MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO
AUDITORIA INTERNA
Rua do Rouxinol, 115 – Bairro do Imbuí - CEP: 41.720-052 - Salvador – BA
Fone: (71) 3186-0046. E-mail: audin@ifbaiano.edu.br

TIPO DE AUDITORIA: OPERACIONAL
UNIDADE AUDITADA: INST. FED. DE EDUC., CIENC. E TEC. BAIANO – REITORIA
CÓDIGO: 158129
RELATÓRIO FINAL Nº: 02/2022
UAIG: AUDIN/IF Baiano
PROCESSO SUAP: 23327.250731.2022-31

RELATÓRIO FINAL DE AUDITORIA nº 02/2022

1 INTRODUÇÃO

Em atendimento ao Plano de Atividades de Auditoria Interna do Instituto Federal de Educação, Ciência e Tecnologia Baiano (IF Baiano) para o exercício de 2022, foi realizada avaliação 2.6.5 do PAINT 2022, que trata de Avaliação da Gestão de Riscos e Controles Internos. Como componente essencial da Governança e do ambiente de controle (COSO), a gestão de riscos é um processo que deve ser avaliado quanto à sua adequação, suficiência e eficácia da sua estrutura e cabe à Auditoria Interna emitir recomendação para o aprimoramento desse processo.

Segundo o TCU, no referencial "Dez passos para a boa governança",

> A **gestão de riscos** serve para identificar, entender os riscos e manter as instâncias responsáveis informadas, para que as respostas aos riscos sejam apropriadas. Para isso, a organização precisa implantar estrutura de gestão de riscos adequada às suas necessidades, definir o processo de gestão de riscos e integrá-lo à gestão e à tomada de decisão, garantindo a alocação de recursos e a existência dos canais de comunicação necessários.
> (TCU[1], 2021 - grifo nosso).

[1] TCU. Tribunal de Contas da União. **Dez passos para a boa governança** / Tribunal de Contas da União. Edição 2 – Brasília: TCU, Secretaria de Controle Externo da Administração do Estado, 2021. Disponível em: https://portal.tcu.gov.br/data/files/D5/F2/B0/6B/478F771072725D77E18818A8/10_passos_para_boa_governanca_v4.pdf

Nessa mesma linha, a portaria SEAUD/SEGECEX/TCU Nº 9, de 18 de maio de 2017 entende que:

> A **gestão de riscos** é elemento fundamental para a construção da governança corporativa. A implantação e o aprimoramento da gestão de riscos na organização constituem um processo de aprendizagem organizacional que começa com o desenvolvimento de uma consciência sobre a importância de gerenciar riscos e avança com a implantação de práticas e estruturas necessárias à gestão de riscos O ápice desse processo se dá quando a organização conta com uma abordagem consistente para gerenciar riscos e com uma cultura organizacional aderente aos princípios e práticas da gestão de riscos.
> (SEAUD/SEGECEX/TCU[2], 2017, p.20 – grifo nosso)

No âmbito do Poder Executivo Federal, o Referencial Técnico de Auditoria Interna Governamental, item 73, enfatiza que:

> O processo de gerenciamento dos riscos é responsabilidade da alta administração e do conselho, se houver, e deve alcançar toda a organização, contemplando a identificação, a análise, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos a que a Unidade Auditada está exposta.
> (CGU[3], 2017, p.15)

Tratando-se então da necessidade e importância do processo de gerenciamento de riscos no setor público, mais especificamente no caso do IF Baiano, entende-se que esse processo deve ser planejado, estruturado e sistematizado tendo como base os seus objetivos e a sua missão, conforme o Plano de Desenvolvimento Institucional 2021-2025 (PDI):

> Ofertar educação profissional, científica e tecnológica pública, gratuita e de excelência em diferentes níveis e modalidades, voltada ao desenvolvimento humano, social, econômico, cultural, tecnológico e científico de todos e de todas, em diferentes regiões da Bahia e do Brasil.
> (IF BAIANO, 2020[4], p.30)

Em relação aos principais riscos **a que a unidade está exposta e os controles internos associados a estes riscos,** compete ao Comitê de Governança, Riscos e Controles elaborar, manter e revisar periodicamente o processo de gestão de riscos, alinhado às estratégias institucionais, coordenar o processo de gestão de riscos, zelando pela execução das atividades e implementação dos controles decorrentes desta Política.

---

[2] Brasil. Tribunal de Contas da União. **Roteiro de Auditoria de Gestão de Riscos**: Tribunal de Contas da União. Métodos e Suporte ao Controle Externo, 2017 123 p. Disponível em: https://portal.tcu.gov.br/data/files/46/B3/C6/F4/97D647109EB62737F18818A8/Manual_gestao_riscos_TCU_2_edicao.pdf

[3] Tribunal de Contas da União**. Instrução Normativa nº 3, de 09 de junho de 2017**. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. 2017. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/auditoria-e-fiscalizacao/pgmq/arquivos/in-sfc-03-2017-referencial-tecnico.pdf

[4] IF BAIANO**. Plano de Desenvolvimento Institucional - PDI - 2021 2025.** 2020. Disponivel em: https://ifbaiano.edu.br/portal/pdi/

2 CONTEXTUALIZAÇÃO

No âmbito do Poder Executivo Federal, com o advento da publicação da Instrução Normativa Conjunta MP/CGU nº 01de 2016, que dispõe sobre a sistematização de práticas relacionadas à governança, à gestão de riscos e aos controles internos no âmbito de órgãos e entidades do Poder Executivo Federal, os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança.

O IF Baiano, através da Resolução nº 17 de 09/05/2017, aprovou a sua Política de Gestão de Riscos, Controles Internos e Governança. Ao instituir tal política, o Instituto se comprometeu a promover:

- a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais;
- o alinhamento do apetite ao risco com as estratégias adotadas;
- o fortalecimento das decisões em resposta aos riscos;
- o aprimoramento dos controles internos de gestão.

Importante destacar que a Política de Gestão de Riscos, Controles Internos e Governança, foi revisada pela Resolução nº 62 de 20/12/2018 e estabelece que o Instituto deverá promover:

- a interação entre os setores de Comunicação e a Alta Gestão para divulgação dos objetivos institucionais;
- a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais;
- o alinhamento do apetite ao risco com as estratégias adotadas;
- o fortalecimento das decisões em resposta aos riscos;
- o aprimoramento dos controles internos de gestão.

Partindo-se do pressuposto de que que o gerenciamento de riscos deverá ser um processo sistemático, estruturado e oportuno (art.14 da IN Conjunta MP/CGU nº01/2016), ou seja, deve possuir uma estrutura na sua implementação (art.16), a administração deverá implementar uma estratégia para atender a diversas etapas que a implementação de um modelo de gerenciamento de riscos deverá ter.

Conforme demonstrado no art. 10 da Política de Gestão de Riscos mais atual do IF Baiano (2018), a Alta Administração, bem como os Agentes da Administração, deverá observar os seguintes componentes da estrutura de gestão de riscos, segundo o artigo 16 da IN Conjunta MP/CGU nº01/2016, COSO ERM (COSO II), e com os princípios da ISO NBR31000:2018:

- Entendimento de contexto;
- Ambiente interno;
- Fixação de objetivos;
- Identificação de eventos;
- Avaliação de riscos;
- Resposta a riscos;
- Atividades de controles internos;

- Informação e comunicação;
- Monitoramento.

Dessa forma, buscando cumprir com a sua missão institucional, a Auditoria Interna buscou avaliar o processo de gerenciamento de riscos do IF Baiano, conforme exposto nos próximos itens deste Relatório.

3 OBJETIVO E ESCOPO

De acordo com a Política de Gestão de Riscos do Instituto Federal Baiano, aprovada pela Resolução CONSUP nº 62/2018, cabe ao Comitê de Governança, Riscos e Controles elaborar, manter e revisar periodicamente o processo de gestão de riscos, alinhado às estratégias institucionais. Desse modo, o presente trabalho buscou avaliar se a política de gerenciamento de riscos está sendo implementada e em que nível de maturidade se encontra, com a finalidade de que sejam emitidas recomendações em relação a aperfeiçoamentos no processo de gerenciamento de riscos, dessa forma, agregando valor ao processo de governança institucional.

4 METODOLOGIA

Para determinar o nível de maturidade da gestão de riscos, foi adotado como referência o Roteiro de Avaliação de Maturidade de Gestão de Riscos desenvolvido e disponibilizado pelo TCU, elaborado a partir das melhores práticas internacionais em uso no setor público, provenientes dos modelos de gerenciamento de riscos COSO GRC (COSO, 2004 e 2016), ABNT NBR ISO 31000 Gestão de Riscos – Princípios e Diretrizes (ABNT, 2009) e Orange Book (UK, 2004 e 2009), bem como a Instrução Normativa Conjunta MP/CGU Nº 01/2016.

