AVALIAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS NA SABESP

Márcio Savoia Coelho[(1)]
Engenheiro Eletricista pela Escola Politécnica da Universidade de São Paulo – USP. Pós-Graduado em Administração de Produção pela Fundação Carlos Alberto Vanzolini. Pós-Graduado em Engenharia de Saneamento Básico pela Faculdade de Saúde Pública da Universidade de São Paulo – USP. Certificado em Formação Executiva em GRC ("Governance, Risk e Compliance") pela Risk University – KPMG. Engenheiro do Departamento de Riscos Corporativos e de Negócios da SABESP.
Luciano Sousa Diaz[(2)]
Bacharel em Matemática. Pós-Graduado em Administração de Empresas pela FAAP – Fundação Armando Álvares Penteado – SP. Coordenador Adjunto da Câmara Temática de Governança Corporativa e Jurídica da ABES-Nacional. Membro da Comissão de Estudo Especiais de Gestão de Riscos da ABNT. Atua na Sabesp desde 1986, com experiências em Auditoria Interna, Compliance e Segurança Empresarial. Atualmente é o Gerente do Departamento de Gestão de Riscos Corporativos e de Negócios da SABESP.

Endereço[(1)]**:** Rua Costa Carvalho, 300 - São Paulo - SP - CEP: 05429-900 - Brasil - Tel: +55 (11) 3388-8832 - e-mail: msavcoelho@gmail.com

RESUMO

A Companhia de Saneamento Básico do Estado de São Paulo (SABESP) possui um processo estruturado de gestão de riscos fundamentado na aplicação do framework COSO ERM "Committee of Sponsoring Organization of the Treadway Commission - Enterprise Risk Management Framework 2017" e a na norma ABNT NBR ISO 31000:2018. Em 2022, com o objetivo de avaliar o nível de desenvolvimento do trabalho existente em relação aos melhores referenciais de mercado e obter insumos para o seu aperfeiçoamento, a administração encomendou a contratação de uma consultoria para avaliação do seu atual grau de maturidade. Neste trabalho, será apresentado uma síntese do relatório de conclusão da empresa contratada para esta finalidade e das ações em andamento para aprimoramento das práticas existentes.

PALAVRAS-CHAVE: Gestão de Riscos, Maturidade, Avaliação.

1. INTRODUÇÃO

Os riscos são inerentes a qualquer uma das atividades humanas e num contexto de organização com finalidade pública, mais do que nunca envolve riscos decorrentes da natureza de suas atividades, de realidades emergentes, de mudanças nas circunstâncias e nas demandas sociais, da própria dinâmica da administração. Com isso, as ações de governança e de gestão das organizações públicas devem buscar, de maneira integrada, entregar mais valor para a população. Dentre as principais exigências corporativas e legais, há a necessidade da transparência e prestação de contas, no sentido do cumprimento dos requisitos legais e regulatórios.

Desta forma, gerenciar riscos por meio da aplicação das melhores práticas de mercado aplicadas de forma sistemática, estruturada e focada nos riscos mais críticos, em alinhamento com as normas específicas vigentes, passa a ser essencial para a melhoria da eficiência operacional da Administração Pública. A gestão de riscos baseada nas etapas de identificação, análise, avaliação e tratamento dos riscos priorizados, deve ser realizada não apenas para evitar prejuízos ou cumprir exigências legais. Os gestores públicos precisam focar esta gestão como a chave para gerar mais valor à sociedade, entregando serviços mais eficientes, permitindo aos órgãos públicos atingir seus objetivos estratégicos de maneira sustentável. Além disso, ao gerenciar riscos de modo eficaz, os gestores passam a ter melhores informações para a tomada de decisão mais tempestiva, contribuindo assim não só na prevenção de perdas e gerenciamento de incidentes, mas também no aumento da confiança dos cidadãos nas organizações públicas.

2. A GESTÃO DE RISCOS NA SABESP

A SABESP possui uma Superintendência de Gestão de Riscos e Conformidade (PK), que é a autoridade funcional em conformidade e gestão de riscos e está subordinada hierarquicamente ao Diretor Presidente, atuando de maneira integrada às outras áreas da Companhia e à Comissão de Gestão de Riscos Corporativos.

