes treinamentos poderão ser presenciais ou remotos, ao vivo ou gravados, a depender do porte e necessidade da instituição.

10 MONITORAMENTO CONTÍNUO: Implementado o Programa de Compliance, será monitorado o seu bom andamento, com o recebimento, investigação e tratamento das denúncias, realizando a revisão anual da matriz de riscos, o treinamento anual etc.

Os membros da Alta Administração foram então convocados para participar de uma reunião, no intuito de contar com o engajamento de todos para o bom andamento do Programa de Compliance da **CISAL CONSTRUÇÕES LTDA**. Posteriormente, os membros da Alta Administração da empresa assinaram um termo de compromisso com o Programa de Integridade.

Em sequência, a equipe de Consultoria **ALOÍSIO ZIMMER ADVOGADOS** realizou entrevistas com os principais colaboradores da **CISAL CONSTRUÇÕES LTDA**, a fim de conhecer toda a estrutura organizacional da empresa, bem como identificar os riscos pelos quais está exposta, aperfeiçoando o modelo existente e propondo novo olhar sobre a matriz de riscos.

Assim, realizadas as entrevistas, elaborou-se a relação dos riscos detectados, classificando-os conforme **ISO 31000:2018 ABNT**, o que foi objeto de acompanhamento e avaliação por parte dos Diretores.

Após a aprovação da Diretoria, foi definitivamente aprovada e consolidada a **MATRIZ DE RISCOS** da **CISAL CONSTRUÇÕES LTDA**, com o encaminhamento da gestão dos riscos encontrados.

RISK ASSESSMENT

Toda organização, seja empresarial ou não, é fundada no intuito de se atingir os **OBJETIVOS** estabelecidos nos seus atos constitutivos, que vão sendo implementados e gradativamente aprimorados ao longo de suas atividades. Estes objetivos, por vezes, não são descritos nos atos constitutivos, mas fazem parte do espírito da organização, como atender todos os clientes com dignidade e respeito, prestar o serviço de forma eficiente e rápida etc.

Todavia, é preciso entender que organizações de todos os tipos e tamanhos enfrentam influências e fatores externos e internos que afastam os gestores de seus objetivos, o que se convencionou chamar de **RISCOS**, provocando incertezas e inseguranças à governança corporativa.

Por isso, detectar e gerenciar periodicamente os **RISCOS** é ferramenta que auxilia as empresas no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas, levando-se em conta as perspectivas interna e externa, incluindo o comportamento humano e os fatores culturais.

Além disso, administrar **RISCOS** é parte da governança e liderança, cujo objetivo também é melhorar o desempenho da organização, encorajar a alta administração nos caminhos seguros para garantir a longevidade e eficiência econômica da empresa e apoiar o alcance dos objetivos.

A Committee of Sponsoring Organizations of the Treadway Commission (COSO) define risco como a possibilidade de que um evento ocorra e afete desfavoravelmente a realização dos objetivos. Já o Instituto Brasileiro de Gestão Corporativa define risco da seguinte forma:

> Costuma-se entender risco como possibilidade de algo não dar certo. Mas seu conceito atual no mundo corporativo vai além: envolve a quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organizações. Sendo o risco inerente a qualquer atividade – e impossível de eliminar –, a sua administração é um elemento-chave para a sobrevivência das companhias e demais entidades.[2]

[2] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de riscos corporativos**: evolução em governança e estratégia / Instituto Brasileiro de Governança Corporativa. São Paulo, SP: IBGC, 2017. (Série Cadernos de Governança Corporativa, 19). p. 11

Entender a quais riscos a instituição está exposta é fundamental não somente para os assuntos relacionados à integridade ou propriamente de direito, mas também para a própria atividade fim da organização. Entender os riscos é entender a instituição.

O Decreto Federal n. 8.420/2015, que regulamenta a Lei Federal n. 12.846/2013 (Lei Anticorrupção), quando conceitua o que é um programa de integridade, em seu parágrafo único, dispõe que "*O programa de integridade deve ser estruturado, **aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica**, a qual por sua vez deve garantir o constante aprimoramento e adaptação do referido programa, visando garantir sua efetividade*".[3]

Desta forma, o inciso V do mesmo Decreto determina que é obrigatória a "***análise periódica de riscos** para realizar adaptações necessárias ao programa de integridade*".[4]

Sobre a Análise de Riscos, a Controladoria-Geral da União teceu as seguintes considerações:

> Além da análise do perfil da empresa, a estruturação de Programa de Integridade depende também de uma avaliação de riscos que leve em conta as características dos mercados onde a empresa atua (cultura local, nível de regulação estatal, histórico de corrupção). Essa avaliação deve considerar principalmente a probabilidade de ocorrência de fraudes e corrupção, inclusive ligadas a licitações e contratos, e o impacto desses atos lesivos nas operações da empresa. Com base nos riscos identificados, serão desenvolvidas as regras, políticas e procedimentos para prevenir, detectar e remediar a ocorrência dos atos indesejados. É importante que o processo de mapeamento de riscos seja periódico a fim de identificar eventuais novos riscos, sejam eles decorrentes de alteração nas leis vigentes ou de edição de novas regulamentações, ou de mudanças internas na própria empresa, como ingresso em novos mercados, áreas de negócios ou abertura de filiais, por exemplo.

Assim, a **ANÁLISE DE RISCOS** serve para estabelecer quais serão os caminhos que o Programa de Compliance seguirá, a fim de resguardar a empresa de eventual conduta em desacordo com a legislação ou até mesmo de seu regramento interno.