O referido modelo de avaliação da maturidade da gestão de riscos propõe a análise a partir 04 (quatro) dimensões, conforme figura seguir:

Figura 1: Dimensões para avaliação da maturidade da gestão de riscos

Fonte: Modelo de avaliação da maturidade em gestão de riscos elaborado pelo TCU (BRASIL, 2013[5]).

[5] TRIBUNAL DE CONTAS DA UNIÃO. **Gestão de Riscos – Avaliação da Maturidade**. Brasília: TCU, SEGECEX/ADGECEX/SEMEC, janeiro, 2018. Disponível https://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm. Acessado em: agosto, 2022.

Os pesos de cada dimensão foram determinados usando-se a técnica AHP (*Analytic Hierarchy Process*, COYLE, 2004) aplicada às respostas dadas por oito especialistas do TCU a comparações duas-a-duas da importância relativa das quatro dimensões do modelo. A planilha de avaliação da maturidade da gestão de riscos com os resultados por dimensão está no **Apêndice I** deste Relatório.

4.1 Dimensões do modelo

O modelo adotado pelo TCU é composto por quatro dimensões, portanto, a proposta de avaliação do procedimento de gerenciamento de riscos descrita neste trabalho buscou avaliar a maturidade nas dimensões descritas no diagrama acima: "**Ambiente**", "**Processos**", "**Parcerias**" e "**Resultados**".

- Dimensão "**Ambiente**"

Engloba boas práticas relacionadas com a *cultura*, a *governança de riscos* e a *consideração do risco na definição da estratégia e dos objetivos* em todos os níveis, procurando avaliar as capacidades existentes para que a gestão de riscos tenha as condições necessárias para prosperar na organização.

- Dimensão "**Processos**"

Esta dimensão aborda os aspectos relacionados ao processo de gestão de riscos, procurando avaliar em que medida a organização estabeleceu um processo formal, com padrões e critérios definidos para a *identificação e análise de riscos, avaliação e resposta a riscos*, incluindo a seleção e a implementação de respostas aos riscos avaliados, e *monitoramento e comunicação* relacionada a riscos e controles com partes interessadas, internas e externas.

- Dimensão "**Parcerias**"

Esta dimensão trata de 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 sobre o seu gerenciamento.

- Dimensão "**Resultados**"

Esta dimensão trata de aspectos relacionados aos 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 os 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.

4.2 Cálculo da maturidade da gestão de riscos

O índice de maturidade global da gestão de riscos é obtido pela média ponderada dos índices de maturidade das dimensões (IMD) pelos seguintes pesos:

Tabela 01: Pesos e exemplo de cálculo do IMD

DIMENSÃO	PESO	EXEMPLO		
		IMD	PESO	PONDERADO
Ambiente	40	52,6	0,4	21,0
Processos	30	45,9	0,3	13,8
Parcerias	10	80,1	0,1	8,0
Resultados	20	49,5	0,2	9,9
ÍNDICE DE MATURIDADE GLOBAL				52,7

Fonte: adaptado de BRASIL[6],2013

O índice de maturidade global da gestão de riscos é obtido pela média ponderada dos índices de maturidade das dimensões (IMD) pelos seguintes pesos:

Tabela 2: Níveis de maturidade da gestão de riscos

ÍNDICE DE MATURIDADE APURADO	NÍVEL DE MATURIDADE
De 0% a 20%	Inicial
De 20,1% a 40%	Básico
De 40,1% a 60%	Intermediário
De 60,1% a 80%	Aprimorado
De 80,1% a 100%	Avançado

Fonte: BRASIL[7], 2013

O **índice de maturidade de cada um dos aspectos (questões)** foi calculado a partir do somatório de pontos do conjunto de questões que compõe o aspecto, calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível, expressando esse quociente com um número entre 0% e 100%.

Nível de maturidade do aspecto = (Soma da pontuação obtida no aspecto/ Pontuação máxima do aspecto) * 100.

O **índice de maturidade de cada dimensão** (Ambiente; Processos; Parcerias; e Resultados) foi calculado a partir do somatório de pontos do conjunto de questões que compõe cada dimensão, calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível, expressando esse quociente com um número entre 0% e 100%.

Nível de maturidade da dimensão = (Soma da pontuação obtida na dimensão/Pontuação máxima da dimensão) * 100

---

[6] Brasil. Tribunal de Contas da União. **Roteiro de Avaliação de Maturidade da Gestão de Riscos** / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018. 164 p.

[7] Brasil. Tribunal de Contas da União. **Roteiro de Avaliação de Maturidade da Gestão de Riscos** / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018. 164 p.

O **índice de maturidade global da gestão de riscos** foi obtido pela média ponderada dos IMD pelos seguintes pesos:

Tabela 3: Método de avaliação global da maturidade

Dimensão	Peso
Ambiente	40
Processos	30
Parcerias	10
Resultados	20

Fonte: Roteiro de Avaliação de Maturidade da Gestão de Riscos (2018)

O trabalho realizado passou pelas seguintes etapas: planejamento dos trabalhos, fase interna da AUDIN que envolve a elaboração do programa de trabalho de auditoria, reunião de abertura dos trabalhos de avaliação, levantamento das informações (coleta de evidências), execução de análises, relatoria e entrega. Importante destacar a **reunião de abertura dos trabalhos** com o Reitor substituto, onde foram tratados aspectos como:

- Entendimento do escopo dos trabalhos pelo gestor, podendo este esclarecer possíveis pontos a serem considerados nos trabalhos;
- Visão mais apurada das questões do objeto a ser avaliado;
- Mais eficiência e eficácia dos trabalhos, produzindo entrega adequada e geração de valor ao processo avaliado.

Após os esclarecimentos dos principais pontos da avaliação à alta administração, destacando o propósito e metodologia dos trabalhos, foram emitidas solicitações de informações, foi realizada reunião exploratória com o Comitê Executivo de Gestão de Riscos, Controles Administrativos e Transparência (CEGRCAT) e, de forma a proceder análise mais apurada sobre o processo de gerenciamento de riscos do IF Baiano, bem como a sua maturidade.

As técnicas de auditoria empregadas neste trabalho foram: indagação escrita e oral (entrevistas, reuniões, questionário), análise documental e *benchmarking*.

5 CRITÉRIOS, QUESTÕES E SUBQUESTÕES DE AUDITORIA

A base normativa e referencial utilizada para subsidiar os trabalhos foi a seguinte:

- Instrução Normativa Conjunta CGU/MP N° 1, DE 10.05.2016;
- Política de Gestão de Riscos, Controles Internos e Governança do IF Baiano;
- Referencial de Governança do Tribunal de Contas da União;
- Roteiro de Avaliação de Maturidade da Gestão de Riscos / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018;
- Relatório de Auditoria 003/2021 – Auditoria Interna do Instituto Federal Educação, Ciência e Tecnologia de Pernambuco;
- Instrução Normativa da Secretaria Federal de Controle nº 03/2017 - Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal;
- Plano de Desenvolvimento Institucional do IF Baiano – PDI 2021-2025.

Com vistas a compor o programa de trabalho de auditoria, na fase inicial do processo de avaliação, a matriz de planejamento foi elaborada com a seguinte estrutura:

5.1 Questões de Auditoria

De modo a se obter informações, dados e explicações que contribuam efetivamente para o alcance dos objetivos do trabalho de auditoria foram formuladas perguntas com a finalidade de avaliar se:

i. A gestão de riscos do IF Baiano está sendo implementada de acordo com as orientações dispostas nas normas correlatas?

ii. A gestão de riscos está sendo realizada de forma sistemática e estruturada e oportuna?

5.2 Subquestões de Auditoria

i. Foi elaborada e institucionalizada Política de Gestão de Riscos?

ii. Os riscos foram identificados e tratados ao ponto de que foram estabelecidos níveis de exposição a riscos adequados?

iii. Foram estabelecidos procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização?

iv. Foi utilizado mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico?

v. A gestão de riscos foi utilizada para apoiar a melhoria contínua dos processos organizacionais?

vi. O Comitê de Governança, Riscos e Controles aprovou política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos, liderou e supervisionou a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade?

vii. Riscos significativos são identificados e avaliados?

viii. Respostas aos riscos são estabelecidas de forma compatível com o apetite a risco?

ix. O processo de gerenciamento dos riscos alcança toda a organização, contemplando a identificação, a análise, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos a que a Unidade Auditada está exposta?