A estrutura da Superintendência e sua relação com o restante da estrutura de Governança está demonstrada na figura 1 a seguir:

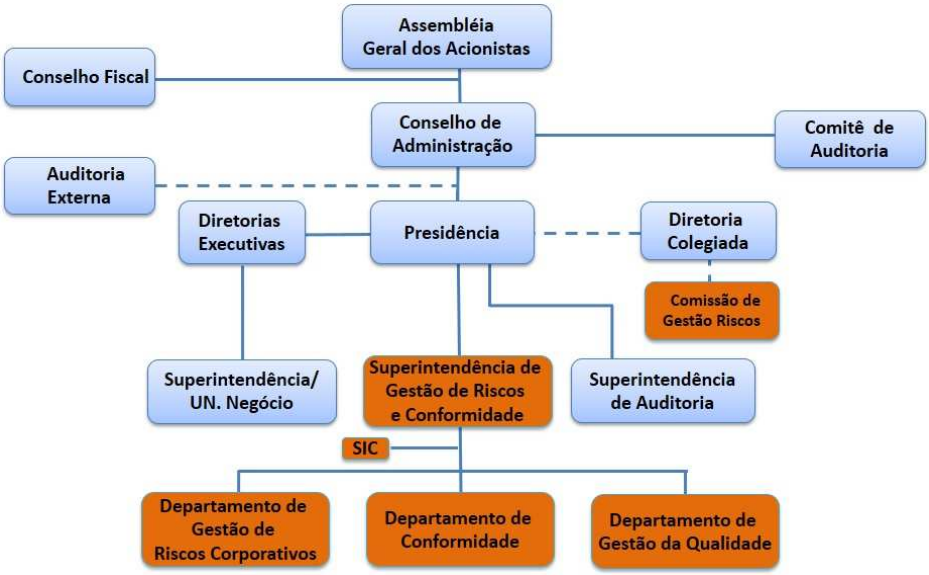

Figura 1 – Estrutura de Governança da SABESP

A SABESP adota como processo de gestão de riscos, o modelo internacional COSO ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework 2017 e as normas ABNT NBR ISO 31000:2018 e ABNT ISO GUIA 73, com enfoque nos negócios empresariais, proporcionando auxiliar a empresa para atingir seus objetivos de negócios estratégicos.

A empresa possui uma Política Institucional de Gestão de Riscos Corporativos alinhada com o modelo recomendado pelo Instituto de Auditores Internos do Brasil (IIA Brasil), conhecida como "As Três Linhas de Defesa", publicado em janeiro de 2013. Esse modelo é adotado por várias instituições como referência na estratégia para implantação de um sistema de gerenciamento de riscos e controles internos. A seguir, um breve relato sobre o modelo:

- 1ª Linha de Defesa é a área de negócio, responsável por identificar, mensurar, avaliar e mitigar os riscos. Cada unidade de negócio tem riscos operacionais inerentes e é responsável por manter controles internos eficientes e implementar ações corretivas para resolver deficiências em processos e controles.
- 2ª Linha de Defesa inclui funções de gerenciamento de risco e conformidade, deve trabalhar em conjunto com a área de negócios para garantir que a 1º linha de defesa tenha identificado, avaliado e reportado corretamente os riscos.
- 3º Linha de Defesa é representada pela Auditoria Interna, que deve revisar de modo sistemático e eficiente às atividades das duas primeiras linhas de defesa e contribuir para seu aprimoramento.

O processo de gestão de riscos adotado pela SABESP está descrito em um procedimento empresarial interno e em linhas gerais passa por 4 (quatro) etapas principais:

- Identificação de riscos;
- Análise de riscos;
- Avaliação e Tratamento;
- Comunicação e Monitoramento.

A Companhia mantém um mapa de riscos corporativos e acompanha as tendências globais e nacionais a fim de antever cenários que possam afetar adversamente suas operações, garantindo, desta forma, o cumprimento dos seus objetivos estratégicos e consequentemente a sustentabilidade da empresa. O tratamento dos riscos se dá em função da sua natureza, que pode ser estratégica, financeira, operacional e de conformidade; já a sua mensuração é feita considerando-se o impacto e probabilidade de ocorrência.

Os riscos dos processos devem ser identificados, analisados, avaliados, comunicados, tratados e monitorados como oportunidade de melhoria.

O mapa de riscos corporativos da Sabesp está estruturado de forma matricial, com a escala de Impacto em um dos eixos e a Probabilidade no outro. O impacto dos riscos é calculado através do valor financeiro (vetor principal) e conforme o caso, também por vetores auxiliares específicos: Conformidade, Operação, Imagem, Qualidade de Água Tratada, Segurança e Saúde e Meio Ambiente.

O nível de criticidade do risco corporativo é a combinação das réguas de impacto e probabilidade. O nível de criticidade do risco é representado pela associação do impacto e a probabilidade de ocorrência do evento (impacto x probabilidade).

O posicionamento dos riscos no mapa estratégico, vincula aos níveis hierárquicos competentes, os quais serão responsáveis pelas ações mitigatórias exigidas por cada situação. Todos os riscos corporativos são revisitados periodicamente, objetivando a implementação de ações mitigadoras suplementares, caso haja necessidade.

