SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
AUDITORIA INTERNA – AUDINT

RELATÓRIO DE AUDITORIANº 001/2018– AVALIAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS NO IFS.

ARACAJU/SE, ABRIL DE 2018.

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
AUDITORIA INTERNA – AUDINT

RELATÓRIO DE AUDITORIA Nº:
001/2018

ÁREA:
GESTÃO OPERACIONAL

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
AUDITORIA INTERNA – AUDINT

SUMÁRIO

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
AUDITORIA INTERNA – AUDINT

LISTA DE QUADROS

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
AUDITORIA INTERNA – AUDINT

LISTA DE TABELAS

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
AUDITORIA INTERNA – AUDINT

LISTA DE FIGURAS

1 - INTRODUÇÃO

O presente Relatório de Auditoria refere-se aos resultadosdos trabalhos realizados na área de Gestão Operacional, mais precisamente na Gestão de Riscos do IFS, em consonância com o disposto no item 5.1 do Plano Anual de Auditoria Interna – PAINT/2018.

A Ação foi deflagrada por meio do Memorando Eletrônico nº 019/2018/AUDINT, em 29/01/2018 e os trabalhos realizados por dois auditores perduraram até 24/04/2018, totalizando 460 horas junto ao Departamento de Gestão de Riscos e Controle – DGR, no intuito de examinar as capacidades existentes em termos de liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho do IFS no cumprimento de sua missão institucional e em conformidade com a Instrução Normativa Conjunta MP/CGU n° 01, de 10 de maio de 2016.

Para subsídio aos trabalhos de auditoria, a equipe realizou reunião na qual estavam presentes a chefe do Departamento de Gestão de Riscos – DGRe a coordenadora da Coordenadoria de Planejamento – COPLAN. Após esta reunião foram expedidas Solicitações de Auditoria (SA's) demandando informações e documentos dos setores envolvidos na implantação da gestão de riscos do IFS.

Os trabalhos conclusivos foram realizados por meio de análise documental, confronto de informações, consolidação de informações recolhidas e indagações escritas, em estrita observância às normas de Auditoria Interna, em especial às aplicáveis ao Serviço Público Federal.

Finalizada a execução dos procedimentos de auditoria, foi possível elaborar o relatório preliminar contendo as constatações identificadas durante os trabalhos, bem como possíveis recomendações a serem adotadas pelo gestor para dirimir as falhas apontadas. Tal relatório foi apresentado aos gestores da Prodin e Reitoria durante a reunião de busca conjunta de soluções realizada no dia 10/04/2018, com o objetivo de debater as constatações identificadas durante a realização dos trabalhos da Audint.

Após a realização da reunião de busca conjunta de soluções, a Prodin e a Reitoria enviaram sua manifestação quando às constatações apresentadas no Relatório Preliminar.

Finalmente, após análise da manifestação dos gestores, foi possível finalizar a execução da Ação por meio do presente Relatório de Auditoria.

1.1 – Objetivos da Ação

O trabalho de auditoria teve por objetivo de **(1) determinar o nível de maturidade da gestão de riscos do IFS** e **(2) identificar os aspectos da Gestão de Riscos que necessitam ser aperfeiçoados**.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1854/1880, E-mail: audint@ifs.edu.br

Assim, para auxiliar na avaliaçãodo nível de maturidade da gestão de riscos do IFS, foram traçados objetivos específicos, descritos a seguir, para analisar as quatros dimensões(Ambiente, Processos, Parcerias e Resultados) estabelecidas pelo Modelo de Avaliação da Maturidade Organizacional em Gestão de Riscos desenvolvido pelo TCU, conforme Portaria-SEGECEX TCU nº 2/2018:

a) Avaliar, sob a ótica da dimensão "**Ambiente**", **as capacidades existentes no IFS** em termos de (1) **liderança**, (2) **políticas e estratégias** e de (3) **preparo das pessoas**, **para que a gestão de riscos tenha as condições necessárias para prosperar** na Organização;

b) Avaliar, sob a ótica da dimensão "**Processos**", em que medida o IFS dispõe de um modelo de processo formal, com padrões e critérios definidos para (1) **a identificação e a análise de riscos**, (2) **a avaliação de riscos** e **respostas aos riscos avaliados** e (3) **o monitoramento** e **comunicação dos riscos**;

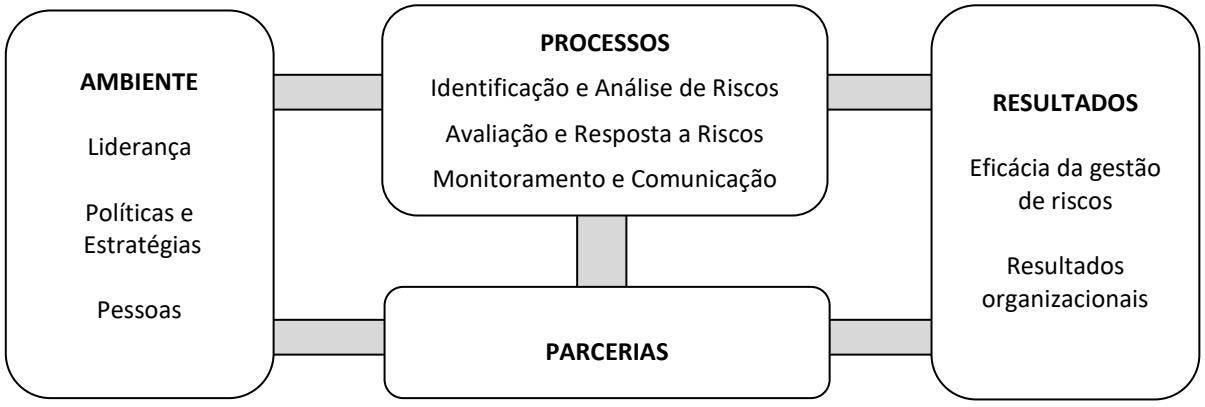
c) Avaliar, sob a ótica da dimensão "**Parcerias**", **em que medida o IFS estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem**, e **como se darão as trocas de informações sobre o assunto**, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento;

d) Avaliar, sob a ótica da dimensão "**Resultados**", **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.

1.2 – Metodologia do trabalho

Para determinar o nível de maturidade da gestão de riscos do IFS foi adotado o Roteiro de Avaliação de Maturidade de Gestão de Riscos desenvolvido e disponibilizado pelo TCU.Este roteiro estabelece como instrumento um questionário de avaliação de gestão de riscos com critérios definidos (Anexo I), o qual é composto por quatro dimensões, que se desdobram em certos aspectos, conforme Figura 1:

***Figura 1**- Modelo de avaliação da maturidade em gestão de riscos elaborado pelo TCU*



Fonte: TCU (2013)

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1854/1880, E-mail: audint@ifs.edu.br

O modelo adotado neste trabalho parte do princípio de que a maturidade da gestão de riscos de uma organização é determinada pelo preparo das pessoas (**ambiente**) parautilização da gestão de riscos, pela utilização dos conhecimentos nos **processos** e **parcerias**, assim como pelos **resultados** obtidos para organização.