As questões e subquestões acima estão inseridas nas dimensões avaliativas no modelo de avaliação de maturidade, sendo que estas questões foram respondidas preliminarmente às questões elencadas na planilha de maturidade (**Apêndice I**).

6 ANÁLISE DAS EVIDÊNCIAS

Subsidiando o resultado do nível de maturidade da gestão de riscos feito por aplicação de questionário, foi emitida solicitação de auditoria para obtenção de análises de questões, pesquisas no site institucional bem como a realização de reuniões exploratórias. As questões foram direcionadas ao Comitê de Governança, Riscos e Controles do IF Baiano, sendo que o Comitê Executivo de Gestão de Riscos, Controles Adm. e Transparência se encarregou de fornecer as respostas e se reunir com a AUDIN para esclarecer aspectos do tema em avaliação.

Foi verificado que o IF Baiano possui diretriz (Política de Gestão de Riscos) para implementação do processo de gestão de riscos, além disso, foram realizadas diversas reuniões do Comitê de Governança, Riscos e Controles. Da análise de atas das reuniões do CGRC desde o ano de 2018 até 2021, verificou-se que foram tratados diversos temas referentes a gestão da pandemia da COVID 19, que trouxe um risco significativo à saúde dos servidores e comunidade do Instituto, além de assuntos como análise de Editais, encaminhamentos de Pró-Reitorias, remoções de servidores dentre outros.

Não ficou evidenciado, entretanto, a existência ou execução de um plano de ação de gestão de riscos que evidenciasse a existência de um processo sistematizado ou estruturado, conforme a própria Política de Gestão de Riscos do IF Baiano e Instrução Normativa Conjunta CGU/MP N° 1, DE 10.05.2016.

Em 2022, em análise da ata da 8ª reunião extraordinária do CGRC, verificou-se que a pauta foi contemplada com o assunto "O papel do Comitê de Governança, Riscos e Controle - CGRC do IF Baiano" sendo deliberado o que segue:

> Definido a elaboração do Plano de Gestão Risco das Pró-Reitorias, das Diretorias Sistêmicas e do Gabinete/Reitoria para viabilizar a supervisão dos riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público.
> (IF Baiano, 2022[8])

Importante destacar que a existência de um documento norteador da execução do processo de gestão de riscos é essencial para entendimento de que gestão de riscos é um processo estruturado e sistemático, devendo possuir elementos trazidos no art. 10 da Política de Gestão de Riscos do IF Baiano.

Em relação à necessidade de se executar o processo de gestão de riscos em conformidade com as normativas vigentes, o Comitê Executivo de Gestão de Riscos, Controles Administrativos e Transparência (CEGRCAT) do IF Baiano reconhece a necessidade de aprimoramento do processo de gestão de riscos do IF Baiano, conforme trecho de ata de reunião realizada com a AUDIN em 14/06/2022:

> O servidor (membro do CEGRCAT) fez considerações sobre a documentação apresentada, informando as situações e dificuldades na implementação da gestão de riscos, manifestando interesse em adotar tais modelos apresentados

[8] ATA DA 8ª REUNIÃO EXTRAORDINÁRIA-2022 do Comitê de Governança. Riscos e Controles. Disponível em: https://ifbaiano.edu.br/portal/wp-content/uploads/2022/06/8a-Reuniao-Extraordinaria-19.04.22-OA-CGGRC.IFBAIANO-1.pdf

> (item 4), reconhecendo a necessidade de aprimoramento do processo de gestão de riscos no IF Baiano. O servidor descreveu também ações desenvolvidas pelo Comitê de Governança em relações a riscos que o IF Baiano estava e está exposto;

Por sua vez, diante desse cenário, a AUDIN faz as seguintes considerações:

> O servidor (membro da AUDIN) reconheceu as dificuldades de implementação do processo de gestão de riscos, considerando os diversos aspectos desse processo, incluindo a mobilização e rotatividade de servidores e gestores, interrupção do processo de gestão de riscos devido à pandemia da COVID 19 e estruturação desse processo nos Campi;

Considerando o exposto, entende-se que esforços devem ser envidados na criação de um ambiente ou cultura de gestão de riscos, de forma contínua, em que o IF Baiano, nos seus processos e atividades, no estratégico, técnico e operacional, incorporem a prática de se gerenciar riscos. Trata-se da dimensão "**ambiente**" do modelo de avaliação de maturidade aplicado aos exames.

Por sua vez, verifica-se que, na dimensão "**processos**", o IF Baiano ainda carece de implementar os elementos que indiquem a execução do processo de gerenciamento de riscos de forma sistemática e estruturada, onde foram relacionadas dificuldades organizacionais nesse sentido. De fato, a implementação de processo de gerenciamento de riscos exige uma mobilização de recursos humanos, financeiros e ambientais (organizacionais) e que o IF Baiano tem recursos limitados para implementar esse processo.

7 RESULTADO DOS EXAMES

Importante destacar e reafirmar que a obtenção dos resultados dos exames se deu com base em análises de evidências obtidas através de entrevistas, busca de documentações no site do IF Baiano, solicitações de informações e reuniões com o Comitê Executivo de Gestão de Riscos, Controles Administrativos e Transparência (CEGRCAT).

7.1 Dimensão "Ambiente"

Sendo o "Ambiente" a dimensão como o maior peso do modelo (40), onde se 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, temos o resultado **35,61%,** obtendo-se uma avaliação no nível **básico.**

Compondo o índice desta dimensão, temos o resultado de cada seção:

- Liderança: **39%** - nível básico;
- Políticas e estratégias: **35%** - nível básico;
- Pessoas: **33%** - nível básico;

7.2 Dimensão “Processos”

A dimensão “Processos” possui um peso de 30, ou seja o segundo maior peso do modelo. De acordo com os exames, confirmando o nível de maturidade apurado na planilha, temos um resultado de **9%,** obtendo-se uma avaliação no nível **inicial.** De acordo com os exames nessa dimensão, verificou-se que o IF Baiano não possui um processo sistemático e estruturado de gestão de riscos com todos os componentes e estruturas inerentes conforme normativas e modelos existentes, embora atenda a alguns aspectos identificados nesta dimensão como “**Documentação do Estabelecimento do Contexto**” e “**Identificação e Análise dos Riscos**”.

Compondo o índice desta dimensão, temos o resultado de cada seção:

- Identificação e análise de riscos: **30%** - nível básico;
- Avaliação e resposta a riscos: **0%** - nível inicial;
- Monitoramento e comunicação: **5%** - nível inicial.

Apesar do nível de maturidade da seção “**Identificação e análise de riscos**” apontar para um resultado de 30%, indicando uma maturidade de nível básico, não temos evidências em relação a existência de um processo ou modelo definido, sistemático e estruturado de gerenciamento de riscos, entende-se que o IF Baiano conhece o seu contexto estratégico e possui documentação do estabelecimento desse contexto (Plano de Desenvolvimento Institucional – PDI). Na questão “**Documentação da Identificação e Análise de Riscos**”, obtemos uma avaliação no nível “Inexistente”, por verificarmos ausência dessa documentação em um processo de gerenciamento de riscos sistemático e estruturado. A mesma situação se encontra a questão “**Avaliação e Resposta a Riscos** “e “**Informação e Comunicação**”, onde encontramos aspectos inerentes a existência de processo sistemático e estruturado de gerenciamento de riscos.

7.3 Dimensão “Parcerias”

A dimensão “Parcerias” possui um peso de 10, ou seja, o menor peso do modelo. De acordo com os exames, confirmando o nível de maturidade apurado na planilha, temos um resultado de **0%,** obtendo-se uma avaliação no nível **inicial.** A avaliação dos aspectos inerentes a processo de gerenciamento de riscos no âmbito de parcerias concluiu que a organização não adota um conjunto de práticas essenciais para ter segurança razoável de que riscos são adequadamente gerenciados e os objetivos alcançados.

Compondo o índice desta dimensão, temos o resultado de cada seção:

- Gestão de riscos em parcerias: **0%** - nível inicial;
- Planos e medidas de contingência: **0%** - nível inicial.

7.4 Dimensão “Resultados”

A dimensão “Resultados” possui um peso de 20, ou seja, o terceiro maior peso do modelo. De acordo com os exames, confirmando o nível de maturidade apurado na planilha, temos um resultado de **0%,** obtendo-se uma avaliação no nível **inicial.** Nesta dimensão, o resultado da maturidade está coerente com a maturidade da dimensão “**Processos**”, pois reflete as

consequências de um processo sistemático e estruturado de gerenciamento de riscos, caso este estivesse sido implementado na organização.