Como aprimoramento recente no processo de gestão de riscos, a SABESP implantou em 2019 o módulo da SAP GRC RM - Risk Management e o PC - Process Control, uma solução integrada que unifica a gestão de riscos e controles, permitindo uma visão holística e eficiente dos riscos aos quais a companhia está exposta.

A descrição dos principais fatores de riscos, pode ser encontrada no item 4 do Formulário de Referência, disponível no site de Relações com Investidores da Companhia, na seção “Informações Financeiras e Operacionais”.

3. OBJETIVO

Este trabalho tem como principal objetivo, apresentar resumidamente o diagnóstico elaborado pela consultoria especializada (Voyager IT Quality Assurance), que resultou no grau de maturidade do processo de Gestão de Riscos Corporativos da SABESP, com a identificação de aspectos que necessitam ser aperfeiçoados.

As principais questões que direcionaram a contratação estão pontuadas abaixo e serão discutidas na sequência deste trabalho:

- Em que medida as políticas e estratégias de gestão de riscos definidas estão sendo comunicadas e postas em prática na SABESP?
- Qual o nível de maturidade de gestão de riscos da SABESP em relação às empresas do mercado?

4. METODOLOGIA

4.1 Modelo de avaliação utilizado

A Contratada aplicou método baseado no Modelo de Avaliação de Maturidade proposto pelo Tribunal de Contas da União (TCU), que por sua vez foi desenvolvido a partir das melhores práticas internacionais em uso no setor público, oriundas dos modelos de gerenciamento de riscos COSO GRC (COSO, 2004 e 2017), ABNT NBR ISO 31000 Gestão de Riscos – Princípios e Diretrizes (ABNT, 2018), bem como da IN-MP/CGU Nº 1/2016.

O modelo do TCU é composto pelas quatro dimensões descritas abaixo:

a) Ambiente: esta dimensão, busca avaliar as capacidades existentes na organização em termos de liderança, políticas, estratégias e de preparo das pessoas, incluindo aspectos relacionados com cultura, a governança de riscos e a consideração do risco na definição da estratégia e dos objetivos em todos os níveis, para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento da missão institucional na geração de valor para as partes interessadas. Nesta dimensão há 3 (três) seções:

- Liderança: Nesta seção, busca-se avaliar em que medida os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos e cultura, assumindo um compromisso forte e sustentado e exercendo supervisão para obter comprometimento com a gestão de riscos em todos os níveis da organização, promovendo-a e dando suporte, de modo que possam ter uma expectativa razoável de que no cumprimento da sua missão institucional. Avalia-se ainda se a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir os seus objetivos de agregar, preservar e entregar valor às partes interessadas, tendo o cidadão e a sociedade como vetores principais.
- Política e Estratégica: nesta seção, buscou-se avaliar em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.
- Pessoas: nesta seção, buscou-se avaliar em que medida as pessoas na organização estão informadas, habilitadas e autorizadas para exercer seus papéis e suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.

b) Processos: nesta dimensão, são examinados os processos de gestão de riscos adotados pela gestão, procurando avaliar em que medida a organização dispõe de um modelo de processo formal, com padrões e critérios definidos para a identificação, a análise e a avaliação de riscos; para a seleção e a implementação de respostas aos riscos avaliados; para o monitoramento de riscos e controles; e para a comunicação sobre riscos com partes interessadas, internas e externas. Nesta dimensão há 3 (três) seções:

- Identificação e Análise de Riscos: Nesta seção, busca-se avaliar em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente às operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização), de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos.
- Avaliação e Resposta a Riscos: Nesta seção, busca-se avaliar em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento.
- Monitoramento e Tratamento: Nesta seção, busca-se avaliar em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes no desenho e na operação.

c) Parcerias: esta dimensão, examina os aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas (quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas), procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento. Nesta dimensão há 2 (duas) seções:

- Gestão de Riscos e Parcerias: nesta seção, busca-se avaliar em que medida a organização adota um conjunto de práticas essenciais de gestão de riscos para ter segurança razoável de que os riscos no âmbito das parcerias serão adequadamente gerenciados e os objetivos alcançados.
- Planos e Medidas de Contingência: nesta seção, busca-se avaliar em que medida a organização estabelece, em conjunto com as entidades parceiras, planos e medidas de contingência para garantir a recuperação e a continuidade da prestação de serviços em caso incidentes.

d) Resultados: nesta dimensão, examinam-se os efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos. Nesta dimensão há 2 (três) seções:

- Planos e Medidas de Contingência: nesta seção, busca-se avaliar em que medida a organização integra a gestão de riscos em seus processos de governança e gestão e isso tem sido eficaz para a sua melhoria.
- Resultados-Chave da Gestão de Risco: nesta seção, busca-se avaliar em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.