[3] BRASIL, Decreto 8.420 (2015), art. 41. Disponível em <*http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm*>. Acesso em dez 2022.
[4] BRASIL, Decreto 8.420 (2015), art. 41. Disponível em <*http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm*>. Acesso em dez 2022.

É a partir da análise de riscos que o Código de Ética e Conduta é gerado, pois este Código deverá se adequar à realidade da empresa e atacar frontalmente os pontos mais sensíveis da organização, de modo a mitigar a ocorrência dos eventos indesejáveis.

O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.[5]

Segundo **ISO 31000:2018 ABNT**:

> O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da Alta Direção.[6]

Além disso, identificados os riscos, as políticas e procedimentos serão criadas a partir das demandas existentes derivadas destes riscos. De mesmo modo, os treinamentos aos colaboradores terão enfoque maior nas áreas onde os riscos se mostrem mais sensíveis à empresa.

Identificados e analisados os riscos, cabe à Alta Administração, com apoio do Departamento de Compliance, a realização da gestão destes riscos.

A ABNT define as **GESTÕES DE RISCOS** como atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos[7]. Conforme abordado pela **ISO 31000:2018 ABNT**, a importância da Gestão de Riscos é:

- **desenvolvimento do ambiente de gestão do programa de integridade;**
- **melhorar a identificação de oportunidades e ameaças;**

[5] BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). **Manual Prático de Avaliação de Programa de Integridade em PAR**. p. 42. Disponível em <*https://repositorio.cgu.gov.br/bitstream/1/46645/1/Manual_pratico_integridade_PAR.pdf*>. Acesso em dez 2022.
[6] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO 31000**. Gestão de Riscos - Diretrizes. *Risk Management – Guidelines.* Segunda Edição, 28/03/2018. p. 4.
[7] ABNT ISO GUIA 73:2009, definição 2.1.

- **atender às normas internacionais e requisitos legais e regulatórios pertinentes;**
- **melhorar o reporte das informações financeiras;**
- **melhorar a governança;**
- **melhorar a confiança das partes interessadas;**
- **estabelecer uma base confiável para a tomada de decisão e o planejamento;**
- **melhorar os controles;**
- **alocar e utilizar eficazmente os recursos para o tratamento de riscos;**
- **melhorar a eficácia e a eficiência operacional;**
- **melhorar o desempenho em saúde e segurança, bem como a proteção do meio ambiente; — melhorar a prevenção de perdas e a gestão de incidentes;**
- **minimizar perdas;**
- **melhorar a aprendizagem organizacional; e**
- **aumentar a resiliência da organização.**

Dito isso, a **ANÁLISE DE RISCOS** é um pilar fundamental para o Programa de Compliance efetivo, na medida em que desencadeará todos os demais passos que se desenvolverão ao longo da sua implementação. Segundo disposição da **ISO 31000:2018 ABNT**:

> O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos. Convém que o processo de avaliação de riscos seja conduzido de forma sistemática, iterativa e colaborativa, com base no conhecimento e nos pontos de vista das partes interessadas. Convém que use a melhor informação disponível, complementada por investigação adicional, como necessário.[8]

[8] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO 31000**. Gestão de Riscos - Diretrizes. *Risk Management – Guidelines.* Segunda Edição, 28/03/2018. p. 12.

Logo, uma boa análise de riscos permite que a empresa entenda melhor o seu funcionamento e desenvolva melhores mecanismos de governança, proporcionando uma maior efetividade e conformidade legal, além de acreditação perante terceiros.

Ponto importante a se ressaltar é que o inciso IV do art. 42 do Decreto n. 8.420/2015 obriga que a análise de riscos seja periódica. Embora não haja uma previsão legal quanto à periodicidade, a **CONTROLADORIA-GERAL DA UNIÃO**[9] prevê como critério de avaliação em seu formulário a atualização da análise de riscos após 24 meses.

De outra banda, o Plano de Integridade do **MINISTÉRIO DA INFRAESTRUTURA** (MInfra), que serve de modelo de consulta para o setor, define que:

> O monitoramento será feito de forma contínua, pela primeira linha (gestores), de forma periódica, quando houver alguma mudança relevante no Ministério, ou quando provocado por alguma das instâncias de segunda ou terceira linha. Os aspectos a serem monitorados são: se os riscos continuam afetando os objetivos, como concluído na última avaliação do processo, se surgiram novos riscos e se os controles internos permanecem eficientes.[10]

Como se nota, a CGU e o MInfra estabelecem modelos diferentes de revisão periódica de riscos, optando a primeira pelo modelo de revisão bienal e a segunda pela revisão apenas no caso de "*mudança relevante*" no Ministério ou quando provocado. Como "*mudança relevante*", o MInfra definiu, pelo menos, quatro fatores: ***i)*** inovação tecnológica, ***ii)*** mudanças relevantes nas lideranças e nos colaboradores, ***iii)*** mudança do ambiente regulatório ou econômico e ***iv)*** necessidade de crescimento rápido de determinada atividade/processo.[11]

Ou seja, não há uma regra definida, podendo ser estabelecido pela organização o modelo que melhor se adequar à gestão estratégica desenhada pela Alta Administração.

---

[9] BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). **Manual Prático de Avaliação de Programa de Integridade em PAR**. p. 42. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/46645/1/Manual_pratico_integridade_PAR.pdf

[10] BRASIL. MINISTÉRIO DA INFRAESTRUTURA. Comitê Estratégico de Governança. **Manual de Gestão de Riscos dos Processos de Trabalho**. Portaria MInfra n. 55/2021, art. 35, anexo II. Versão 1.0. 05/2021. Disponível em <*https://www.gov.br/infraestrutura/pt-br/assuntos/ManualGestao_de_Risco2021_Minfra_final.pdf*>. Acesso em dez 2022. p. 54.