Compondo o índice desta dimensão, temos o resultado de cada seção:

- Melhoria dos processos de governança: **0%** - nível inicial;
- Resultados-chave da gestão de riscos: **0%** - nível inicial;

7.5 Índice de Maturidade Global

O índice de maturidade global da gestão de riscos foi obtido pela média ponderada dos índices de maturidade das dimensões (IMD). Com um índice de Maturidade de **17,07%,** a classificação do nível de maturidade da gestão de riscos da Instituição é **Inicial** (Figura 01 e Tabela 2).

Figura 01: pela média ponderada IMD

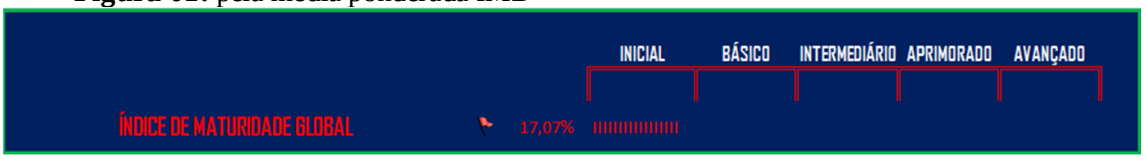

Tabela 2 – Referência para classificação do nível de maturidade

Índice de maturidade apurado	Nível de maturidade
De 0% a 20%	Inicial
De 20,1% a 40%	Básico
De 40,1% a 60%	Intermediário
De 60,1% a 80%	Aprimorado
De 80,1% a 100%	Avançado

Fonte: Roteiro de Avaliação de Maturidade da Gestão de Riscos (2018)

Com base nesses resultados, foram feitas propostas de encaminhamentos junto a alta gestão para acompanhar a evolução do amadurecimento da gestão de riscos. As informações obtidas seguiram monitoradas pela AUDIN, em busca de soluções que envolvam todo o IF Baiano, no que for pertinete. Espera-se assim que a AUDIN possa contribuir positivamente para auxiliar nesse processo.

8 PROPOSTAS DE ENCAMINHAMENTOS

Diante dos resultados levantados do nível de maturidade do processo de gerenciamento de riscos do IF Baiano, propomos o que segue, considerando aspectos:

I. Elaborar Plano de Ação do Processo de Gerenciamento de Riscos, a exemplo do que foi feito no Instituto Federal de Alagoas. Por se tratar de uma **proposta de Plano de Ação**, não obsta o IF Baiano elaborar o seu Plano de Ação conforme entender mais adequado;

II. Dimensão "**Ambiente**":

- O **Plano de Ação** poderá estabelecer aspectos de conscientização da gestão de riscos (capacitações, palestras, campanhas etc.) como fator do ambiente visando preparar o IF Baiano para implementação das estruturas referentes ao **processo de gerenciamento de riscos.** Nesta etapa, segundo o TCU, "busca-se avaliar em que medida os responsáveis pela governança e a alta administração exercem as 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."

III. Dimensão "**Processos**":

- Compondo esta dimensão no **Plano de Ação** do processo de gerenciamento de riscos, implementar as ações necessárias dispostas na **Política de Gestão de Riscos do IF Baiano** onde estão elencadas as etapas do gerenciamento de riscos propriamente dito ou **execução do processo de gerenciamento de riscos,** que são: estabelecimento do contexto, identificação dos riscos, tratamento dos riscos e monitoramento de riscos, atentando-se para a **atualização da exposição aos riscos e respectivas respostas a riscos,** considerando fatores internos e externos e que trata-se de um processo contínuo e dinâmico.

IV. Dimensão "**Parcerias**":

- Segundo o TCU, "Parcerias são quaisquer arranjos estabelecidos para possibilitar relacionamento colaborativo entre partes, visando o alcance de objetivos de interesse comum. As parcerias são usualmente estabelecidas para atingir um objetivo estratégico ou a entrega de um produto ou serviço, sendo formalizadas por um determinado período, implicando a negociação e o claro entendimento das funções de cada parte, bem como dos benefícios decorrentes (BRASIL,2009, p. 21). Envolvem, portanto **riscos e benefícios compartilhados**. (grifo nosso)"

Partindo dos pressupostos em relação à gestão de riscos relacionados às parcerias, onde o IF Baiano necessita implementar conforme o nível de maturidade alcançado (inicial) nesta dimensão, sugere-se o que segue:

- Incorporar o processo de gerenciamento de riscos às parcerias do IF Baiano,

considerando:

i. Realizar avaliação fundamentada e documentada da capacidade das potenciais organizações parceiras para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado;

ii. Aplicar o processo de gestão de riscos para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado das políticas de gestão compartilhadas;

iii. Definir planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços em casos de desastres ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar.

iv. Outros aspectos definidos, não menos importantes, no modelo de maturidade relacionadas no Apêndice I.

V. Dimensão "**Resultados**"

Essa dimensão trata do resultado, consequências ou agregação de valor decorrentes da implementação do processo de gestão de riscos nos processo de governança e gestão. Considerando o nível de maturidade inicial desta dimensão, propõe-se o que segue:

- Implementar o processo de gerenciamento de riscos no IF Baiano, integrado e coordenado por todas as áreas, funções, atividades relevantes e críticas para a realização dos objetivos-chaves de modo que se obtenha uma avaliação capaz de demonstrar que 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.

9 MANIFESTAÇÃO DO GESTOR

O Diretor Executivo (Reitor substituto) demonstrou concordância em relação aos apontamentos da AUDIN no processo de avaliação da maturidade da GR, inclusive para subsidiar a implementação do modelo a ser proposto pelo Grupo de Trabalho do CONIF.

10 CONCLUSÃO DE CONSIDERAÇÕES FINAIS

Diante do diagnóstico atual da maturidade do processo de gerenciamento de riscos no IF Baiano, foram identificadas situações que necessitam de implementações ou aprimoramentos, conforme as respectivas proposições por dimensão do modelo de maturidade. Essas proposições visam, através da implementação de um processo estruturado e sistemático de gestão de riscos, adicionar mais valor aos serviços públicos ofertados.

Dessa forma, após a concordância do Gestor em relação aos encaminhamentos consignados no Relatório Preliminar nº02/2022, o levantamento da maturidade da GR está concluído. A AUDIN acompanhará junto ao Gestor a implementação do processo de GR. A AUDIN se colocou à disposição para realizar serviços de consultoria e facilitação no processo de implementação do processo de gestão de riscos do IF Baiano.

Salvador, 29 de novembro de 2022.

Guilherme Principe de Oliveira Galheigo
Auditor/AUDIN

João Vitor Miranda de Menezes
Coordenador/AUDIN

Apêndice I

1. AMBIENTE	Índice de Maturidade da Dimensão
Nesta dimensão, busca-se 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.	**Básico** **36%**

A seguir, temos o detalhamento das capacidades da dimensão:

1.1. Liderança	Índice de Maturidade desta Seção
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, 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.	Básico 39%

CULTURA			
Questão 1.1.1 A alta administração e os responsáveis pela governança reconhecem importância da cultura, integridade e valores éticos, e da consciência de riscos como aspectos-chaves para o reforço da accountability:	Critério	Avaliação	Descrição
a) fornecendo normas, orientações e supervisionando a inclusão desses aspectos-chaves nos programas de apoio ao desenvolvimento de gestores;	IIN-MP/CGU 1/2016, Art. 8º, I e II; Art. 11, I; Art. 16, I e Art. 21;	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.

b) reforçando o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização;	COSO GRC 2004, 2; COSO GRC Public Exposure (PE) 2016, Princípios 3, 4 e 5; ISO 31000:2009, 3, "h" e 4.2; OCDE, 2011.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
c) instituindo políticas, programas e medidas definindo padrões de comportamento desejáveis, tais como códigos de ética e de conduta, canais de comunicação para cima e de denúncia, ouvidoria, e avaliação da aderência à integridade e aos valores éticos.		Aprimorado	Prática realizada de acordo com normas e padrões definidos na maior parte das áreas relevantes para os objetivos-chaves da organização.
GOVERNANÇA DE RISCOS Questão 1.1.2	Critério	Avaliação	Descrição
Os responsáveis pela governança e a alta administração utilizam instâncias internas (p.ex.: comitês de governança, riscos e controles, auditoria, coordenação de gestão de riscos etc.) e outras medidas para apoiar suas responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chaves da organização.	IN-MP/CGU 1/2016, Art. 23, II, Art. 17, II, "a" e "d"; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, e 2; ISO 31000:2009, 3, "b", "c", "e" e 4.1.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
SUPERVISÃO DA GOVERNANÇA E DA ALTA ADMINISTRAÇÃO Questão 1.1.3 Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos, inclusive mediante:	Critério	Avaliação	Descrição

a) incorporação explícita e monitoramento regular de indicadores-chaves de risco e indicadores-chaves de desempenho nos seus processos de governança e gestão;	IN-MP/CGU 1/2016, Art. 16, parágrafo único; Art. 19, 20 e 23, IX; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, 2 e 5; ISO 31000:2009, 4.2.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
b) notificação regular e oportuna sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos;		Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
c) revisão sistemática da visão de portfólio de riscos em contraste com o apetite a riscos e fornecimento de direção clara para gerenciamento dos riscos;		Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
d) utilização dos serviços da auditoria interna e de outras instâncias de asseguração para se certificarem de que a administração tem processos eficazes de gerenciamento de riscos e controle; e		Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
e) definição do nível de maturidade almejado para a gestão de riscos e monitoramento do progresso das ações para atingir ou manter-se no nível definido.		Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.