Dentro desta realidade, o trabalho envolveu a análise e avaliação de toda a arquitetura da gestão de riscos corporativos da SABESP, englobando os princípios, a estrutura, os componentes e os processos definidos. Foram avaliadas as ações desenvolvidas para o gerenciamento de riscos por toda a organização, nos diversos níveis e nos contextos internos e externos. Além do processo de planejamento estratégico e sua implementação pelas diversas áreas ou funções da organização, os processos de governança, finalísticos e de apoio ou os programas, projetos e atividades relevantes para os objetivos chaves da organização relacionados a gestão dos riscos.

4.2 Escopo de avaliação

Em termos de escopo de avaliação, conforme termo de referência da contratação, foram considerados os seguintes aspectos direcionadores dos trabalhos avaliados sempre numa visão global do modelo de avaliação proposto pela SABESP. Estes direcionadores foram agrupados dentro das 4 dimensões do modelo do TCU, conforme apresentado na tabela 1 abaixo:
a) Análise do vínculo entre a Estratégia e o Risco;
b) Governança em Gestão de Riscos;
c) Cultura de Riscos;
d) Avaliação e Tratamento do Risco;
e) Gestão e Acompanhamento de Risco;
f) Relatórios e Análises de Dados; e
g) Dados e Tecnologia.

Dimensão	Aspecto Direcionador	Fatores Associados
Ambiente	Análise do vínculo entre a Estratégia e o Risco	Integração da Gestão de Riscos ao Processo de Planejamento
		Consideração dos riscos como critérios para avaliação de investimentos
		Contribuição da gestão de riscos no alcance dos objetivos estratégicos e no auxílio na tomada de decisão
		Relação entre alçada de riscos definido pela Companhia e as principais decisões adotadas
		Avaliação da adequação dos níveis de impacto e probabilidade atualmente utilizados
	Cultura de Riscos	Grau de entendimento e participação da Companhia no processo e na disseminação das informações de gestão de riscos
		Percepção de cultura de riscos praticada na Companhia, graduando os resultados obtidos;
		Programa de treinamento de Gestão de Riscos aos membros de Conselho, Comitês, Diretorias e Comissão de Gestão de Riscos;
		Existência / alcance do plano de treinamento e atualização institucional para os colaboradores sobre o tema gestão de riscos
		Plano de educação continuada para a equipe de gestão de riscos;
		Avaliação periódica de desempenho e revisão do processo de gestão de riscos
		Metas/indicadores de desempenho relacionados ao gerenciamento de

		riscos.
Parcerias	Governança em Gestão de Riscos	Patrocínio e supervisão da alta administração
		Foco de atuação da função de gestão de riscos
		Nível de comprometimento, responsabilidade e supervisão da gestão de riscos
		Atuação e nível de reporte da área de gestão de riscos
		Avaliação dos documentos normativos do processo de gestão de riscos (política e procedimentos empresariais);
		Grau de autonomia/independência da área de gestão de riscos
		Envolvimento das áreas de auditoria interna e de conformidade no processo de gestão de riscos
		Avaliação da suficiência de recursos e apropriados (pessoas, estruturas, sistemas de TI, programas de treinamento, métodos e ferramentas para gerenciar riscos) para a gestão de riscos
Processos	Avaliação e Tratamento do Risco	Conexão entre a área de gestão de riscos e o canal de denúncia para eventos de riscos
		Avaliação do retorno sobre investimento no processo de gestão de riscos
		Avaliação da qualidade da mensuração dos riscos
		Frequência de revisão do mapa de riscos corporativos e operacionais;
		Nível de abrangência e adequação das ações propostas no tratamento dos riscos
		Integração do processo de gestão de riscos e o sistema de avaliação de performance do negócio
	Dados e Tecnologia	Base de dados de eventos de risco armazenados de forma padronizada
		Existência de uma governança definida sobre acesso base de dados de eventos de risco
		Base de dados de eventos de risco ligadas diretamente a tomadas de decisões estratégicas
		Ferramenta suporte p/ o proc.de gestão de riscos
Resultados	Gestão e Acompanhamento de Risco.	Avaliação periódica do processo de gestão de riscos em relação ao desempenho/ objetivo / papéis e responsabilidades
		Existência de key risk indicators - KRI´s (Indicadores de Risco) adequados para monitorar a exposição dos riscos corporativos;
		Alçadas de escalonamento dos KRI's definidas
	Relatórios e Análises de Dados	Mensuração financeira dos impactos de ocorrências associadas a gestão de riscos
		Suficiência no conteúdo dos reportes aos diferentes níveis de alçada
		Frequência de reporte dos riscos corporativos ao Conselho de Administração
		Participação na elaboração dos relatórios financeiros divulgados ao mercado
		Análise por parte da área de gestão de riscos dos registros recebidos pelo canal de denúncia /ouvidoria

Tabela 1 - Dimensões e aspectos direcionadores do escopo do trabalho

4.3 Método para o diagnóstico

A etapa de diagnóstico da situação atual do processo de Gestão de Riscos Corporativos da SABESP foi composta de duas atividades principais, que foram: a análise documental e reuniões de levantamento de dados (entrevistas com amostra de superintendentes / gerentes de áreas corporativas e operacionais).