[11] BRASIL. MINISTÉRIO DA INFRAESTRUTURA. Comitê Estratégico de Governança. **Manual de Gestão de Riscos dos Processos de Trabalho**. Portaria MInfra n. 55/2021, art. 35, anexo II. Versão 1.0. 05/2021. Disponível em <*https://www.gov.br/infraestrutura/pt-br/assuntos/ManualGestao_de_Risco2021_Minfra_final.pdf*>. Acesso em dez 2022. p. 55.

Logo, é importante que o Compliance Officer defina, juntamente com a Alta Administração, o melhor modelo de revisão periódica para a **CISAL CONSTRUÇÕES E LTDA,** anotando-se, desde já, que, em razão do setor em que atua, a instituição precisa estar atenta a eventuais novos riscos, sejam eles decorrentes de alteração nos marcos legais vigentes e edição de novas regulamentações infralegais, inovações tecnológicas, além de relevantes mudanças no ambiente de negócios, bem como em reestruturações internas na própria organização, como ingresso em novos mercados, áreas de negócios ou abertura de filiais, por exemplo.

METODOLOGIA

Conforme abordado nos tópicos anteriores e utilizando a metodologia definida na **ISO 31000:2018 ABNT**, na **CGU** e pelo **COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION** (**COSO**), a Consultoria **ALOÍSIO ZIMMER ADVOGADOS** realiza entrevistas com atores da **CISAL CONSTRUÇÕES LTDA**, além da análise de documentos e de perfil da empresa.

Estas entrevistas possibilitaram um maior entendimento do funcionamento da organização e dos riscos aos quais a **CISAL CONSTRUÇÕES LTDA** está exposta.

A etapa de avaliação dos riscos visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimativa da probabilidade de ocorrência e do impacto destes eventos identificados como risco nos objetivos dos processos organizacionais. Normalmente, as causas se relacionam à probabilidade de o evento ocorrer e as consequências ao impacto, caso o evento se materialize.

Como metodologia de **COMPLIANCE RISK ASSESSMENT** (CRA), a Consultoria **ALOÍSIO ZIMMER ADVOGADOS** se utilizou do padrão estabelecido pela **CONTROLADORIA-GERAL DA UNIÃO**, pela **ISO 31000:2018 ABNT** e pelo **COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION** (**COSO**), através da matriz **PROBABILIDADE X IMPACTO**[12].

Nesta metodologia, o CRA é realizado a partir das seguintes etapas:

[12] BRASIL. CONTROLADORIA-GERAL DA UNIÃO. **Guia Prático de Gestão de Riscos para a Integridade**: Orientações para a administração pública federal direta, autárquica e fundacional, 2018, P. 31. Disponível em: <*https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf*>. Acesso em dez 2022.

1. **Identificação do Risco;**
2. **Classificação do Risco;**
3. **Avaliação do Risco (Risco Inerente, Controles Existentes, Risco Residual);**
4. **Gestão do Risco.**

Para facilitar, detalhou-se, abaixo, cada uma das quatro etapas ligadas à metodologia utilizada para a consolidação da **MATRIZ DE RISCOS**.

1. IDENTIFICAÇÃO DO RISCO

A primeira etapa consiste na análise profunda da estrutura e do funcionamento da organização e de qual legislação ela está subordinada, que proporciona o entendimento e aferição dos seus objetivos, missões valores.

A partir deste entendimento, é possível verificar que tipo de evento pode impactar negativamente no alcance de seus objetivos, missões e valores. Estes eventos são denominados **RISCOS** e estarão listados no CRA.

A finalidade da etapa de identificação de risco é gerar uma relação abrangente de riscos, baseada em eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos definidos pela organização.

A Identificação dos **RISCOS** é realizada, num primeiro momento, pela Consultoria **ALOÍSIO ZIMMER ADVOGADOS**, que apresenta uma relação preliminar à Alta Administração, a quem cabe aprovar, reprovar ou acrescentar os **RISCOS** listados pela Consultoria. E é a partir desta listagem que as demais etapas do CRA serão elaboradas.

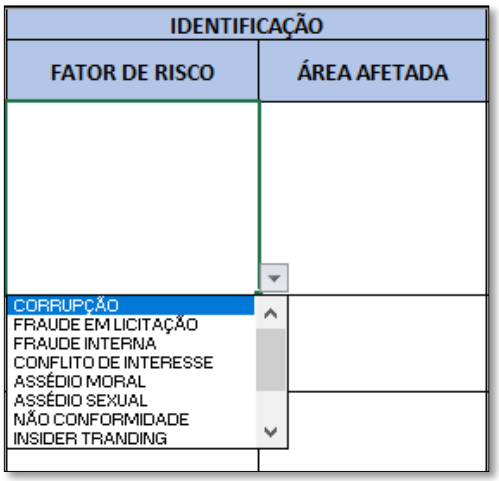
2. CLASSIFICAÇÃO DO RISCO

Identificado o risco, cumpre estabelecer as premissas que balizarão a análise da probabilidade e do impacto, a partir do ***i)*** fator de risco e da ***ii)*** área afetada.