1.2. Políticas e estratégias	**Índice de Maturidade da Seção**	
Nesta seção, busca-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.	Básico	35%

DIRECIONAMENTO ESTRATÉGICO

Questão 1.2.1	Critério	Avaliação	Descrição

A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico (objetivos-chaves, missão, visão e valores fundamentais da organização), alinhado com as finalidades e as competências legais da entidade, traduzindo uma expressão inicial do risco aceitável (apetite a risco) para a definição da estratégia e a fixação de objetivos estratégicos e de negócios, e para o gerenciamento dos riscos relacionados.	IN-MP/CGU 1/2016, Art. 2º, II; Art. 14, II; Art. 16, II; e Art. 19; COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 1, 3 e 7. ISO 31000:2009, 5.3.3.	Aprimorado	Prática realizada de acordo com normas e padrões definidos na maior parte das áreas relevantes para os objetivos-chaves da organização.
Questão 1.2.2	Critério	Avaliação	Descrição
A alta administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o apetite a risco na forma de uma expressão ampla, porém suficientemente clara, de quanto risco a organização está disposta a enfrentar na implementação da estratégia para cumprir sua missão institucional e agregar valor para as partes interessadas, a fim de orientar a definição de objetivos por toda a organização; a seleção de estratégias para realizá-los; a alocação de recursos entre as unidades e iniciativas estratégicas; e a identificação e o gerenciamento dos riscos, alinhados com o apetite a risco.	IN-MP/CGU 1/2016, Art. 2º, II, e Art. 14, II; Art. 16, II, e V; COSO GRC 2004, 1, 2 e 3; COSO GRC PE 2016, Princípios 1, 7 e 8; ISO 31000:2009, 3, “g” e 5.3.3.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
INTEGRAÇÃO DA GESTÃO DE RISCOS AO PROCESSO DE PLANEJAMENTO Questão 1.2.3 A organização dispõe de um processo de planejamento estratégico implementado para, a partir do direcionamento estratégico e do apetite a risco definidos conforme abordado nos seguintes subitens:	Critério	Avaliação	Descrição
a) os ***objetivos estratégicos*** de alto nível alinhados e dando suporte à missão, à visão e aos propósitos da organização e selecionadas as estratégias para atingi-los, considerando as várias alternativas de cenários e os riscos associados, de modo a estabelecer uma base consistente para a definição dos objetivos de negócios específicos em todos os níveis da organização;	IN-MP/CGU 1/2016, Art. 8º, VI; Art. 14, IV; Art. 16, II. COSO GRC 2004, 3; COSO GRC PE 2016,	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.

b) os ***objetivos de negócios*** específicos associados a todas as atividades, em todos os níveis, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade e as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho), alinhados aos objetivos estratégicos e ao apetite a risco estabelecidos.	Princípios 9, 10 e 11; INTOSAI GOV 9130/2007, 1.3 e 2.2.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
Questão 1.2.4	Critério	Avaliação	Descrição
A administração define os objetivos mencionados na alínea "b", do item 1.2.3, e as respectivas medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho), explicitando-os com clareza suficiente, em termos específicos e mensuráveis, comunicando-os a todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização e aos responsáveis em todos os níveis, a fim de permitir a identificação e avaliação dos riscos que possam ter impacto no desempenho e nos objetivos.	IN-MP/CGU, Art. 16, II. COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 10 e 11; COSO 2013, Princípio 6, atributos "a" e "b"; INTOSAI GOV 9130, 2.2.	Inexistente	Prática inexistente, não implementada ou não funcional.
POLÍTICA DE GESTÃO DE RISCOS Questão 1.2.5 A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, comunicada apropriadamente e disponível para acesso a todos, abordando os seguintes aspectos:	Critério	Avaliação	Descrição
a) os princípios e objetivos relevantes da gestão de riscos na organização e as ligações entre os objetivos e políticas da organização com a política de gestão de riscos;	IN-MP/CGU, Art. 17, I. ISO 31000:2009, 4.3.2.	Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.

b) as diretrizes para a integração da gestão de riscos a todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão em todos os níveis da organização e as parcerias com outras organizações;	IN-MP/CGU, Art. 17, II, "a"; ISO 31000:2009, 3, "b" e 4.3.4;	Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
c) a definição clara de responsabilidades, competências e autoridade para gerenciar riscos no âmbito da organização como um todo e em todas as suas áreas (unidades, departamentos, divisões, processos e atividades), incluindo a responsabilidade pela implementação e manutenção do processo de gestão de riscos e de asseguração da suficiência, eficácia e eficiência de quaisquer controles;	IN-MP/CGU, Art. 17, II, "d" e III; ISO 31000:2009, 4.3.3. COSO GRC 2004, 10; COSO GRC PE 2016, Princípio 5;	Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
d) diretrizes sobre como e com qual periodicidade riscos devem ser identificados, avaliados, tratados, monitorados e comunicados, através de um plano de implementação do processo de gestão de riscos, em todos os níveis, funções e processos relevantes da organização;	IN-MP/CGU, Art. 17, II, "b" e 18; ISO 31000:2009, 4.3.4 e 4.4.2. COSO GRC 2004, 4 a 9; COSO GRC PE 2016, Princípios 12 a 16 e 21.	Inexistente	Prática inexistente, não implementada ou não funcional.
e) diretrizes sobre como o desempenho da gestão de riscos, a adequação da estrutura, a aplicação do processo de gestão de riscos e a efetividade da política de gestão de riscos serão medidos e reportados;	IN-MP/CGU, Art. 17, II, "c"; ISO 31000:2009, 4.3.2, 4.3.3 e 4.5. COSO GRC 2004, 8 e 9; COSO GRC PE 2016, Princípios 20 e 21.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.

f) atribuição clara de competências e responsabilidades pelo monitoramento, análise crítica e melhoria contínua da gestão de riscos, bem como diretrizes sobre a forma e a periodicidade como as alterações devem ser efetivadas.	IN-MP/CGU, Art. 17, II, "c" e III; ISO 31000:2009, 4.3.3, 4.5 e 4.6. COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 22 e 23.	Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
COMPROMENTIMENTO DA GESTÃO			
Questão 1.2.6	Critério	Avaliação	Descrição
A alta administração e o corpo executivo da gestão (tática e operacional) estão completa e diretamente envolvidos em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade	IN-MP/CGU, Art. 12 e 16, § único; Art. 17, II, "e" e "f"; Art. 19 e 20; ISO 31000:2009, 4.2 e 4.3.3.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
ALOCAÇÃO DE RECURSOS			
Questão 1.2.7	Critério	Avaliação	Descrição
A administração aloca recursos suficientes e apropriados (pessoas, estruturas, sistemas de TI, programas de treinamento, métodos e ferramentas para gerenciar riscos) para a gestão de riscos, considerando uma relação equilibrada com o tamanho da organização, a relevância das áreas, funções e atividades críticas para a realização dos seus objetivos-chaves, bem como com a natureza e o nível dos riscos.	IN-MP/CGU, Art. 17, II, "f"; Art. 23, II, III e IX. ISO 31000:2009, 4.3.5. COSO GRC PE 2016, Princípio 2.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
1.3. Pessoas			**Índice de Maturidade da Seção**
Nesta seção, busca-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.		Básico	33%