Na atividade de avaliação documental, a partir de uma seleção prévia de amostra de áreas relevantes da empresa, foram avaliados: estatuto, políticas institucionais, procedimentos e documentos dos processos de: Gestão de Riscos,

Conformidade, Auditoria Interna, Planejamento Estratégico, Empreendimentos, Gestão Patrimonial, Contabilidade, Jurídico, Comercial / Relações com Clientes e Operação (água e esgoto).

Nas reuniões de levantamento de dados, foram feitas 16 entrevistas com superintendentes, gerentes e profissionais chave dos processos citados acima visando complementar as informações e obter evidências das práticas existentes.

4.4 Critérios de avaliação

Na atividade de Avaliação Documental, foram utilizados os seguintes critérios de avaliação:

- Formalização: foco na existência e publicação do documento pela autoridade competente em pelo menos um canal corporativo (intranet, portal etc.)
- Padronização: foco na forma de elaboração do documento de acordo com as melhores práticas existentes considerando os tópicos obrigatórios (templates, modelos etc.);
- Conteúdo: foco no valor das informações descritas em cada tópico do documento.

Na atividade de levantamento da situação atual da Gestão de Riscos Corporativos da SABESP, cada aspecto direcionador informado na tabela 1, foi avaliado conforme os seguintes critérios de avaliação do modelo referencial do TCU:

- Inexistente – Nível 0: Não há evidências do resultado descrito. Prática inexistente, não implementada ou não funcional;
- Inicial – Nível 1: Existe a percepção entre os gestores e o pessoal de que o resultado descrito tenha sido obtido em alguma medida. Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização;
- Básico – Nível 2: Existem indicadores definidos que mostram que o resultado descrito vem sendo obtido em grau baixo. Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização;
- Aprimorado – Nível 3: Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau moderado;
- Avançado – Nível 4: Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau elevado. Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.

Estes níveis estão diretamente relacionados a pontuação obtida em termos do percentual de conformidade das avaliações que é representado pela nota dentro dos seguintes intervalos:

- De 0,0 a 0,15 - Inexistente (0%)
- De 0,16 a 1,0 - Inicial (1% a 25%)
- De 1,10 a 2,0 - Básico (26% a 50%)
- De 2,10 a 3,0 - Aprimorado (51% a 75%)
- De 3,10 a 4,0 - Avançado (76% a 100%)

4.5 Critérios para o benchmarking

Desde 2007, o TCU vem realizando trabalhos para levantar informações sobre a situação da governança na administração pública, e estimular as suas organizações jurisdicionadas a adotarem as boas práticas no tema. A partir de 2017, o TCU passou a reunir, em um único estudo, temas que em anos anteriores foram analisados separadamente – tecnologia da informação, pessoas, contratações e governança pública.

Nesse contexto, surgiu o Índice Integrado de Governança e Gestão (iGG), que constitui o mais amplo diagnóstico sobre a governança pública no País, abrangendo empresas estatais, sociedades de economia mista, autarquias, ministérios, tribunais, fundações, entre outros, num total de quase 500 órgãos e entidades da Administração Pública Federal.

O iGG é composto por outros 4 (quatro) índices, que representam na verdade as dimensões avaliadas no modelo:

- Governança Pública (iGovPub);
- Gestão de Pessoas (iGovPessoas);

- Gestão de TI (iGovTI) e
- Gestão de Contratações (iGovContrat).

Dentro da dimensão Governança Pública, o iGG avalia mecanismos e práticas conforme a figura abaixo:

Figura 2 - Práticas relacionadas aos mecanismos de governança

Em termos do mecanismo Estratégia, temos cinco práticas, onde a primeira delas é a que foi utilizada para a avaliação de benchmarking com as demais organizações avaliadas pelo TCU por meio do iGG:
a) Gerir riscos (2110);
b) Estabelecer a estratégia (2120);
c) Promover a gestão estratégica (2130);
d) Monitorar os resultados organizacionais (2140) e
e) Monitorar o desempenho das funções de gestão (2150).