A determinação do nível de maturidade da gestão de riscos no IFS envolveu três etapas: (1) Avaliação da maturidade dos aspectos de cada uma das quatro dimensões, (2) Determinação dos índices de maturidade de cada dimensão e (3) Determinação do nível de maturidade global da gestão de riscos. Ressalta-se que, para a realização da avaliação foi utilizada como ferramenta de apoio a "Planilha de Análise da Maturidade da Gestão de Riscos" disponibilizada pelo TCU em sua página da internet.

Para a realização da primeira etapa foi necessário que a equipe de auditoria respondesse, com base nas informações e documentos coletados durante os trabalhos, as90 questões que integram o questionário utilizado como instrumento de avaliação da maturidade da gestão de riscos, divididas entre as quatro dimensões e 10 aspectos, conforme Quadro a seguir:

***Quadro 1** - Quantitativo de questões respondidas*

Dimensão	Aspectos	Número de questões
1. Ambiente	1.1. Liderança	9
	1.2. Políticas e estratégias	13
	1.3. Pessoas	4
2. Processos	2.1. Identificação e análise de riscos	20
	2.2. Avaliação e Resposta a riscos	10
	2.3. Monitoramento e comunicação	16
3. Parcerias	3.1. Gestão de riscos em parcerias	6
	3.2. Planos e medidas de contingência	2
4. Resultados	4.1. Melhoria dos processos de governança	4
	4.2. Resultados-chaves da gestão de riscos	6
Total		**90**

Fonte: Audint

A avaliação dos auditores foi feita com base na análise do nível de implementação da prática ou característica de gestão descrita em cada questão, podendo ser classificada em "inexistente", "inicial", "básico", "aprimorado" e "avançado". Sendo atribuída uma pontuação (de zero a quatro pontos) para cada avaliação, conforme descrição constante no Quadro 2.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1854/1880, E-mail: audint@ifs.edu.br

***Quadro 2** - Escala de variação das respostas*

Critério	Avaliação	Descrição	Pontuação
1. Ambiente 2. Processos 3. Parcerias	Inexistente	Prática inexistente, não implementada ou não funcional.	0
	Inicial	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.	0,8
	Básico	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.	1,6
	Aprimorado	Prática realizada de acordo com normas e padrões definidos na maior parte das áreas relevantes para os objetivos-chaves da organização.	3,2
	Avançado	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.	4
4. Resultados	Inexistente	Não há evidências de que o resultado descrito tenha sido obtido.	0
	Inicial	Existe a percepção entre os gestores e o pessoal de que o resultado descrito tenha sido obtido em alguma medida.	0,8
	Básico	Existem indicadores definidos que mostram que o resultado descrito vem sendo obtido em grau baixo.	1,6
	Aprimorado	Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau moderado.	3,2
	Avançado	Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau elevado.	4

Fonte: Audint

A maturidade de cada aspecto foi apurada levando-se em conta o somatório de pontos do conjunto de questões que o compõe e calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível, expressando esse quociente com um número entre 0% e 100%.

$$\text{Nível de maturidade do aspecto (\%)} = \left(\frac{\text{Soma da pontuação obtida no aspecto}}{\text{Pontuação Máxima da Aspecto}} \right) *100$$

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

$$\text{Nível de maturidade da dimensão (\%)} = \left(\frac{\text{Soma da pontuação obtidanos aspectos da dimensão}}{\text{Pontuação Máxima da Dimensão}} \right) *100$$

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1854/1880, E-mail: audint@ifs.edu.br

Para determinar o nível de maturidade global da gestão de riscos do IFS, considerou-se a média ponderada dos índices de maturidade das dimensões (obtidas na segunda etapa da avaliação) pelos pesos descritos na Tabela, conforme definido no Modelo do TCU:

Tabela 1 *- Pesos das dimensões*

Dimensão	Peso
Ambiente	40
Processos	30
Parcerias	10
Resultados	20
Índice de Maturidade Global	**100**

Fonte: TCU

Por fim, o índice global derivado do cálculo da média ponderada permitiu classificar o nível de maturidade do IFS em uma das cinco faixas: Inicial, Básico, Intermediário, Aprimorado ou Avançado.

Ressalta-se que algumas questões avaliadas pelos auditores também serviram de base para identificar aspectos da Gestão de Riscos do IFS que necessitam ser aperfeiçoados, além do mais, a aplicação de técnicas de auditoria, tais como: análise documental, correlação de informações obtidas e indagação oral junto ao DGR, permitiram a identificação das constatações descritas neste Relatório.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1854/1880, E-mail: audint@ifs.edu.br

2–RESULTADOS DOS TRABALHOS

A análise das informações e documentos obtidos durante as atividades permitiu aos auditores calcular o nível de maturidade da gestão de riscos no IFS, bem como identificaraspectos da Gestão de Riscos do IFS que necessitam ser aperfeiçoados, cujo resultados e constatações serão apresentados a seguir.

2.1 – Constataçõesevidenciadas

CONSTATAÇÃO 001: Insuficiência de recursos tecnológicos e capacitação para os servidores do Departamento de Gestão de Riscos e Controles Internos.

a) Evidências:
Instrução Normativa MP/CGU nº 1/2016;
Resposta à SA 30/2018/Audint/IFS;
Deliberação nº 01-2017/ CGRC/IFS;
ISO 31000;
Memorando Eletrônico nº 42/2018/PRODIN/REI

b) Fato:

Através da SA n 30/2018 – Audint/IFS o DGRC foi questionado sobre o montante de recursos alocados, até o momento, em termos de pessoas, estruturas, sistemas de TI, programas de treinamento, métodos e ferramentas para a implantação da gestão de riscos no IFS.

Pela análise da resposta a SA 30/2018 – Audint/IFS, assim como as observações realizadas durante esta ação de auditoria, entendemos que o quantitativo de pessoal envolvido na implementação da Política de Gestão de Riscos é insuficiente diante da quantidade e complexidade das competências do departamento, uma vez que o DGRC, tem apenas um servidor lotado no departamento.

Sobre os recursos de TI no processo de implantação da Gestão de Riscos, foi informado que até o momento o IFS não utiliza sistema com esta finalidade específica. Considerando que a utilização de recursos de TI é de suma importância para que a instituição obtenha eficiência na gestão de riscos, é necessário que seja realizada pesquisa a fim de identificar soluções de TI que possam auxiliar nestas atividades. Ressaltamos que tais recursos, necessariamente, não precisam ser sistemas complexos, os quais demandam custo a administração. Deve-se pesquisar a existência ferramentas de TI que possam facilitar o trabalho de implementação da gestão de riscos no IFS.