REFORÇO DA *ACCOUNTABILITY*			
Questão 1.3.1	Critério	Avaliação	Descrição
Todo o pessoal na organização, inclusive prestadores de serviços e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de se levar a sério suas responsabilidades de gerenciamento riscos, bem como é orientado e sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes. Ademais, o pessoal designado para atividades de identificação, avaliação e tratamento de riscos recebe capacitação suficiente para executá-las, inclusive no que diz respeito à identificação de oportunidades e à inovação.	IN-MP/CGU, Art. 11, IV e II; e Art. 16, III a VI; INTOSAI GOV 9130/2007, 2.7.3. ISO 31000:2009, 5.2. COSO GRC 2004, 2, 8 e 10; COSO GRC PE 2016, Princípios 3, 5, 20.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
ESTRUTURA DE GERENCIAMENTO DE RISCOS E CONTROLES			
Questão 1.3.2 Os grupos de pessoas que integram as três linhas de defesa na estrutura de gerenciamento de riscos e controles por toda a organização têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização, especialmente quanto aos seguintes aspectos:	Critério	Avaliação	Descrição
a) Na **primeira linha de defesa,** os gestores: I. têm plena consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes; e II. são regularmente capacitados para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema.	IN-MP/CGU Nº 1/2016, Art. 2º, III; e Art. 3º; IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.

b) Na **segunda linha de defesa**, o pessoal que integra funções de coordenação de atividades de gestão de riscos e/ou de gerenciamento de riscos específicos por toda a organização: I. apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade; II. fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos; III. define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização; IV. estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos; V. orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la; VI. comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização.	IN-MP/CGU Nº 1/2016, Art. 2º, III; e Art. 6º; IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
c) Na **terceira linha de defesa**, o pessoal que integra a auditoria interna, especialmente o dirigente dessa função: I. tem conhecimento dos papéis fundamentais que a função de auditoria interna deve assumir em relação ao gerenciamento de riscos, dos que não deve assumir e dos que pode assumir com salvaguardas à independência, previstos na Declaração de Posicionamento do IIA: “O papel da Auditoria Interna no gerenciamento eficaz de riscos corporativo”, e de fato exerce seus papéis em conformidade com essas orientações; II. tem compreensão clara da estratégia da organização e de como ela é executada, incluindo objetivos, metas, riscos associados e como esses riscos são gerenciados, e alinha as atividades da auditoria interna com as prioridades da organização; III. detém as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.	IN-MP/CGU Nº 1/2016, Art. 2º, III; IIA 2009, O papel da Auditoria Interna no gerenciamento de riscos corporativo. IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.	Aprimorado	Prática realizada de acordo com normas e padrões definidos na maior parte das áreas relevantes para os objetivos-chaves da organização.

	IIA IPPF Norma 2010, 2100, 2110 e 2210. RES CNJ 171/2013, Art. 10 e 12.	

5.2 Dimensão “Processos”

2. PROCESSOS	Índice de Maturidade da Dimensão	
Nesta dimensão, examinam-se 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.	**Inicial**	**9%**

A seguir, temos o detalhamento das capacidades da dimensão:

2.1. Identificação e análise de riscos	Índice de Maturidade desta Seção	
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.	Básico	30%

ESTABELECIMENTO DO CONTEXTO			
Questão 2.1.1			
O processo de identificação de riscos é precedido de uma etapa de estabelecimento do contexto envolvendo o entendimento, por parte de todos os participantes do processo, da organização, dos seus objetivos-chaves e do ambiente no qual eles são perseguidos, com o fim de obter uma visão abrangente dos fatores internos e externos que podem influenciar a capacidade da organização de atingir seus objetivos, incluindo:	Critério	Avaliação	Descrição

a) a identificação dos objetivos-chaves da atividade, do processo ou do projeto objeto da identificação e análise de riscos é realizada considerando o contexto dos objetivos-chaves da organização como um todo, de modo a assegurar que os riscos significativos do objeto sejam apropriadamente identificados;	IN-MP/CGU Nº 1/2016, Art. 8º, VI Art. 16, II ISO 31000:2009 5.3.3, "a" e "b" COSO GRC 2004 3; COSO GRC PE 2016, Princípio 10.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
b) a identificação das partes interessadas (internas e externas), bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, de modo a incluir essas partes interessadas em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta; e	IN-MP/CGU Nº 1/2016, Art. 22 ISO 31000:2009 5.3.2 e 5.3.3 COSO GRC 2004 3; COSO GRC PE 2016, 1, item 1.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
c) a comunicação e consulta com partes interessadas (internas e externas) para assegurar que as suas visões e percepções, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração no processo de gestão de riscos;	IN-MP/CGU Nº 1/2016, Art. 22 ISO 31000:2009 5.2. COSO GRC PE 2016, Princípio 20.	Inexistente	Prática inexistente, não implementada ou não funcional.
DOCUMENTAÇÃO DO ESTABELECIMENTO DO CONTEXTO Questão 2.1.2 A documentação da etapa de estabelecimento do contexto inclui pelo menos os seguintes elementos essenciais, para viabilizar um processo de avaliação de riscos consistente:	Critério	Avaliação	Descrição
a) a descrição concisa dos objetivos-chaves e dos fatores críticos para que se tenha êxito (ou fatores críticos para o sucesso) e uma análise dos fatores do ambiente interno e externo (por exemplo, análise SWOT);	ISO 31000:2009, 5.3.4, 5.3.5 e 5.7	Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
b) a análise de partes interessadas e seus interesses (por exemplo, análise de stakeholder, análise RECI, matriz de responsabilidades); e		Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.

c) os critérios com base nos quais os riscos serão analisados, avaliados e priorizados (como serão definidos a probabilidade e o impacto; como será determinado se o nível de risco é tolerável ou aceitável; quais os critérios de priorização para análise, avaliação e tratamento dos riscos identificados).		Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
IDENTIFICAÇÃO E ANÁLISE DOS RISCOS Questão 2.1.3 Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos, notadamente quanto aos seguintes aspectos:	Critério	Avaliação	Descrição
a) são envolvidas pessoas com conhecimento adequado, bem como os gestores executivos das respectivas áreas;	ISO 31000:2009 5.4.2 e A.3.2.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
b) são utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de risco;	ISO 31000:2009 5.4.2 .	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
c) O processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e outros atos impróprios, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos;	ISO 31000:2009 5.4.2; COSO 2013 Princípio 8.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
d) O processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto;	IN-MP/CGU 1/2016, Art. 16, III; ISO 31000:2009, 5.4.2.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
e) A seleção de iniciativas estratégicas, novos projetos e atividades também têm os riscos identificados e analisados, incorporando-se ao processo de gestão de riscos; e	IN-MP/CGU 1/2016, Art. 14, IV ISO 31000:2009, 3 “b”.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.

f) Os riscos identificados são analisados em termos de probabilidade de ocorrência e de impacto nos objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos.	IN-MP/CGU, Art 16, IV ISO 31000:2009 5.4.3.	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.
DOCUMENTAÇÃO DA IDENTIFICAÇÃO E ANÁLISE DE RISCOS Questão 2.1.4 No registro de riscos, a documentação da identificação e análise de riscos contém elementos suficientes para apoiar o adequado gerenciamento dos riscos, incluindo pelo menos:	Critério	Avaliação	Descrição
a) o registro dos riscos identificados e analisados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto;	ISO 31000:2009, 5.4.2, 5.4.3 e 5.7.	Inexistente	Prática inexistente, não implementada ou não funcional.
b) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise de riscos;		Inexistente	Prática inexistente, não implementada ou não funcional.
c) os participantes das atividades de identificação e análise;		Inexistente	Prática inexistente, não implementada ou não funcional.
d) a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas;		Inexistente	Prática inexistente, não implementada ou não funcional.
e) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos;		Inexistente	Prática inexistente, não implementada ou não funcional.

f) os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco;		Inexistente	Prática inexistente, não implementada ou não funcional.
g) a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade; e	ISO 31000:2009, 5.5.1	Inexistente	Prática inexistente, não implementada ou não funcional.
h) o risco residual.	ISO 31000:2009, 5.5.1	Inexistente	Prática inexistente, não implementada ou não funcional.
2.2. Avaliação e Resposta a riscos			**Índice de Maturidade desta Seção**
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.			Inicial 0%
CRITÉRIOS PARA PRIORIZAÇÃO DE RISCOS **Questão 2.2.1** Os critérios estabelecidos para priorização de riscos levam em conta, por exemplo, a significância ou os níveis e tipos de risco, os limites de apetite a risco, as tolerâncias a risco ou variações aceitáveis no desempenho, os níveis recomendados de atenção, critérios de comunicação a instâncias competentes, o tempo de resposta requerido, revelando-se adequados para orientar decisões seguras quanto a:	Critério	Avaliação	Descrição
a) se um determinado risco precisa de tratamento e a prioridade para isso;	IN-MP/CGU 1/2016, Art. 16, V; ISO 31000:2009, 5.4.4; COSO GRC 2004, 6;	Inexistente	Prática inexistente, não implementada ou não funcional.

b) se uma atividade deve ser realizada, reduzida ou descontinuada; e	COSO GRC PE 2016, Princípio 14.	Inexistente	Prática inexistente, não implementada ou não funcional.
c) se controles devem ser implementados, modificados ou apenas mantidos.		Inexistente	Prática inexistente, não implementada ou não funcional.