O fator de risco é o tipo em que aquele risco está enquadrado. Na metodologia do Escritório **ALOÍSIO ZIMMER ADVOGADOS**, utilizamos o seguinte rol:

- **Corrupção;**

- **Fraude Interna;**
- **Conflito de Interesses;**
- **Assédio Moral;**
- **Assédio Sexual;**
- **Não Conformidade;**
- **Outros.**



3. AVALIAÇÃO DOS RISCOS

A etapa de avaliação dos riscos tem como intuito a promoção do entendimento do nível do risco na instituição, através de uma abordagem que permite a estimativa da **PROBABILIDADE** de ocorrência e do **IMPACTO** destes eventos identificados como risco nos objetivos dos processos organizacionais.

Aliás, cumpre referir que o **MINISTÉRIO DA INFRAESTRUTURA** utiliza a mesma abordagem em seu Manual de Gestão de Riscos:

> A avaliação do risco deve ser feita por meio de análise quantitativa e qualitativa ou da combinação de ambas e, ainda, quanto à sua condição de inerente (risco bruto, sem considerar qualquer controle) e residual (considerando os controles identificados e avaliados quanto ao desenho e à execução desse controle). Risco inerente é o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou de seu impacto. (Art. 2º, XIV, IN Conjunta MP/CGU Nº 01/2016). Risco residual: risco a que

uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco; (Art. 2º, XV, IN Conjunta MP/CGU Nº 01/2016).[13]

Inicialmente, é realizada a avaliação quanto ao **RISCO INERENTE**. Nesta etapa, é desconsiderado qualquer tipo de controle existente na organização para mitigá-lo ou evitá-lo, ou seja, é o **RISCO BRUTO**. É um risco que a empresa está naturalmente exposta por razão de sua atividade.

Um exemplo de risco inerente é o risco de algum diretor ou preposto da organização participar de um ato de corrupção ou praticar ato de improbidade administrativa. Neste caso, uma empresa que participa de disputas licitatórias, credenciamentos ou chamamentos públicos, naturalmente, corre este risco, em razão do envolvimento com agentes públicos. Aqui, não está considerada a existência de eventual Programa de Integridade, política de brindes e presentes etc.

Esta avaliação será feita com base na matriz *probabilidade x impacto*.

A **PROBABILIDADE** de o risco ocorrer será medida, utilizando-se dos seguintes critérios:

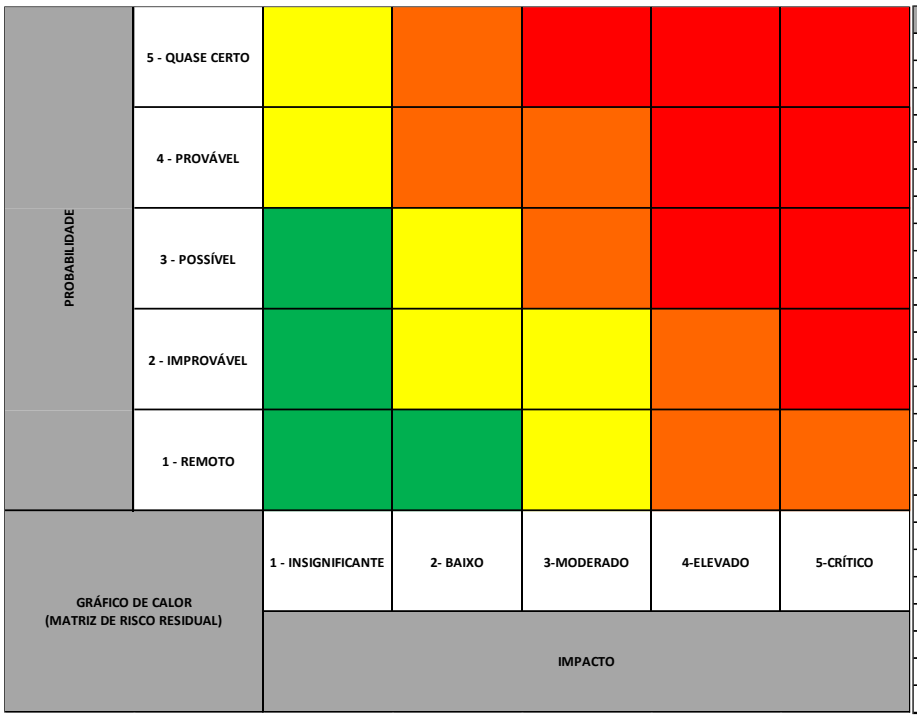
- **REMOTO: Peso 1 (ocorrência: menos de uma vez por ano);**
- **IMPROVÁVEL: Peso 2 (ocorrência: uma vez por ano);**
- **POSSÍVEL: Peso 3 (ocorrência: uma vez por semestre);**
- **PROVÁVEL: Peso 4 (ocorrência: uma vez por mês);**
- **QUASE CERTO: Peso 5 (ocorrência: uma vez por semana).**

Por sua vez, o **IMPACTO** que o risco pode causar na organização seguirá a seguinte classificação:

[13] BRASIL. MINISTÉRIO DA INFRAESTRUTURA. Comitê Estratégico de Governança. **Manual de Gestão de Riscos dos Processos de Trabalho**. Portaria MInfra n. 55/2021, art. 35, anexo II. Versão 1.0. 05/2021. Disponível em <*https://www.gov.br/infraestrutura/pt-br/assuntos/ManualGestao_de_Risco2021_Minfra_final.pdf*>. Acesso em dez 2022. p. 34.