Quanto ao conhecimento técnico sobre a gestão de riscos, foi possível perceber que, apesar dos esforços da gestão em realizar ações voltadas a sensibilização sobre o tema no IFS, o nível de conhecimento ainda é incipiente no IFS. Considerando que o DGRC é responsável, entre outras coisas, pela orientação técnica para implementação da gestão de riscos, conforme art. 20, inciso III, da Deliberação nº 01-2017/ CGRC/IFS, a seguir transcrito, faz-se necessário que os servidores que atuam neste departamento detenham os conhecimentos adequados e suficientes para realização de suas atribuições:

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

> Art. 20. Ao DGRC, departamento subordinado administrativamente à PRODIN, com atuação vinculada ao CGRC, compete:
> I - coordenar e assessorar as áreas finalísticas e de apoio na implementação das metodologias e instrumentos para viabilizar a integridade institucional e a gestão de riscos e controles internos da gestão;
> II - elaborar políticas, diretrizes, metodologias e mecanismos de gestão de integridade, riscos e controles internos da gestão e submetê-las ao CGRC;
> III - prestar orientação técnica às áreas finalísticas e de apoio sobre inovação e boas práticas em governança, integridade institucional e gestão de riscos e controles internos da gestão;
> IV - prestar orientação técnica sobre a aderência às regulamentações, leis e códigos, normas e padrões na condução das políticas e na prestação de serviços de interesse público;
> V - assessorar as áreas finalísticas e de apoio do IFS na proposição de objetivos estratégicos sobre governança, integridade institucional, riscos e controles internos da gestão;
> VI - atuar como facilitador na integração dos agentes responsáveis pela gestão integrada de riscos e controles internos da gestão e de temas correlatos;
> VII - apoiar as ações de capacitação nas temáticas: Controle, Risco, Governança e Integridade da Gestão, sugerindo e promovendo levantamentos das necessidades, oficinas e outras iniciativas sobre assuntos correlatos;
> VIII - apoiar a promoção da disseminação da cultura da integridade institucional, da gestão de riscos e controles internos da gestão; e a implementação de práticas e princípios de conduta e padrões de comportamento;
> IX – Emitir relatório consolidado, com o reporte a riscos e controles por área estratégica, projetos, programas ou conforme demanda, submetendo-o ao CGRC com respectivo parecer, sugerindo, no que couber, melhores práticas.
> X - apoiar o CGRC e os Grupos de Trabalho no cumprimento de suas competências e responsabilidades; e
> XI - praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

Neste sentido, deve ser oportunizada a capacitação dos servidores, especialmente aos que atuam na DGRC, uma vez que podem como multiplicadores, disseminar os conhecimentos sobre a gestão de riscos, além de prestar orientação técnica.

Conforme determina a ISO 31000:2009, para que a gestão de riscos de fato avance no âmbito da instituição deve ser observado a responsabilização e a capacitação dos indivíduos, além da disponibilização de recursos adequados as atividades, vejamos:

> Formas avançadas de gestão de riscos incluem uma forma de responsabilização abrangente, integralmente aceita e muito bem definida, relativa aos riscos, controles e tarefas do tratamento dos riscos. Indivíduos designados aceitam suas responsabilidades, são adequadamente qualificados, e possuem recursos adequados para verificar controles, monitorar riscos, melhorar os controles, e comunicar-se eficazmente com as partes interessadas internas e externas sobre os riscos e sua gestão. (ISO 31000:2009, A.3.2.)

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Nesta perspectiva, a IN 01/2016/MP/CGU estabelece que o Comitê de Governança, Riscos e Controles deve atuar de forma a proporcionar o suporte para que a gestão de riscos no IFS seja implementada de forma efetiva em todo o órgão, vejamos:

> Art. 23. Os órgãos e entidades do Poder Executivo federal deverão instituir, pelos seus dirigentes máximos, Comitê de Governança, Riscos e Controles.
> [...]
> § 2º São competências do Comitê de Governança, Riscos e Controles
> [...]
> IX – liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade;

Sendo assim, para que a implementação da política de gestão de riscos ocorra de forma efetiva no IFS, é necessário que sejam destinados servidores que detenham conhecimento técnico para atuarem neste setor, além promover a utilização de ferramentas de TI que possam auxiliar nas atividades relacionadas ao gerenciamento de riscos.

c) Causa:
Deficiência na fase de planejamento para criação do Departamento de Gestão de Riscos e Controles Internos do IFS.

d) Manifestação da Unidade:
Em resposta ao Relatório Preliminar de Auditoria, encaminhado através do Memorando Eletrônico nº 42/2018/AUDINT/REI, a Gestão apresentou resposta através do Memorando Eletrônico nº 42/2018/PRODIN/REI, nos seguintes termos:

A constatação e o respectivo fato ratificam indicativo de fraqueza do ambiente interno registrado no Relatório Anual das Iniciativas do DGR – Exercício 2017, de 31/01/2018 (Quadro 2, folha 8) e disponibilizado à Audint em resposta à solicitação de auditoria nº 030/2018, qual seja: "inadequação dos recursos humanos, materiais etecnológicos para o planejamento e desenvolvimento das iniciativas". Portanto, previamente reconhecido comouma vulnerabilidade que compromete a atuação do setor.

Nesse sentido, com base nas competências do departamento, esta gestão reconhece necessário definir umaestrutura de recursos para o setor de forma que viabilize seu campo de atuação. Não obstante, limitações emtermos de recursos humanos também se apliquem a outros setores do IFS, será proposta pela PRODIN umaestrutura administrativa para o DGR em termos de recursos humanos e tecnológicos, considerando ascompetências e a abrangência de atuação do setor bem como as necessidades de capacitação da eventualequipe do setor, a ser submetida oportunamente à instância decisória competente.

*Por oportuno, cumpre-nos dar ciência de que, por ordem do Mag. Reitor, a servidora A. A. S. C., matrícula 222****, ocupante do cargo de Assistente em Administração, do quadro de pessoalpermanente desta Instituição Federal de Ensino a partir do dia 11/04/2018 (quarta-feira), passou a desenvolver suas atividadesjunto ao Departamento de Gestão de Riscos, mantendo sua lotação na PRODIN, conforme Portaria nº 751 de27/03/2017.*

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Iniciativa prevista: Propor estrutura administrativa para o DGR, considerando as competências e a abrangência de atuação do setor bem como as necessidades de capacitação da eventual equipe do setor, a ser submetida à anuência do Reitor e à apreciação pelo colegiado competente.

Prazo: Até 31/07/2018

e) Análise da Manifestação:

A manifestação do gestor corrobora com o achado, uma vez que reconhece que, em análise anterior, as situações apontadas no fato desta constatação já haviam sido identificadas como fraquezas no ambiente interno da DGR.