AVALIAÇÃO E SELEÇÃO DAS RESPOSTA A RISCOS **Questão 2.2.2**	Critério	Avaliação	Descrição
A avaliação e a seleção das respostas a serem adotadas para reduzir a exposição aos riscos identificados considera a relação custo-benefício na decisão de implementar atividades de controle ou outras ações e medidas, além de controles internos, para mitigar os riscos.	IN-MP/CGU 1/2016, Art. 14, III ISO 31000:2009 5.5.2; COSO GRC PE 2016, Princípio 15.	Inexistente	Prática inexistente, não implementada ou não funcional.

Questão 2.2.3	Critério	Avaliação	Descrição
Todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento, bem como são formalmente comunicados das ações de tratamento decididas, para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas.	IN-MP/CGU 1/2016, Art. 20 ISO 31000:2009 5.5.2 e A.3.2;	Inexistente	Prática inexistente, não implementada ou não funcional.

PLANOS E MEDIDAS DE CONTINGÊNCIA **Questão 2.2.4**	Critério	Avaliação	Descrição
Todas as áreas, funções e atividades relevantes (unidades, departamentos, divisões, processos, projetos) para a realização dos objetivos-chaves da organização têm identificados os elementos críticos de sua atuação e têm definidos planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos seus serviços em casos de desastres.	IN-MP/CGU 1/2016, Art. 16, VI ISO 31000:2009, 5.5.3.	Inexistente	Prática inexistente, não implementada ou não funcional.

DOCUMENTAÇÃO DA AVALIAÇÃO E SELEÇÃO DE RESPOSTAS A RISCOS

Questão 2.2.5			
A documentação da avaliação e seleção de respostas aos riscos inclui:	Critério	Avaliação	Descrição
a) o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos da organização, que identifica claramente os riscos que requerem tratamento, suas respectivas classificações (probabilidade, impacto, níveis de risco etc.), a ordem de prioridade para cada tratamento;	ISO 31000:2009, 5.5.3 e 5.7.	Inexistente	Prática inexistente, não implementada ou não funcional.
b) as respostas a riscos selecionadas e as razões para a seleção das opções de tratamento, incluindo a justificativa de custo-benefício; as ações propostas, os recursos requeridos, o cronograma e os benefícios esperados;		Inexistente	Prática inexistente, não implementada ou não funcional.
c) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; e		Inexistente	Prática inexistente, não implementada ou não funcional.
d) os responsáveis pela aprovação e pela implementação do plano de tratamento de riscos, com autoridade suficiente para gerenciá-lo.		Inexistente	Prática inexistente, não implementada ou não funcional.

2.3. Monitoramento e comunicação	**Índice de Maturidade desta Seção**
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	Inicial 5%

INFORMAÇÃO E COMUNICAÇÃO

Questão 2.3.1

As atividades de informação e comunicação estão estabelecidas em diretrizes e protocolos efetivamente aplicados durante o processo de gerenciamento de riscos:	Critério	Avaliação	Descrição

a) diretrizes e protocolos estão estabelecidos para viabilizar o compartilhamento de informações sobre riscos e a comunicação clara, transparente, tempestiva, relevante e recíproca entre pessoas e grupos de profissionais no âmbito da organização, para que se mantenham informados e habilitados para exercer suas responsabilidades no gerenciamento de riscos; e	IN-MP/CGU 1/2016, Art. 16, VII; ISO 31000:2009, 5.2 e A.3.4; COSO GRC 2004, 8; COSO GRC PE 2016, Princípio 20.	Inexistente	Prática inexistente, não implementada ou não funcional.
b) há efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos.	ISO 31000:2009, 5.2 e A.3.4.	Inexistente	Prática inexistente, não implementada ou não funcional.
SISTEMA DE INFORMAÇÃO **Questão 2.3.2** A gestão de riscos é apoiada por um registro de riscos ou sistema de informação que:	Critério	Avaliação	Descrição
a) apoia a gestão de riscos da organização e facilita a comunicação entre pessoas e grupos de profissionais com responsabilidades sobre o processo de gestão de riscos, permitindo uma visão integrada das atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, incluindo a sua documentação; e	ISO 31000:2009, 5.7.	Inexistente	Prática inexistente, não implementada ou não funcional.
b) é mantido atualizado pelas diversas pessoas e funções que têm responsabilidades pela gestão de riscos em todas as áreas da organização, tanto em função das decisões e ações implementadas em todas as etapas do processo de gestão de riscos, quanto pelas atividades de monitoramento e correção de deficiências (tratadas a seguir), pelo menos quanto aos seus resultados e com referências para a documentação original completa.	ISO 31000:2009, 5.7 e 5.6 (final).	Inexistente	Prática inexistente, não implementada ou não funcional.
MONITORAMENTO CONTÍNUO E AUTOAVALIAÇÕES **Questão 2.3.3** Em todos os níveis da organização, os gestores que têm propriedade sobre riscos (primeira linha de defesa) monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade:	Critério	Avaliação	Descrição
a) de modo contínuo, ou pelo menos frequente, por meio de indicadores-chaves de risco, indicadores-chaves de desempenho e verificações rotineiras, para manter riscos e resultados dentro das tolerâncias a riscos definidas ou variações aceitáveis no desempenho;	IN-MP/CGU Nº 1/2016, Art. 11, V; Art. 16, VIII; ISO 31000:2009, 5.6; COSO 2013,	Inexistente	Prática inexistente, não implementada ou não funcional.

b) por meio de autoavaliações periódicas de riscos e controles (Control and Risk Self Assessment – CRSA), que constam de um ciclo de revisão periódica estabelecido; e	Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.,	Inexistente	Prática inexistente, não implementada ou não funcional.
c) a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança.		Inexistente	Prática inexistente, não implementada ou não funcional.

Questão 2.3.4 As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha de defesa):	Critério	Avaliação	Descrição
a) exercem uma supervisão efetiva dos processos de gerenciamento de riscos, inclusive das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa; e	IN-MP/CGU Nº 1/2016, Art. 11, V; Art. 16, VIII; ISO 31000:2009, 5.6; COSO 2013, Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.,	Inexistente	Prática inexistente, não implementada ou não funcional.
b) fornecem orientação e facilitação na condução das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa, mantém sua documentação e comunica os seus resultados às instâncias apropriados da administração e da governança.		Inexistente	Prática inexistente, não implementada ou não funcional.

MONITORAMENTO PERÍODICO E AVALIAÇÕES INDEPENDENTES **Questão 2.3.5** A função de auditoria interna exerce o seu papel de auxiliar 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, controle e governança:	Critério	Avaliação	Descrição
a) estabelece planos anuais ou plurianuais baseados em riscos, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança;	IIA IPPF Norma 2010, 2100 e 2110. RES CNJ 171/2013, Art. 10 e 12.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.

b) utiliza abordagem baseada em risco ao definir o escopo e planejar a natureza, época e extensão dos procedimentos de auditoria em seus trabalhos, incluindo a identificação e análise dos riscos e o exame de como eles são gerenciados pela gestão da área responsável; e	IIA IPPF Norma 2201 e 2210. RES CNJ 171/2013, Art. 24.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.
c) fornece asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gestão de riscos e controle operam de maneira eficaz e que os riscos significativos são gerenciados adequadamente em todos os níveis da organização.	IIA 2009, O papel da Auditoria Interna no gerenciamento de riscos corporativo.	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.

Questão 2.3.6	Critério	Avaliação	Descrição
Há planos e as medidas de contingência definidos para os elementos críticos da atuação da entidade, em todos as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização e estes são periodicamente testados e revisados.	ISO 31000:2009 5.6.	Inexistente	Prática inexistente, não implementada ou não funcional.

MONITORAMENTO DE MUDANÇAS SIGNIFICATIVAS

Questão 2.3.7	Critério	Avaliação	Descrição
Estão estabelecidos e em funcionamento procedimentos e protocolos para monitorar e comunicar mudanças significativas nas condições que possam alterar o nível de exposição a riscos e ter impactos significativos na estratégia e nos objetivos da organização.	COSO 2013 Princípio 9 COSO GRC 2004 9; COSO GRC PE 2016, Princípio 22.	Inexistente	Prática inexistente, não implementada ou não funcional.