A prática Gerir Riscos (2110) considera 5 itens relevantes na sua avaliação, que são:

- 2111 - A estrutura da gestão de riscos está definida;
- 2112 - Atividades típicas de segunda linha estão estabelecidas;
- 2113 - O processo de gestão de riscos da organização está implantado;
- 2114 - Os riscos considerados críticos para a organização são geridos;
- 2115 - A organização executa processo de gestão de continuidade do negócio.

5. RESULTADOS OBTIDOS

5.1 Resultados Gerais

Em 2021, foram 378 organizações públicas que participaram do levantamento considerando respostas válidas. Em termos gerais, como pode ser observado na figura 3, comparando-se os anos de 2018 e 2021, percebe-se uma sensível melhora na prática "Gerir Riscos" no estágio inicial. Em 2021 o índice foi de 85%, em comparação com os 51% em

2018, mesmo considerando o conjunto maior de itens de controle utilizados para avaliar essa prática no questionário aplicado em 2021.

Esta evolução pode ter sido resultado, dentre outros fatores, dos novos requisitos normativos e esforços orientativos e normativos relacionados ao tema Estratégia na Administração Pública Federal. Dentre estas iniciativas, destacam-se o Decreto 9.203/2017 e a Lei das Estatais (Lei 13.303/2016), que abordam diversos aspectos de Governança ligadas diretamente a esta prática de Gestão de Riscos que passaram a exigir das organizações públicas da administração federal direta e indireta uma maior atenção. Além dessas, foram publicados manuais no repositório de conhecimento da CGU sobre gestão de riscos e integridade (PORTAL CGU).

No entanto, a melhoria, não representa na verdade o cenário satisfatório, pois de modo geral, ainda há mais da metade das organizações declarando "não adotar" ou "adotar em menor parte" (Figura 4, coluna 2110) esta prática amplamente aceita e já pacificado o entendimento que é um dos pilares para uma boa governança, inclusive já normatizada no Brasil.