Quanto à necessidade de realização de definição de estrutura do DGRC, esta Audint esclarece que durante a execução desta auditoria não foi analisada se a estrutura organizacional do departamento é adequada às suas atribuições, uma vez queo objetivo da auditoria não contemplava esta análise. Sendo assim, para chegarmos à conclusão sobre a necessidade de aumento no quantitativo de servidores lotados no DGRC verificou-sea quantidade e a complexidade das atribuições do DGRC, alémdo quantitativo de servidores lotados no departamento (possuindo apenas um servidor lotado no departamento).

Sobre a insuficiência de recursos humanos, o próprio gestor reconhece a carência, ao informar a existência de designação de uma nova servidora, lotada na PRODIN, para atuar prestando suporte ao DGRC, corroborando com o achado de auditoria. Entendemos que a designação de uma nova servidora para atuar junto ao DGRC reflete o comprometimento do gestor em viabilizar a realização dos trabalhos do departamento. Sendo assim, com a designação esta nova servidora, afasta-se em parte o achado.

No tocante a capacitação, reforçamos a necessidade de que os servidores, especialmente da DGRC, sejam capacitados para o desempenho das atividades relacionadas a gestão de riscos. Assim como, também, salientamos sobre a importância de utilização de recursos de TI que auxiliem a atividade implementação da gestão de riscos.

f) Riscos e Efeitos:

A quantidade insuficiente de servidores para atuar na implementação da política de gestão de riscos pode levar a não implementação desta política, fazendo com que os gestores sejam responsabilizados.

Recomendação 001: (PRODIN)

Envidar esforços para que seja capacitadaa equipe que atua no Departamento de Gestão de Riscos e Controle Internos do IFS, a fim de que estes atuem como multiplicadores dos conhecimentos sobre a implantação da gestão de riscos no IFS.

Recomendação 002: (PRODIN)

Realizar uma análise sobre a utilização de soluções de TI que possam auxiliar na gestão de riscos no IFS e, caso sejam identificadas soluções viáveis, utilizá-las.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

CONSTATAÇÃO 002: Ausência de Plano de Gestão de Riscos e cronograma para a realização das atividades de implantação da gestão de riscos no IFS.

a) Evidências:

Deliberação CGRC nº 01/2017 – Política de Gestão de Riscos e Controles Internos da Gestão do IFS;

Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão (MP) de 2017;
Memorando Eletrônico nº 042/2018/PRODIN/REI.

b) Fato:

A Política de Gestão de Riscos, aprovada por meio da Deliberação n° 01/2017/CGRC/IFS, publicada em 31/01/2017, determinou que a metodologia e os instrumento para implementação da gestão riscos no IFS será descrita no Plano de Gestão de Riscos, vejamos:

> Art. 24. A descrição detalhada da metodologia e dos instrumentos complementares de que tratam o artigo 9º, incisos II e IV, bem como outros necessários à implementação do processo de gestão integrada de riscos e controles internos no IFS serão definidos no documento Plano de Gestão de Riscos - PGR, a ser elaborado em 150 (cento e cinquenta) dias, a contar da publicação desta Política.

Ocorre que, o prazo de 150 (dias) para publicação do Plano de Gestão de Riscos encerrou em 30/06/2017, porém, até a presente data, não houve a publicação deste documento.

Conforme definido na Política de Gestão de Riscos do IFS, o Plano de Gestão de Riscos deve conter a metodologia e os instrumentos a serem utilizados na gestão de riscos. Sendo assim, é de suma importância que este documento esteja aprovado, uma vez que servirá de norte para as decisões no processo de gerenciamento de riscos.

> **4.3.4 Integração nos processos organizacionais**
> Convém que exista um plano de gestão de riscos para toda a organização, a fim de assegurar que a política de gestão de riscos seja implementada e que a gestão de riscos seja incorporada em todas as práticas e processos da organização. O plano de gestão de riscos pode ser integrado em outros planos organizacionais, tais como um plano estratégico.

Ademais, com o objetivo de compreender o processo implantação da Política de Gestão de Riscos no IFS, foram realizadas consultas nas cinco deliberações expedidas pelo Comitê de Governança, Riscos e Controles – CGRC vigentes durante os trabalhos de auditoria.

Quanto à execução das iniciativas de implantação da gestão de riscos, o §1º do art. 23 da Deliberação CGRC nº 01/2017, que trata da Política de Gestão de Riscos e Controles Internos da Gestão do IFS, prevê:

> Art. 23. As iniciativas inerentes à integridade institucional e ao processo de gestão integrada de riscos e controles internos da gestão no IFS deverão ser realizadas em ciclos, em períodos não superiores a 2 (dois) anos, com base nos processos finalísticos e

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

> de apoio a serem priorizados em decisão colegiada, em função da complexidade e abrangência dos temas afetos às iniciativas de boas práticas de gestão.
>
> § 1° As práticas em integridade institucional, governança e gestão de riscos e controles de gestão a serem promovidas no biênio 2017-2018 identificarão a fase de implementação do processo de integração, ciclo inicial do processo de maturidade institucional sobre as temáticas, em cujo período serão estabelecidos os níveis toleráveis de exposição a riscos das áreas finalísticas e de apoio.

Contudo, não foi identificado a existência de um cronograma para aplicação da metodologia de gerenciamento dos riscos, inclusive no que diz respeito ao mapeamento e a aplicação do Método de Priorização dos processos, definindo prazos para a realização de cada uma das etapas e os respectivos responsáveis pela realização.

Neste sentido, o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão (MP) trouxe, em suas considerações finais, a seguinte conclusão:

> Por fim, ressalta-se que **o levantamento e gerenciamento de riscos devem fazer parte dos processos das unidades**, **assim, é necessário elaborar cronograma para a realização dos trabalhos**, **observados os prazos institucionais**, e submeter às instâncias para aprovação e acompanhamento. (Grifo nosso)

Assim, para que haja a implantação da Gestão de Riscos no IFS, bem como seu acompanhamento pelas instâncias responsáveis, é imprescindível a elaboração do Plano de Gestão de Riscos e um cronograma dos principais atores envolvidos nessas atividades, desde a sensibilização dos gestores sobre a temática de gestão de riscos, mapeamento e priorização dos processos até a aplicação da metodologia de gestão de riscos e controles.

c) Causa

Falha no planejamento quando da estipulação do prazo para elaboração e aprovação do Plano de Gestão de Riscos.

d) Manifestação da Unidade:

Em resposta ao Relatório Preliminar de Auditoria, encaminhado através do Memorando Eletrônico nº 42/2018/AUDINT/REI, a Gestão apresentou resposta através do Memorando Eletrônico nº 42/2018/PRODIN/REI, nos seguintes termos:

Embora prevista para realização até 30/06/2017, a elaboração do Plano de Gestão de Riscos do IFS –instrumento de apoio à implementação da Política de Gestão de Riscos e Controles Internos, dependeria dedeliberações prévias, algumas das quais foram promovidas no segundo semestre de 2017 e outras estão emandamento. Nesse propósito, foram definidas, por exemplo, as naturezas e categorias de riscos a serem geridasno IFS (Deliberação nº 03/2017/DGRC/IFS) bem como os parâmetros da Matriz de Riscos do órgão (Deliberaçãonº 04/2017/DGRC/IFS), as quais passaram a vigorar a partir de 10/11/2017, ou seja, após o prazo estimadopara formalização do plano.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Destaca-se que o Relatório Anual das Iniciativas do DGR – Exercício 2017, disponibilizado à Audint nessa ação, sinaliza essa dependência ao informar que "houve a necessidade de substituição de instrumentos e técnicas deapoio, em razão da prioridade dos institucionalizados em relação aos previstos inicialmente" (subitem 1.2.3.página 5). Ressalta-se que a formalização desse instrumento de apoio se encontra previsto no plano de ação doDGR – exercício 2018 (plano em processo de registro no Geplanes), item 2.2 Desenvolvimento eaperfeiçoamento de instrumentos de apoio à implantação da gestão de riscos, cuja ferramenta deverácontemplar, no que couber, cronograma de realização do plano.

Iniciativa prevista: Formalizar o Plano de Gestão de Riscos estabelecendo, no que couber, cronograma para aimplementação da gestão de riscos no IFS.

Prazo: Até 31/12/2018.

e) Análise da Manifestação:

A manifestação do gestor corrobora com o achado, uma vez que reconhece que o prazo para aprovação do Plano de Gestão de Riscos estabelecido na Política de Gestão de Riscos e Controles Internos da Gestão do IFS, art. 23, expirou sem que houvesse ocorrido a aprovação do referido plano. Assim como, também, informou que está prevista no plano de ação da DGRC para o exercício 2018, a formalização do Plano de Gestão de Riscos.Sendo assim, mantêm-se a constatação em todos os seus termos.

Ressaltamos que o Plano de Ação é uma ferramenta importante para a gestão das atividades a serem desenvolvidas na implementação da Política de Gestão de riscos,esta ferramenta possibilita que o servidor siga uma sequência de tarefas logicamente encadeada, permitindo a concretização dos objetivos de forma mais rápida e prática. Além disso, o Plano de Ação permitirá ao Comitê de Gestão de Riscos e Controle acompanhar as atividades do DGRC.

f) Riscos e Efeitos:

A ausência do Plano de Gestão de Riscos poderá dificultar a execução da implementação da política de gestão de riscos, o que poderá levar a não implementação da gestão de risco do IFS de forma adequada.

Recomendação 001: (PRODIN)

Elaborar e formalizar o Plano de Gestão de Riscos do IFS, conforme estabelecido na Política de Gestão de Riscos.

Recomendação 002: (PRODIN)

Elaborar um plano de ação com a previsão do cronograma e indicação de responsáveis pelas atividades relacionadas com a implementação da política de gestão de riscos no IFS e encaminhá-lo ao CGRC para ciência.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

CONSTATAÇÃO 003: Ausência da formalização da estrutura de governança do IFS.

a) Evidências:
Instrução Normativa MP/CGU nº 1/2016, art. 16, I e art. 23º, §2º, II;
Referencial Básico de Governança Pública do TCU, 2014 (Versão 2);
PGRC do IFS, art. 4º, XI e art. 17º.
Memorando Eletrônico nº 042/2018/PRODIN/REI

b) Fato:

A Instrução Normativa MP/CGU nº 1/2016 prevê, em seu art. 16, inciso I, que na implementação do modelo de gestão de riscos, a alta administração deve observar como um dos componentes da estrutura de gestão de riscos o seguinte:

> Art. 16. **Na implementação** e atualização **do modelo de gestão de riscos**, **a alta administração**, bem como seus servidores ou funcionários, **deverá observar os seguintes componentes da estrutura de gestão de riscos**:
>
> **I –ambiente interno**: inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, **estrutura de governança organizacional** e políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos;

Adicionalmente, a IN 01/2016/MPOG/CGU estabelece a competência para implementação da estrutura de governança, vejamos:

> Art. 23. Os órgãos e entidades do Poder Executivo federal deverão instituir, pelos seus dirigentes máximos, Comitê de Governança, Riscos e Controles.
> § 2o **São competências do Comitê de Governança, Riscos e Controles**:
> (...)
> II – **institucionalizar estruturas adequadas de governança**, gestão de riscos e controles internos; (Grifo nosso)

O art. 4º, XI, da Política de Gestão de Riscos e Controles do IFS traz a seguinte definição para governança:

> **XI - governança**: combinação de processos e estruturas implantadas pela alta administração do Instituto Federal de Sergipe, para informar, dirigir, administrar e monitorar suas atividades, com o intuito de alcançar os seus objetivos;

Ademais, o Referencial de Governança Pública do TCU, pg. 27 a 29 e 47, define "Sistema de Governança" do seguinte modo:

> O **sistema de governançareflete a maneira como diversos atores se organizam, interagem e procedem para obter boa governança**. Envolve, portanto, as **estruturas administrativas** (instâncias), os **processos de trabalho**, os **instrumentos** (ferramentas, documentos etc), o **fluxo de informações** e o **comportamento de pessoas** envolvidas direta, ou indiretamente, na avaliação, no direcionamento e no monitoramento da organização.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

> Além dessas instâncias, **existem outras estruturas que contribuem para a boa governança da organização**: **a administração executiva**, **a gestão tática** e a **gestão operacional**.
>
> Depreende-se daí que **o alcance de uma boa governança pela organização depende fundamentalmente da definição e implantação de um sistema de governança ao mesmo tempo simples e robusto.** (Grifo nosso)

Contudo, durante a realização dos trabalhos de auditoria, foi possível constatar que não há no IFS uma estrutura de governança organizacional formalmente definida, fato corroborado pela chefia do Departamento de Gestão de Riscos do IFS.

Considerando, ainda, que o art. 17 da Política de Gestão de Riscos do IFS, a seguir descrito,prevê queo Gestor do Processo de Gestão responde pela gestão de riscos e controle internos do processo sob sua responsabilidade, seja no nível estratégico, tático ou operacional:

> Art. 17. O Gestor de Processo de Gestão – GP é todo e qualquer responsável pela execução de um determinado processo de trabalho em cada estrutura organizacional constituída.
> Parágrafo Único. **O GP responde pela gestão de riscos e controles internos do seu processo de trabalho em nível estratégico, tático ou operacional**, ainda que não exerça titularidade de Cargo de Direção (CD) ou Função Gratificada (FG).