- **INSIGNIFICANTE: Peso 1 (descrição: sem danos e prejuízos, perda financeira pequena ou indireta);**
- **BAIXO: Peso 2 (descrição: compromete somente o processo em questão, com impacto referente à eficiência do processo sob dimensão de custo e duração. Ex.: retrabalho, parada de sistemas não críticas, ausência de ferramentas adequadas);**
- **MODERADO: Peso 3 (descrição: requer tratamento, indica significativa perda financeira. Impacto relacionado à perda e/ou comprometimento de ativos não críticos e/ou descumprimento de leis ou regulamentações que não comprometem a imagem da empresa. Ex.: acesso inadequado a dados e/ou informações não críticas, pagamento de multas);**
- **ELEVADO: Peso 4 (descrição: grandes danos e prejuízos financeiros diretos, perda de capacidade de operação. Impacto relacionado à perda e/ou descumprimento);**
- **CRÍTICO: Peso 5 (descrição: eventos relevantes que comprometem fortemente o resultado da empresa e sua estratégia. Eventos deste tipo podem afetar o resultado da instituição de forma relevante).**

A partir da análise da **PROBABILIDADE** de o risco ocorrer e o **IMPACTO** que ele poderá causar, a **MATRIZ** se materializa no gráfico de calor abaixo:



NÍVEL DE RISCO
11-Risco Baixo
12-Risco Baixo
13-Risco Médio
14-Risco Alto
15-Risco Alto
21-Risco Baixo
22-Risco Baixo
23-Risco Médio
24-Risco Alto
25-Risco Elevado
31-Risco Baixo
32-Risco Médio
33-RiscoAlto
34-Risco Elevado
35-Risco Elevado
41-Risco Médio
42-Risco Alto
43-Risco Alto
44-Risco Elevado
45-Risco Elevado
51-Risco Médio
52-Risco Alto
53-Risco Elevado
54-Risco Elevado
55-Risco Elevado

LEGENDA:

 **VERDE**: **RISCO BAIXO;**

 **AMARELA: RISCO MÉDIO;**

 **LARANJA: RISCO ALTO;**

 **VERMELHA: RISCO ELEVADO.**

Analisado o risco inerente, passa-se a avaliar se a organização tem algum tipo de **CONTROLE** que busque eliminar, mitigar ou transferir o risco identificado.

Assim, identificado o controle (caso haja), será verificado se ele é **INEFICAZ, EXISTENTE, EFICAZ** ou **MUITO EFICAZ**.

O **RISCO RESIDUAL**, por fim, é o risco que decorre do risco inerente sobre o filtro do controle existente. Isto é, o risco inerente é o risco atual, o risco em que a empresa se encontra no momento da elaboração da análise de riscos.

Nesta etapa, novamente o risco será medido por meio da equação **PROBABILIDADE X IMPACTO**.

A **PROBABILIDADE** de o risco ocorrer e o **IMPACTO** que poderá causar na organização deverão ser analisados considerando os controles previamente existentes, na forma demonstrada abaixo:

AVALIAÇÃO DO RISCO INERENTE			AVALIAÇÃO DE CONTROLES		AVALIAÇÃO DO RISCO RESIDUAL		
PROBABILIDADE	IMPACTO	RISCO INERENTE	CONTROLES EXISTENTES	NÍVEL DE CONTROLE	PROBABILIDADE	IMPACTO	RISCO RESIDUAL

4. GESTÃO DE RISCOS

Os três processos anteriores (identificação, classificação e análise do risco) são importantes para situar como os riscos impactam ou podem impactar a organização, e se

ela já realiza alguma espécie de controle para mitigá-los. Como dito anteriormente, entender os riscos que uma instituição está exposta é entender a própria instituição.

A próxima etapa consiste na **GESTÃO** destes riscos. A **GESTÃO DE RISCOS** é uma decisão da diretoria da organização, a partir de seu apetite por riscos, isto é, o nível de exposição a riscos previamente estabelecido em cotejo à avaliação que se fez do risco.

Com base na metodologia da Norma **ISO 31000:2018 ABNT**, utiliza-se uma classificação de quatro ações possíveis para gerenciamento dos riscos, quais sejam:

ACEITAR, MITIGAR, TRANSFERIR e **ELIMINAR**

A **CONTROLADORIA-GERAL DA UNIÃO** entende como **ACEITAR** quando "*o nível está na faixa de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco*".[14]

Em complemento, entende-se, ainda, que **ACEITAR** o risco tem relação com o custo da ação. Por vezes, mitigar ou transferir o risco tem um custo elevado, fazendo com que a organização assuma a possibilidade daquele determinado risco ocorrer. Outra hipótese de **ACEITAR** se dá quando a empresa admite se expor aquele determinado risco por questões estratégicas, nas quais o risco é identificado e classificado, mas a organização deliberadamente aceita se expor a ele.

Já quanto a **MITIGAR**, entende-se que devem ser definidas medidas de tratamento para o risco indicado. Segundo a **CONTROLADORIA-GERAL DA UNIÃO**, *"essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco"*.[15]

Ou seja, quando a organização decide **MITIGAR** o risco, decide por empreender esforços para evitar a sua ocorrência.

Exemplificativamente, a empresa que decide mitigar o risco de "*alguém oferecer ou se utilizar de doações, contribuições ou patrocínios, com fins de obtenção de*

[14] BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). **Metodologia de Gestão de Riscos**. p. 24. Disponível em <*https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf*>. Acesso em dez 2022.

[15] BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). **Metodologia de Gestão de Riscos**. p. 24. Disponível em <*https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf*>. Acesso em dez 2022.

vantagens indevidas", poderá coibi-lo por meio da edição de uma política de doação, brindes e presentes que estabeleça as condutas vetadas pela empresa. Este tipo de medida busca evitar a ocorrência do risco, mas não de eliminá-lo completamente, na medida em que o colaborar poderá, deliberadamente, burlar as regras da instituição.