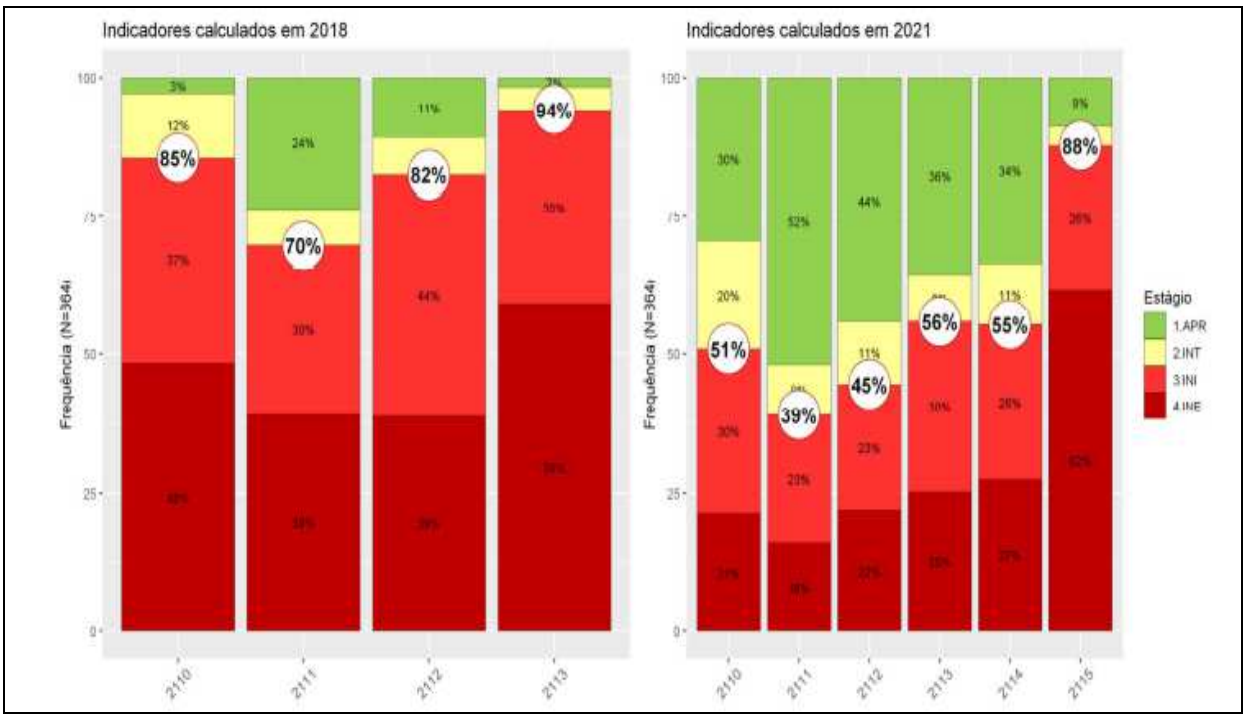

Figura 3 - Resultado comparativo do iGG de 2018 e 2021

Destaca-se também o resultado negativo de 88% das organizações ainda no estágio inicial da implementação do processo de Gestão de Continuidade do Negócio (GCN), item 2115. Este processo está diretamente ligado a Gestão de Riscos, pois dentro das 5 (cinco) etapas de implementação de um Sistema de Gestão de Continuidade de Negócios, definido na norma ABNT NBR 22.301:2013, a Gestão de Risco se faz presente em todas elas.

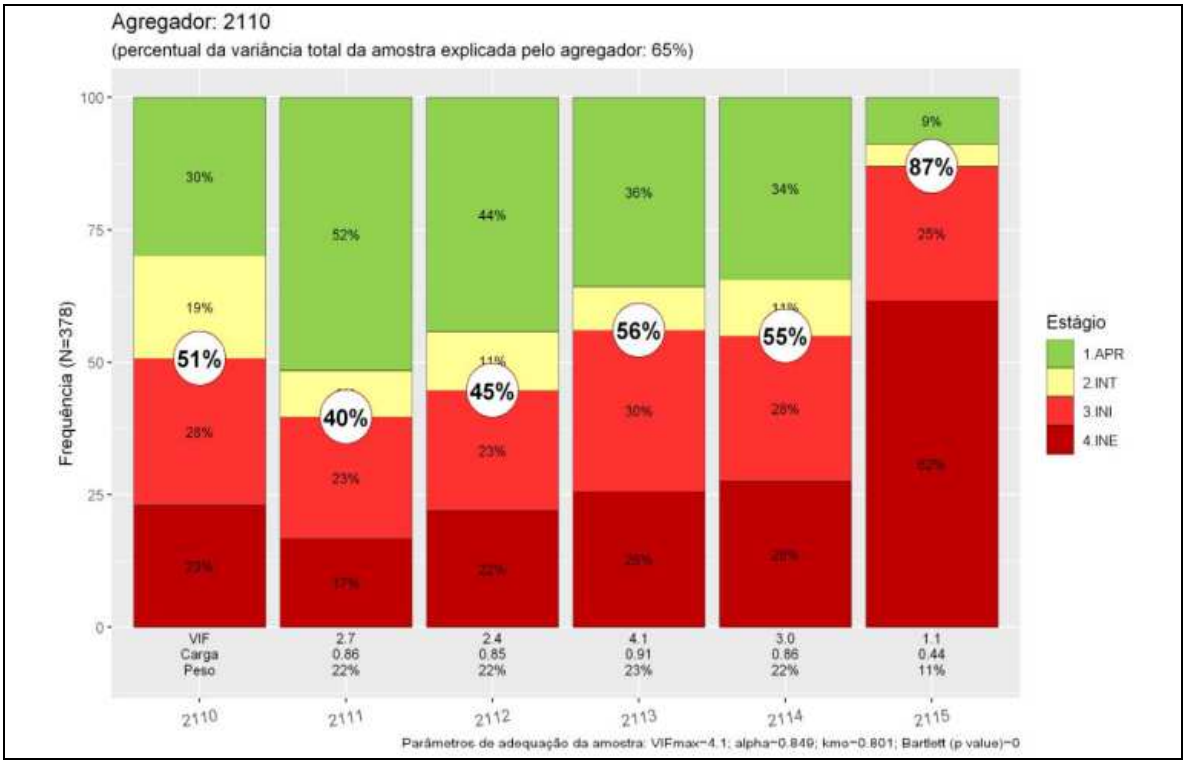

Figura 4 - Resultados gerais do iGG na prática Gerir Riscos

5.2 Resultados da Sabesp

Na tabela 2, é apresentada a consolidação das avaliações feitas em cada uma das dimensões relacionadas ao processo de Gestão de Riscos Corporativos da Sabesp, descritas no item 4.2 – Escopo (tabela 1), considerando todas as análises realizadas (documentais, entrevistas e observações in loco). Vale destacar, que para aumentar a aderência da avaliação aos princípios definidos na ABNT/NBR 31.000:2018, foi definido peso 2 para os aspectos direcionadores relacionados diretamente às etapas de identificação, análise, tratamento e monitoramento do risco.