Sendo assim, resta clara a necessidade do estabelecimento formal do Sistema de Governança do IFS, com definições claras das instâncias e estruturas (administração executiva, gestão tática e gestão operacional), tornando possível a implementaçãodo processo gestão de riscos.

c) Causa:
Falha dos controles internos administrativos no tocante a necessidade de formalização por parte da gestãoda estrutura de governança do IFS.

d) Manifestação da Unidade:

Em resposta ao Relatório Preliminar de Auditoria, encaminhado através do Memorando Eletrônico nº 42/2018/AUDINT/REI, a Gestão apresentou resposta através do Memorando Eletrônico nº 42/2018/PRODIN/REI, nos seguintes termos:

A atuação da chefia do DGR no assessoramento às áreas de gestão no processo de autoavaliação institucional objeto do levantamento de governança integrada ciclo 2017 promovido pelo TCU e na interlocução entre o IFS e o Tribunal, ação registrada no item 2.2 do Relatório Anual das Iniciativas do DGR – Exercício 2017, de 31/01/2018, disponibilizado à Audint nessa auditoria, evidenciou a necessidade de apresentar à gestão superior um diagnóstico das áreas de gestão críticas e sugerir iniciativas de fortalecimento à governança institucional.

Nesse sentido foi elaborada pelo DGR em parceria com a Coordenadoria de Planejamento (COPLAN) e apresentada ao reitor uma avaliação preliminar com propostas de iniciativas em diferentes áreas, conforme memorando eletrônico nº 7/2018/DGR/PRODIN (em

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

anexo), dentre as quais indicou-se a institucionalização do sistema de governança do IFS, necessidade também corroborada por consulta a gestores sobre seus níveis decisórios. Quanto à apreciação pelo colegiado competente essa proposta será pauta da reunião que está prevista para a sexta-feira 13/04/2018, conforme Ofício Circular nº 001/2018/CGRC/IFS de 05/04/2018 (em anexo).

Ação em andamento: Submeter à apreciação e deliberação o modelo proposto para institucionalização do Sistema de Governança do IFS.

Prazo: Até 31/05/2018

e) Análise da Manifestação:

A manifestação do gestor corrobora com o achado, uma vez que informa arealização de ações com o objetivo de formalizar a estrutura de governança do IFS, inclusive com a apresentação de proposta de institucionalização do sistema de governança do IFS, a ser apreciada pelo Comitê de Gestão de Riscos e Controles do IFS. Pelo exposto, mantêm-se a constatação em todos os termos.

f) Riscos e Efeitos:

A ausência de definição e implantação formal de um sistema de governança no IFS pode inviabilizar a implementação da política de gestão de riscos, uma vez que não estão determinadas as instâncias responsáveis pelos processos de trabalho em nível estratégico, tático e operacional.

Recomendação 001 (PRODIN):
Realizar estudos com vistas a propor o estabelecimento formal da Estrutura de Governança do IFScomo subsídio para implementação da gestão de riscos e submeter a aprovação junto ao setor competente.

CONSTATAÇÃO 004: Ausência de diretrizes na Política de Gestão de Riscos do IFS sobre a integração entre a gestão de riscos e o planejamento estratégico, os processos e às políticas da organização.

a) Evidências:
Instrução Normativa MP/CGU nº 1/2016, art. 17, II, "a";
ISO 31000:2009, 4.3.4;
PGRC do IFS, art. 5º, XI e art. 8º.
Memorando Eletrônico nº 042/2018/PRODIN/REI

b) Fato:

O art. 17º, II, "a" da IN-MP/CGU nº 01/2016 prevê que a política de gestão de riscos a ser instituída pelos órgãos e entidades do Poder Executivo Federal deve especificar diretrizes sobre "como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização".

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Neste sentido, o item 4.3.4 da norma ABNT NBR ISO 31000 Gestão de Riscos – princípios e diretrizes, traz à tona a necessidade da integração da gestão de riscos a todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão, *in verbis*:

> **4.3.4 Integração nos processos organizacionais**
> Convém que a gestão de riscos seja incorporada em todas as práticas e processos da organização, de forma queseja pertinente, eficaz e eficiente. Convém que o processo de gestão de riscos se torne parte integrante, e nãoseparado, desses processos organizacionais. Em particular, convém que a gestão de riscos seja incorporadano desenvolvimento de políticas, na análise crítica, no planejamento estratégico e de negócios, e nos processosde gestão de mudanças.

Contudo, ao analisar a Política de Gestão de Riscos do IFS, não foram identificadas diretrizes sobre como será feita a integração da gestão de riscos com os processos organizacionais do IFS, nos termos do art. 17º, II, "a" da IN-MP/CGU nº 01/2016. Ademais, o art. 5º da PGRC limitou-se a trazer como um dos princípios da gestão de riscos o seguinte texto:

> Art. 5º As práticas e os instrumentos organizacionais da gestão de riscos e de controles internos da gestão darão suporte à integridade institucional do IFS orientados pelos seguintes princípios:
>
> XI - integração e utilização das informações e resultados gerados pela gestão riscos econtroles internos da gestão na elaboração do planejamento estratégico, na tomada dedecisões e na melhoria contínua dos processos organizacionais e de integridade;

Assim, fica constatada a ausência de diretrizes na Política de Gestão de Riscos do IFS sobre a integração entre a gestão de riscos e o planejamento estratégico, os processos e às políticas da organização.

c) Riscos e Efeitos:

A ausência de diretrizes específicas na Política de Gestão de Riscos do IFS sobre a integração da gestão de riscos com o planejamento estratégico, os processos e às políticas da organização pode prejudicar a sua implementação pelos responsáveis, tendo em vista a indefinição na própria Norma de como fazê-la.

d) Manifestação da Unidade:

Em resposta ao Relatório Preliminar de Auditoria, encaminhado através do Memorando Eletrônico nº 42/2018/AUDINT/REI, a Gestão apresentou resposta através do Memorando Eletrônico nº 42/2018/PRODIN/REI, nos seguintes termos:

Embora não explicitado no art. 8º da Política de Gestão de Riscos e Controles internos (PGRC) do IFS, o qual trata das diretrizes para a gestão de riscos, a integração de que trata a constatação está evidenciada no conteúdo do art. 2º da norma que dispõe preliminarmente que "a PGRC e seus instrumentos complementares deverão orientar a consecução do planejamento estratégico, programas, projetos e processos de trabalho das atividades finalísticas e de apoio no âmbito das unidades organizacionais do Instituto". Assim posto, uma vez que a palavra diretriz tem entre outras sinônimas, a palavra orientação, a gestão de riscos está incorporada no desenvolvimento desses elementos, portanto, a eles integrada, conforme exposto no item 4.3.4,

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

transcrito no fato desta constatação. Ainda assim, considerando a previsão de revisão da PGRC do IFS neste exercício de 2018, será incorporado da Política de Gestão de Riscos – PGR do Ministério da Transparência, Fiscalização e Controladoria-Geral da União – CGU aprovada pela Portaria nº 915 de 12/04/2017 com o objetivo de suprir a ausência constatada, nesses termos: "a Gestão de Riscos deverá estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional do IFS".
Iniciativa prevista: Indicar expressamente a integração entre a gestão de riscos e o planejamento estratégico,os processos e às políticas do IFS, quando da revisão da PGRC, nesses termos: "a Gestão de Riscos deverá estarintegrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacionaldo IFS".
Prazo: Até 31/12/2018.

e) Análise da Manifestação:

Após análise da manifestação do gestor, verificamos que, de fato, a política de gestão de risco do IFS já estabelece a necessidade de integração entre a gestão de riscos e os processos organizacionais, conforme art. 2º e art. 8º. Dessa forma, as explicações trazidas pelo gestor afastaram o achado de auditoria.