CORREÇÃO DE DEFICIÊNCIAS E MELHORIA CONTÍNUA

Questão 2.3.8 Os resultados das atividades de monitoramento são utilizados para as tomadas de medidas necessárias à correção de deficiências e à melhoria contínua do desempenho da gestão de riscos, incluindo, por exemplo:	Critério	Avaliação	Descrição

a) comunicação às instâncias apropriados da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias; e	IN-MP/CGU 1/2016, Art. 8º, XV; ISO 31000:2009, 4.5, 4.6 e A.3.1; COSO 2013, Princípio 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 23.	Inexistente	Prática inexistente, não implementada ou não funcional.
b) elaboração e devido acompanhamento de planos de ação para corrigir as deficiências identificadas e melhorar o desempenho da gestão de riscos.		Inexistente	Prática inexistente, não implementada ou não funcional.

5.3 Dimensão "Parcerias"

3. PARCERIAS	Índice de Maturidade da Dimensão	
Nesta dimensão, examinam-se 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.	**Inicial**	**0%**

A seguir, temos o detalhamento das capacidades da dimensão:

3.1. Gestão de riscos em parcerias	Índice de Maturidade desta Seção	
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.	Inicial	0%

AVALIAÇÃO DA CAPACIDADE DE GESTÃO DE RISCOS DE ENTIDADES PARCEIRAS Questão 3.1.1	Critério	Avaliação	Descrição
O compartilhamento dos riscos é precedido de avaliação fundamentada e documentada da capacidade das potenciais organizações parceiras para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado.	ISO 31000:2009, 4.3.3 e A.3.3;	Inexistente	Prática inexistente, não implementada ou não funcional.

DEFINIÇÃO DE RESPONSABILIDADES, INFORMAÇÃO E COMUNICAÇÃO Questão 3.1.2	Critério	Avaliação	Descrição
É aplicado o processo de gestão de riscos para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado das políticas de gestão compartilhadas.	IN-MP/CGU Nº 1/2016, Art. 20 e 16, VII; ISO 31000:2009, 4.3.3 e A.3.2.	Inexistente	Prática inexistente, não implementada ou não funcional.
PROCESSO DE GESTÃO DE RISCOS PARCERIAS Questão 3.1.3	Critério	Avaliação	Descrição
O processo de gestão de riscos é aplicado para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado pretendido das políticas de gestão compartilhadas.	ISO 31000:2009, 4.4.2;	Inexistente	Prática inexistente, não implementada ou não funcional.
Questão 3.1.4	Critério	Avaliação	Descrição
Pessoas de todas as áreas, funções ou setores das organizações parceiras com envolvimento na parceria e outras partes interessadas no seu objeto participam do processo de identificação e avaliação dos riscos relacionados a cada objetivo, meta ou resultado esperado das parcerias.	ISO 31000:2009, 5.4.2 e A.3.2.	Inexistente	Prática inexistente, não implementada ou não funcional.
Questão 3.1.5	Critério	Avaliação	Descrição
Um registro de riscos único é elaborado na identificação e avaliação dos riscos e é atualizado conjuntamente pelas organizações parceiras em função das atividades de monitoramento.	ISO 31000:2009, 5.7 e 5.6 (final).	Inexistente	Prática inexistente, não implementada ou não funcional.
Questão 3.1.6	Critério	Avaliação	Descrição

Há informação regular e confiável para permitir que cada organização parceira monitore os riscos e o desempenho em relação a cada objetivo, meta ou resultado esperado.	IN-MP/CGU Nº 1/2016, Art. 16, VII; ISO 31000:2009, 5.2 e A.3.4; COSO GRC PE 2016, Princípio 20	Inexistente	Prática inexistente, não implementada ou não funcional.
3.2. Planos e medidas de contingência			**Índice de Maturidade desta Seção**
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.			Inicial 0%
Questão 3.2.1	Critério	Avaliação	Descrição
As organizações parceiras definem planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços em casos de desastres ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar.	IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.6.	Inexistente	Prática inexistente, não implementada ou não funcional.
Questão 3.2.2	Critério	Avaliação	Descrição
Os planos e medidas de contingência são periodicamente testados e revisados.	IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.6.	Inexistente	Prática inexistente, não implementada ou não funcional.

5.4 Dimensão “Resultados”

4. RESULTADOS	**Índice Maturidade da Dimensão**
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.	**Inicial 0%**

A seguir, temos o detalhamento das capacidades da dimensão:

4.1. Melhoria dos processos de governança			**Índice de Maturidade desta Seção**
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.			Inicial 0%
INTEGRAÇÃO DA GESTÃO DE RISCOS AOS PROCESSOS ORGANIZACIONAIS			
Questão 4.1.1	Critério	Avaliação	Descrição
Os responsáveis pela governança e a alta administração sabem até que ponto a administração estabeleceu uma gestão de riscos eficaz, integrada e coordenada por todas as áreas, funções e atividades relevantes e críticas para a realização dos objetivos-chaves do progresso das ações em curso para atingir ao nível almejado.da organização, tendo consciência do nível de maturidade atual e	IN-MP/CGU Nº 1/2016, Art. 8º, II; Arts. 19, 20, 21, parágrafo único, 22 e 23; ISO 31000:2009, 4.3.4 e A.3.5; COSO GRC 2004, 10. COSO GRC PE 2016, Princípio 1.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.
Questão 4.1.2	Critério	Avaliação	Descrição
Os objetivos-chaves, que traduzem o conjunto de valores a serem gerados, preservados e/ou entregues à sociedade estão identificados e refletidos na cadeia de valor, na missão e visão e da organização e nos seus valores fundamentais, formando a base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios.	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 3 “a” e 5.3.1; COSO GRC 2004, Premissa; COSO GRC PE 2016, Premissa.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.
Questão 4.1.3	Critério	Avaliação	Descrição

Os objetivos estratégicos e de negócios estão estabelecidos, alinhados com o direcionamento estratégico (item anterior), juntamente com as medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho), permitindo medir o progresso e monitorar o desempenho de todas as áreas, funções e atividades relevantes da organização para a realização dos seus objetivos-chaves.	IN-MP/CGU Nº 1/2016, Art. 16, II; ISO 31000:2009, 4.2, itens 3 e 4; COSO GRC 2004, 3. COSO GRC PE 2016, Dimensão 2.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.

Questão 4.1.4	Critério	Avaliação	Descrição
Estão identificados, avaliados e sob tratamento e monitoramento os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, com o desempenho sendo comunicado aos níveis apropriados da administração e da governança.	IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, A.2 e A.3.2. COSO GRC 2004, 4; COSO GRC PE 2016, Princípios 12 a 16.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.

4.2. Resultados-chave da gestão de riscos	**Índice de Maturidade da Seção**
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.	Inicial 0%

ENTENDIMENTO DOS OBJETIVOS, RISCOS, PAPÉIS E RESPONSABILIDADES

Questão 4.2.1	Critério	Avaliação	Descrição
Os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos.	ISO 31000:2009, A.2.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.

GARANTIA PROPORCIONADA PELA GESTÃO DE RISCOS

Questão 4.2.2

Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, que:	Critério	Avaliação	Descrição
a) entendem até que ponto os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chaves da organização;	COSO GRC 2004, 1, Anexo 1.1.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.
b) entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados;		Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.
c) a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável; e		Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.
d) as leis e os regulamentos aplicáveis estão sendo cumpridos.		Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.

EFICÁCIA DA GESTÃO DE RISCOS

Questão 4.2.3	Critério	Avaliação	Descrição
Os riscos da organização estão dentro dos seus critérios de risco, vale dizer, dentro do apetite a risco definido e das variações aceitáveis no desempenho ou tolerâncias a risco estabelecidas, conforme a documentação resultante da aplicação do processo de gestão de risco, atualizada pelas atividades de monitoramento.	ISO 31000:2009, A.2.	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.

Documento Digitalizado Público

Relatório Final de Auditoria 02/2022 - Gestão de riscos

Assunto: Relatório Final de Auditoria 02/2022 - Gestão de riscos
Assinado por: Vitor Menezes
Tipo do Documento: Relatório
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Joao Vitor Miranda de Menezes**, **CHEFE - FG1 - OA-AUDIN**, em 01/12/2022 09:28:02.

Este documento foi armazenado no SUAP em 01/12/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 521212
Código de Autenticação: 523ae0ee7f