Quando se trata da ação **TRANSFERIR** [ou compartilhar], a **CONTROLADORIA-GERAL DA UNIÃO** entende que "*o risco possui probabilidade e impacto tão altos que a organização não pode suportar e decide transferi-los a outra entidade. Por exemplo, um órgão público decide contratar um seguro de acidentes para certos empregados que exercem atividades muito perigosas – ele transfere o seu risco de sinistro para uma outra entidade*".[16]

Uma instituição que tem como risco identificado o roubo de valores transportados fora das suas dependências pode **TRANSFERIR** o risco a uma empresa de carro-forte, por exemplo. Por outro lado, uma instituição em que as suas atividades poderão ocasionar acidentes aos seus trabalhadores ou a terceiros poderá contratar um seguro específico para esses eventos.

Em ambos os exemplos a instituição transferirá o risco para um terceiro que se responsabilizará por tratá-los.

Por fim, a **CONTROLADORIA-GERAL DA UNIÃO** entende que, no caso de **EVITAR**, como a implementação de controles apresenta um custo muito elevado e não se têm condições de compartilhá-lo, faz-se necessário "*alterar o processo visando a evitar a ocorrência do risco. Por exemplo, um órgão pode decidir evitar o oferecimento de determinado serviço por envolver riscos de alto impacto e probabilidade*".[17]

Nesta ação, a organização entende que é necessário encerrar algum tipo de atividade, a fim de **EVITAR** a ocorrência do risco, pois ele é muito alto ou extremo. No exemplo do risco "*oferecer ou se utilizar de doações, contribuições ou patrocínios, com fins de obtenção de vantagens indevidas*", a empresa poderá determinar que é vedado dar ou receber qualquer tipo de brinde, doação, patrocínio, no sentido de **EVITAR** a ocorrência

[16] BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). **Metodologia de Gestão de Riscos**. p. 24. Disponível em <*https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf*>. Acesso em dez 2022.

[17] BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). **Metodologia de Gestão de Riscos**. p. 24. Disponível em <*https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf*>. Acesso em dez 2022.

do risco de estes benefícios serem utilizados com intuito ilícito, como obter vantagens indevidas em processos licitatórios.

Ato contínuo, determinada a medida (**ACEITAR**, **MITIGAR**, **TRANSFERIR** ou **EVITAR**), será definida a **AÇÃO** que a organização tomará para tratar o risco conforme a medida estabelecida. Criação de políticas específicas, código de ética e de conduta, protocolos de *due diligences*, treinamentos dos colaboradores e melhorias no canal de denúncias são exemplos de ações possíveis no âmbito da gestão dos riscos.

Neste momento, é também definido o **RESPONSÁVEL** por implementar a ação dentro da instituição, bem como o **PRAZO** para a sua implementação. Esta análise deverá ser realizada de forma realista, de modo que o responsável seja capacitado a implementar aquela ação e o prazo seja suficiente para que a ação efetivamente seja efetivada dentro dos padrões esperados.

GESTÃO DOS RISCOS			
MEDIDA	**AÇÃO**	**RESPONSÁVEL**	**PRAZO**
ACEITAR TRANSFERIR MITIGAR ELIMINAR			

Apresentada a metodologia de trabalho, passa-se então à **ANÁLISE DE RISCOS** da **CISAL**.

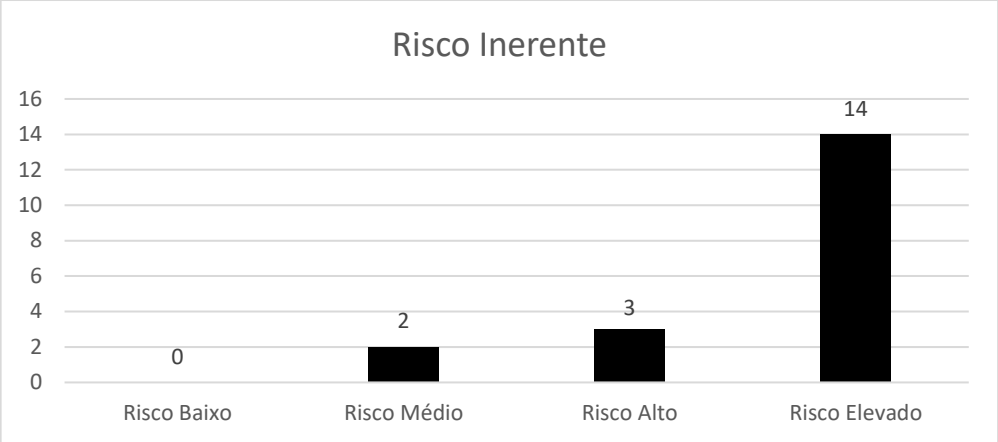
DADOS CONSOLIDADOS

Consolidamos alguns dados para efeitos de melhor avaliação global, conforme gráficos que seguem.