Diante disso, uma vez que se encontra formalizada a necessidade de integração entre a Política de Gestão de Riscos e os processos institucionais, cabe a Prodin envidar esforços para garantir que ocorra, efetivamente, esta integração.

CONSTATAÇÃO 005: Ausência de acompanhamento e supervisão, pelo Comitê de Governança, Riscos e Controles – CGRC, das práticas de institucionalização da Gestão de Riscos.

a) Evidências:
PGRC do IFS, art. 5º, XI e art. 8º;
Resposta do DGR à pergunta 12 da Solicitação de Auditoria nº 030/2018;
Relatório Anual de Iniciativas do DGR – Exercício de 2017.

b) Fato:

Considerando que a Política de Gestão de Riscos do IFS, em seu art. 18º, XIII, prevê como uma das competências do Comitê de Governança, Riscos e Controles – CGRC é a supervisão do modelo de gestão de riscos e controles internos da gestão, analisou-se, durante os trabalhos de auditoria, como se dava esta supervisão e a comunicação entre o Departamento de Gestão de Riscos – DGR e o CGRC, bem como a supervisão da implementação da Política da Gestão de Riscos no IFS.

Conforme resposta da chefia do DGR à pergunta 12 da Solicitação de Auditoria nº 030/2018, a comunicação entre o Departamento de Gestão de Riscos com a alta administração ocorre conforme descrito a seguir:

> **12. De que forma ocorre a comunicação entre o Departamento de Gestão de Riscos com a alta administração e demais servidores sobre o andamento da implementação da Política de Gestão de Risco?**

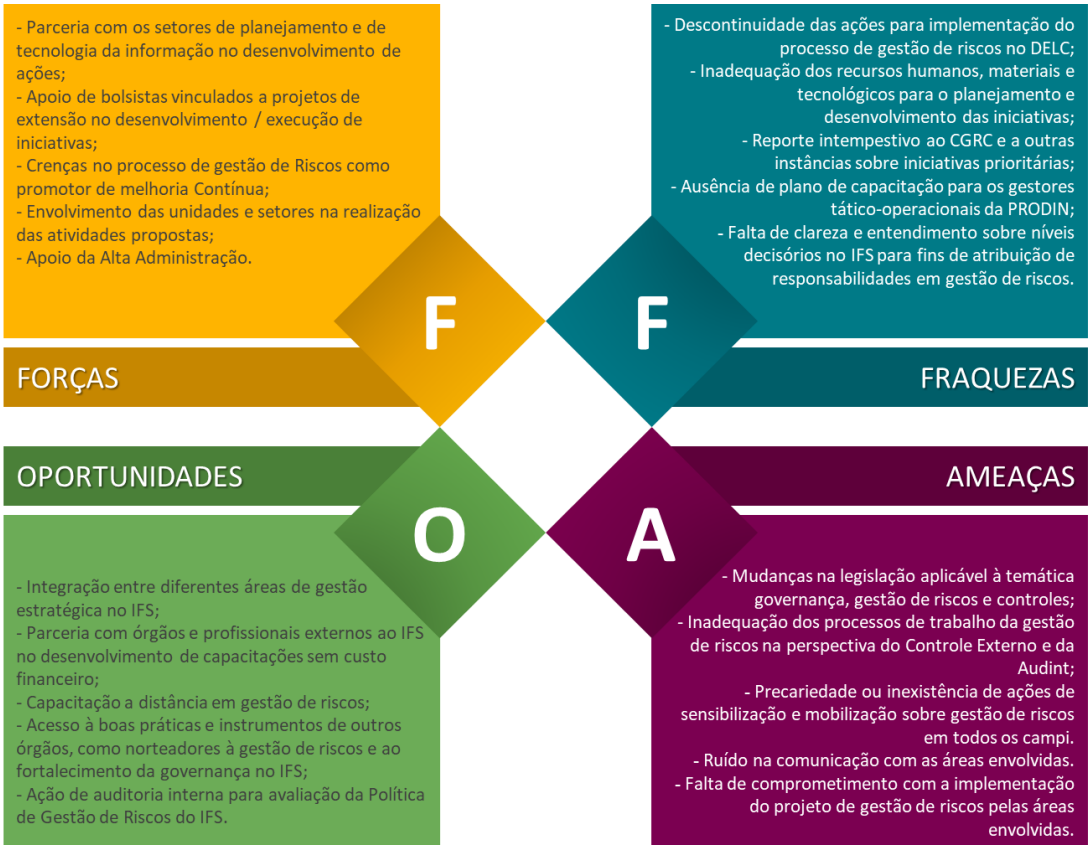
Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

A comunicação do DGR com a alta administração tem ocorrido formal e informalmente, por meio de reuniões, relatórios (físicos e virtuais), formulários de levantamento de informações, memorandos eletrônicos, telefone, *e-mails*, WhatsApp, bem como pelo uso de outras ferramentas digitais (ex.: questionários digitais, *mentimeter*).

Ademais, um dos documentos anexado à resposta enviada pelo DGR foi o Relatório Anual de Iniciativas do DGR – Exercício de 2017. Documento este que descreve as iniciativas planejadas e executadas em 2017, outras iniciativas promovidas no Exercício que não estavam contempladas inicialmente no Plano de Trabalho do Departamento, bem como os resultados alcançados por cada ação e que, conforme a chefia do DGR, foi enviado ao pró-reitor da Prodin e para o gestor máximo da Instituição, contudo, não foi apresentado ao Comitê de Governança, Riscos e Controles – CGRC, por não haver nenhuma reunião agendada.

Levando em consideração as informações e documentos obtidos durante a realização da auditoria, ratificada pela descrição do próprio DGR de suas fraquezas constantes na análise do Ambiente Interno e Externo do Relatório Anual de Iniciativas do DGR – Exercício de 2017 (conforme figura a seguir), como: (1) a descontinuidade das ações para implementação do processo de gestão de riscos no DELC, (2) o reporte intempestivo ao CGRC e a outras instâncias sobre iniciativas prioritárias e (3) a falta de clareza e entendimento sobre níveis decisórios no IFS para fins de atribuição de responsabilidades em gestão de riscos, a equipe de auditoria concluiu que o Comitê de Governança, Riscos e Controles – CGRC não vem cumprindo com as suas competências estabelecidas na PGRC, entre elas, a de supervisionar as práticas de institucionalização da Gestão de Riscos.