Dimensões	Nota Inicial	Peso	Nota Final	Maturidade
Análise do vínculo entre a Estratégia e o Risco	2,80	1	2,80	**Aprimorado**
Governança em Gestão de Riscos	3,50	2	7,00	**Avançado**
Cultura de Riscos	2,86	1	2,86	**Aprimorado**
Avaliação e Tratamento do Risco	3,17	2	6,33	**Avançado**
Gestão e Acompanhamento de Risco	3,67	2	7,33	**Avançado**
Relatórios e Análises de Dados	3,20	1	3,20	**Avançado**
Dados e Tecnologia	3,75	1	3,75	**Avançado**
Geral	3,28	10	33,27	
			3,33	**Avançado**

Tabela 2 - Resultado consolidado da avaliação de maturidade da Sabesp.

6. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Considerando a métrica, as ponderações e os arredondamentos utilizados na apuração da nota final de Maturidade do processo de Gestão de Riscos Corporativos da Sabesp temos como Resultado Final a nota 3,33; que corresponde ao Nível Avançado.

Dos 7 (sete) aspectos avaliados, 5 (cinco) deles já atingiram a nota máxima do modelo referencial e estão no nível avançado.

Em relação aos outros 2 (dois) aspectos que estão hoje no nível abaixo do valor máximo do modelo, o desafio da Cultura de Riscos e do Vínculo da Estratégia com o Risco são os que vão requerer mais ações no médio e longo prazo, pois tratam-se de questões mais abrangentes e que permeiam e dependem de toda a organização.

Dentro deste contexto, a consultoria apresentou recomendações de melhoria relacionadas não só aos 2 (dois) aspectos abaixo do nível máximo do modelo, mas também aos demais, no sentido de promover a melhoria contínua do processo, as quais, na sua maioria, já se encontram priorizadas e inseridas no planejamento operacional da PK.

7. CONCLUSÃO E RECOMENDAÇÕES

É evidente que uma gestão de riscos eficaz melhora as informações para o direcionamento estratégico e para as tomadas de decisões de responsabilidade da governança contribui para a otimização do desempenho na realização dos objetivos de políticas e serviços públicos e, consequentemente, para o aumento da confiança dos cidadãos nas organizações públicas, além de prevenir perdas e auxiliar na gestão de incidentes e no atendimento a requisitos legais e regulamentares.

Integrar a gestão de riscos como elemento-chave da responsabilidade gerencial, implantar uma abordagem de controle interno baseada no risco e incluir a gestão de riscos nos programas de apoio ao desenvolvimento das competências dos gestores públicos são algumas das recomendações deste relatório.

Nesse contexto, o projeto teve o objetivo de avaliar o nível de maturidade do processo de gestão de riscos corporativos na Sabesp e foi focado em duas questões principais. A primeira sobre em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática.

As análises revelaram que a Instituição possui estrutura administrativa e técnica robusta e totalmente aderente às melhores práticas de mercado, alinhadas à NBR/ABNT ISO 31.000:2018 e ao framework COSO ERM. Além disso, há uma Superintendência de Gestão de Riscos e Conformidade (PK) responsável por implementar e fomentar a política e estratégias de gerenciamento de riscos nos processos institucionais.

A segunda questão está focada em determinar qual o nível de maturidade de gestão de riscos corporativos da Sabesp, principalmente em relação ao mercado. Neste ponto, a estratégia adotada foi a de utilizar o Índice de Governança e Gestão (iGG) apurado pelo TCU, que em 2021 abrangeu 378 órgãos públicos de vários setores. As análises deste trabalho mostraram que a Sabesp está entre as melhores empresas, isto é, se tivesse respondido o questionário de avaliação, muito provavelmente estaria dentre a os 9% que atingiram o nível AVANÇADO, com Nota Final de Maturidade de 3,33.

Resumidamente a Sabesp, dispõe de Políticas e Estratégias de gestão de riscos definidas, comunicadas e postas em prática. A identificação, análise, avaliação e a seleção de respostas aos riscos identificados e analisados como significativos é realizada de forma consistente em todos os níveis.

No entanto, mesmo estando no nível AVANÇADO, em termos gerais, a empresa pode ainda melhorar em alguns pontos. Por isso, foram apontadas algumas linhas de melhoria, que quando implantadas, aproximarão a SABESP ainda mais da nota 4 em todos os itens que compõem a prática Gerir Riscos do iGG.

8. REFERÊNCIAS BIBLIOGRÁFICAS

1. TRIBUNAL DE CONTAS DA UNIÃO. Gestão de Riscos – Avaliação de Maturidade, 2018.
2. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 31000, 2018.
3. CONTROLADORIA GERAL DA UNIÃO. Instrução Normativa Conjunta MP / CGU n.01, 2016.
4. BRASIL. Lei 13303 – Lei das Estatais, 2016.
5. THE INSTITUTE OF INTERNAL AUDITORS. Modelo das 3 linhas do IAA, 2020.