RISCO INERENTE

PROBABILIDADE	5 - QUASE CERTO				9	
	4 - PROVÁVEL			17, 18	6, 8, 10	
	3 - POSSÍVEL			1	4, 5, 7, 11, 12, 13, 14	15, 16, 19
	2 - IMPROVÁVEL			2, 3		
	1 - REMOTO					
GRÁFICO DE CALOR (MATRIZ DE RISCO INERENTE)		1 - INSIGNIFICANTE	2- BAIXO	3-MODERADO	4-ELEVADO	5-CRÍTICO
		IMPACTO				

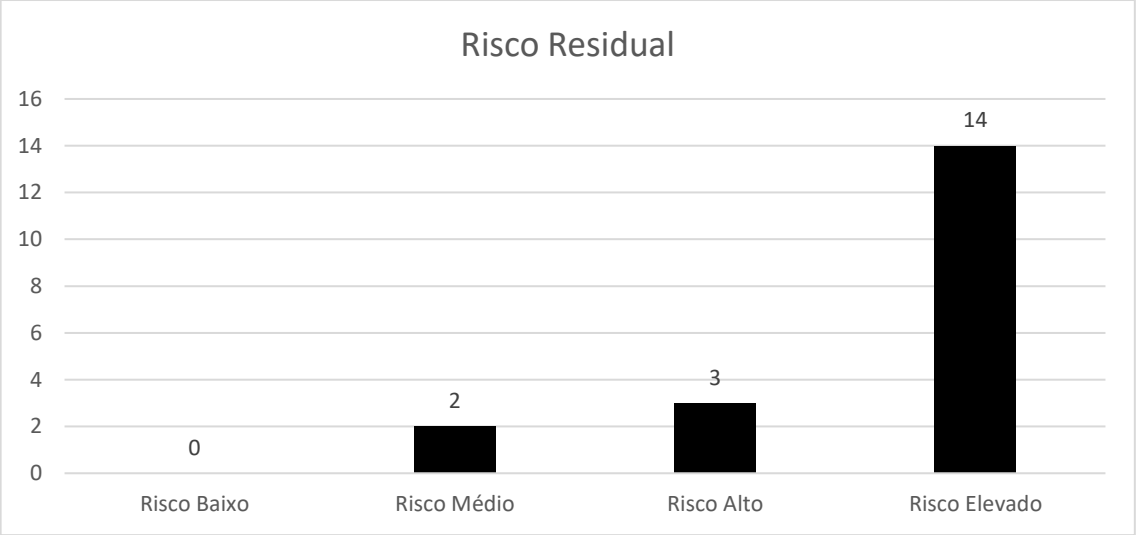
RISCO INERENTE



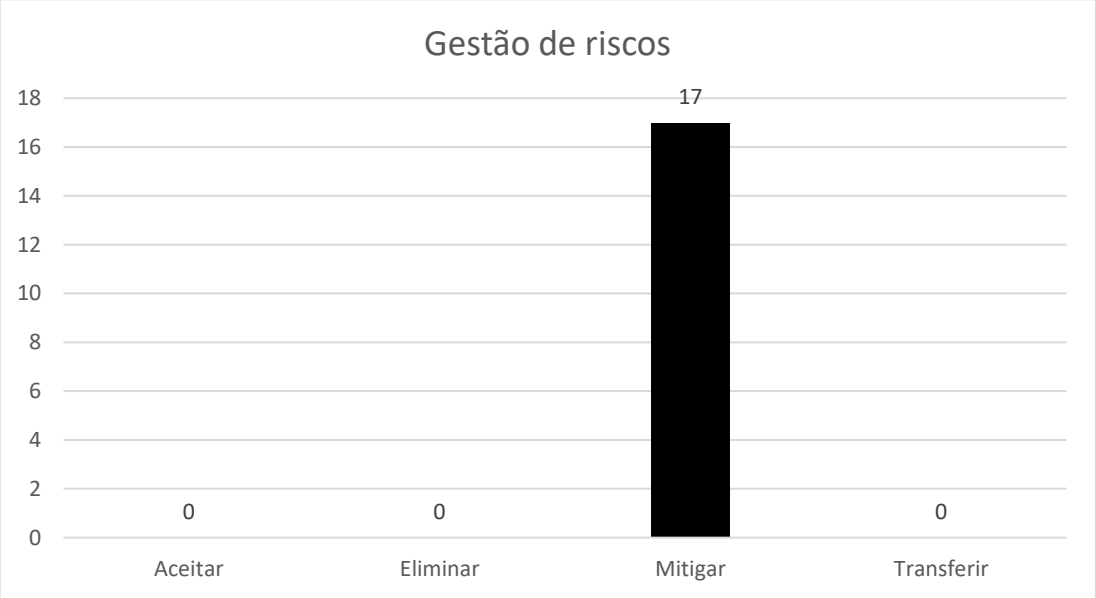
RISCO RESIDUAL

PROBABILIDADE	5 - QUASE CERTO				9	
	4 - PROVÁVEL			17, 18	6, 8, 10	
	3 - POSSÍVEL			1	4, 5, 7, 11, 12, 13, 14	15, 16, 19
	2 - IMPROVÁVEL		3	2		
	1 - REMOTO					
GRÁFICO DE CALOR (MATRIZ DE RISCO RESIDUAL)		1 - INSIGNIFICANTE	2- BAIXO	3-MODERADO	4-ELEVADO	5-CRÍTICO
		IMPACTO				

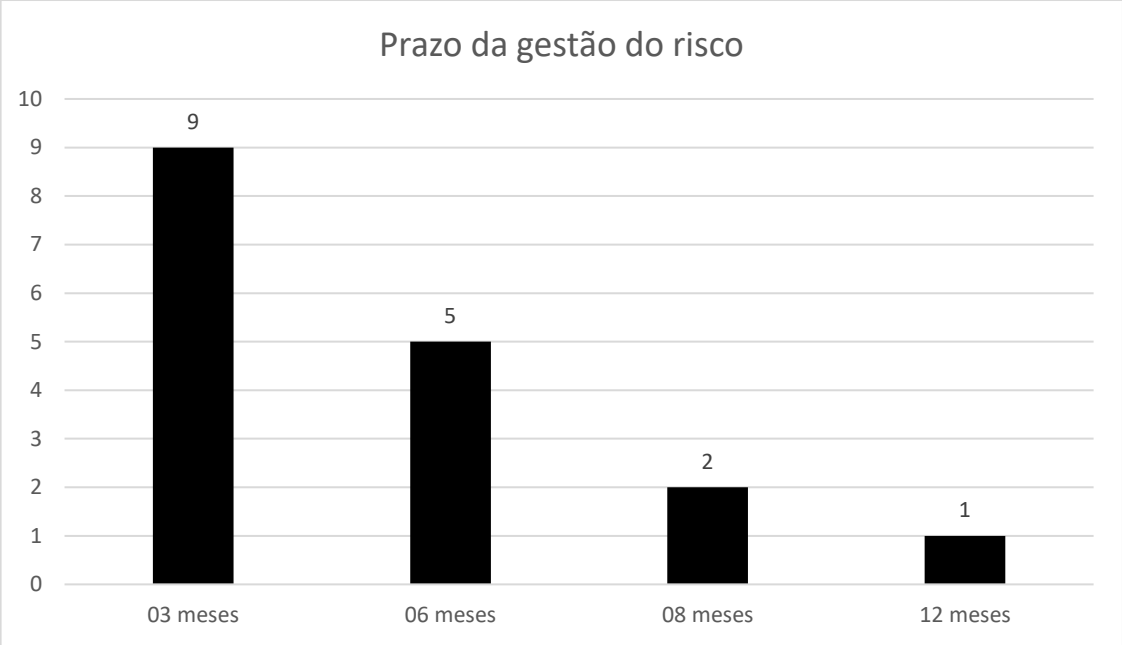
RISCO RESIDUAL



GESTÃO DE RISCOS



PRAZO DA GESTÃO DE RISCO



CONCLUSÕES

Diante do trabalho da Consultoria **ALOÍSIO ZIMMER ADVOGADOS** para desenvolvimento do **COMPLIANCE RISK ASSESSMENT** da **CISAL CONSTRUÇÕES LTDA**, apresentam-se as seguintes **CONCLUSÕES**:

- Foram identificados **19** (dezenove) **RISCOS**;
- **RISCO INERENTE**: nenhuma ocorrência de **RISCO BAIXO**; 02 (duas) ocorrências de **RISCO MÉDIO**; 3 (três) ocorrências de **RISCO ALTO**; e 14 (catorze) ocorrências de **RISCO ELEVADO**;
- Dos 19 (dezenove) riscos identificados, 18 (dezoito) tinham controles existentes, sendo este **EFICAZ**;
- **RISCO RESIDUAL**: nenhuma ocorrência de **RISCO BAIXO**; 2 (duas) ocorrências de **RISCO MÉDIO**; 3 (três) ocorrências de **RISCO ALTO**; e 14 (catorze) ocorrências de **RISCO ELEVADO**;
- **GESTÃO DE RISCOS**: 17 (dezessete) ocorrências de **MITIGAR**; 2 (duas) ocorrências de **ACEITAR**; e nenhuma ocorrência de **TRANSFERIR** e **ELIMINAR**;
- Das ações propostas para mitigação dos riscos, repetiram-se a **CRIAÇÃO DE CÓDIGO DE ÉTICA E TREINAMENTO DOS COLABORADORES** (10 vezes) e **CRIAÇÃO DE POLÍTICAS SETORIAIS** (03 vezes);
- Dos **PRAZOS** estabelecidos para a gestão dos riscos: 09 (nove) serão revisados em **03 MESES**; 05 (cinco) serão revisados em

06 MESES; 02 (dois) serão revisados em **08 MESES**; e 01 (um) será revisado em **12 MESES**;

Desse modo, a Consultoria **ALOÍSIO ZIMMER ADVOGADOS** se compromete a acompanhar o bom andamento das ações propostas e dar encaminhamento naquelas ações cuja responsabilidade lhe foi designada.

Tendo em vista que o presente **COMPLIANCE RISK ASSESSMENT** foi encerrado em janeiro de 2024, o início da revisão do presente material deverá ser definido pelo Compliance Officer em acordo com a Alta Administração, conforme modelos detalhados ao longo deste Relatório.

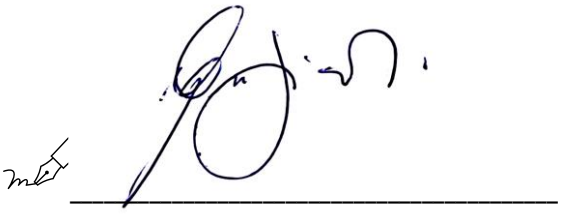
ANÁLISE DE RISCOS CONCLUÍDA EM: 15/01/2024

MENSAGEM FINAL DA CONSULTORIA: Empenhados em colaborar com a Diretoria da **CISAL CONSTRUÇÕES LTDA** na implementação de controles de integridade e com o objetivo de contribuir para a boa governança da organização, nossa equipe, na pessoa do Dr. **Aloísio Zimmer**, tem a honra de concluir este trabalho, agradecendo a confiança, na certeza de que o desafio se tornou mais fácil com a colaboração de toda a Alta Administração da instituição. Nossas homenagens à visão de futuro da CISAL e ao interesse em fazer do Compliance uma prática diária.

Porto Alegre/RS, 15 de janeiro de 2024.

ALOÍSIO ZIMMER JÚNIOR
Consultor em Compliance
OAB/RS 42.306

APROVAÇÃO FINAL



CLAUDIO CARDOSO DA SILVA
SÓCIO-ADMINISTRADOR