***Figura 2**- Análise do Ambiente Interno e Externo*



Fonte: DGR (2017)

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Assim, fica constatada a ausência de acompanhamento e supervisão, pelo Comitê de Governança, Riscos e Controles – CGRC, das práticas de institucionalização da Gestão de Riscos.

c) Causas:

Ausência de definição de estratégias para realização da supervisão, pelo Comitê de Governança, Riscos e Controles – CGRC, sobre o processo de implementação da política de gestão de riscos.

d) Manifestação da Unidade:

Em resposta ao Relatório Preliminar de Auditoria, encaminhado através do Memorando Eletrônico nº 42/2018/AUDINT/REI, a Gestão apresentou resposta nos seguintes termos:

Informamos que está sendo elaborado o plano de comunicação do CGRC onde será submetido para apreciação do mesmo e nele será estabelecido um cronograma de reuniões periódicas onde os trabalhos de institucionalização da gestão de riscos serão supervisionados.

e) Análise da Manifestação:

A manifestação do gestor corrobora com o achado, uma vez que informa que será adotado um cronograma de reuniões periódicas através das quais o Comitê de Governança, Riscos e Controles – CGRC irá supervisionar os trabalhos desenvolvido no âmbito do IFS voltados à implantação da gestão de riscos.

Ressaltamos que a realização desta supervisão é de suma importância, pois através deste procedimento será possível ao Comitê de Governança, Riscos e Controles – CGRC colaborar com a implantação da política de gestão de riscos do IFS, a qual se encontra em fase inicial. Conforme estabelecido na Política de Gestão de Riscos do IFS, cabe ao referido comitê, entre outras atribuições, apoiar a adoção de boas práticas de gestão de riscos, definir sobre ações que tenham por objetivo a disseminação da cultura da gestão de riscos, aprovar práticas, emitir e monitorar as recomendações e orientações para o aprimoramento da gestão de riscos e dos controles internos.

f) Riscos e Efeitos:

Ao considerar o importante papel do Comitê de Governança, Riscos e Controles – CGRC em apoiar governança do IFS nas iniciativas de gestão de riscos e suas competências de supervisão descritas na PGRC, tem-se que a ausência de acompanhamento, pelo CGRC, das práticas de institucionalização da Gestão de Riscos no IFS, pode impactar diretamente o andamento das atividades do DGR e de outros setores, atrasando ou até mesmo inviabilizando a sua implantação.

Recomendação 001:REITORIA (CGRC)

Supervisionar, de forma contínua, os trabalhos de institucionalização da Gestão de Riscos desenvolvidos pelo Departamento de Gestão de Riscos e pelos demais gestores responsáveis, por meio dereuniões periódicas e outras ferramentas que entenderem necessárias.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

CONSTATAÇÃO 006: Ausência de definição de objetivos táticos por parte dos gestores do IFS.

a) Evidências:
PGRC do IFS, art. 8º, I e art. 9º, II, § 1º;
Instrução Normativa MP/CGU nº 1/2016, art. 16, II;
Plano de Desenvolvimento Institucional do IFS – PDI (2014-2019), versão 1.3;
Plano de Desenvolvimento Anual do IFS – PDA (2018);
COSO – Gerenciamento de Riscos Corporativos, 2004, Estrutura "3. Fixação de Objetivos".
Memorando Eletrônico nº 142/2018/PRODIN/REI

b) Fato:

O art. 8º, I, da Política de Gestão de Riscos do IFS prevê que "a implementação da gestão de riscos e de controles internos do IFS será sistematizada e suportada pelos componentes de gestão de riscos e controle internos das metodologias do *Committee of Sponsoring Organization sof the Treadway Commission* – COSO e de boas práticas".

Ademais, a PGRC ratificaem seu art. 9º, II, §1º, que a metodologia utilizada no modelo de gestão de riscos do IFS deve observar os componentes do COSO, quais sejam: ambiente interno, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta a riscos, atividades de controles internos, informação e comunicação, emonitoramento.

Quanto ao componente "fixação de objetivos", o art. 16, II da IN-MP/CGU nº 1/2016 esclarece:

> Art. 16. **Na implementação** e atualização **do modelo de gestão de riscos**, **a alta administração, bem como seus servidores ou funcionários, deverá observar os seguintes componentes** da estrutura de gestão de riscos:
> II– fixação de objetivos: **todos os níveis da organização** (departamentos, divisões, processos e atividades) **devem ter objetivos fixados e comunicados. A explicitação de objetivos**, alinhados à missão e à visão da organização, **é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução**; (Grifo nosso)

Nessa mesma temática, o modelo COSO – Gerenciamento de Riscos Corporativos, 2004 defende:

> A fixação de objetivos é uma **precondição** à identificação de evento, à avaliação de riscos e às respostas aos riscos. **Em primeiro lugar, é necessário que os objetivos existam para que a administração possa identificar e avaliar os riscos quanto a sua realização, bem como adotar as medidas necessárias para administrá-los.**(Grifo nosso)

Contudo, ao analisar o Plano de Desenvolvimento Institucional do IFS – PDI (2014-2019), verificou-se que apenas os objetivos estratégicos foram definidos. Quanto aos objetivos táticos, a Equipe de Auditoria identificou no Plano de Desenvolvimento Anual do IFS – PDA (2018) que apenas a Diretoria de Assistência Estudantil (DIAE) e o campus Estância definiram tais objetivos. Sendo que não foram identificados objetivos operacionais de nenhuma unidade.

Assim, fica constatada a ausência de definição de objetivos táticos e operacionais por parte dos gestores do IFS.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

c) Causa

Falhas nos controles internos administrativos no tocante ao acompanhamento das informações que devem constar no PDA.

d) Manifestação da Unidade:

Em resposta ao Relatório Preliminar de Auditoria, encaminhado através do Memorando Eletrônico nº 42/2018/AUDINT/REI, a Gestão apresentou resposta através do Memorando Eletrônico nº 42/2018/PRODIN/REI, nos seguintes termos:

Considerando o fato apresentado, esclarece-se que o Plano de Desenvolvimento Institucional – PDI do IFS é o documento norteador da estratégia organizacional, tendo como principais instrumentos o Plano Plurianual (PPA), Lei Orçamentária Anual (LOA), Termo de Metas (TAM), Plano Nacional da Educação (PNE). Assim o PDI retrata os objetivos estratégicos traçados e sua integração com as ações orçamentárias e interação com os macroprocessos finalísticos e de apoio. Logo apenas os objetivos estratégicos são nele definidos.

O Plano de Desenvolvimento Anual (PDA) por sua vez é o instrumento que detalha a estratégia nos macroprocessos. É "o documento de planejamento anual do IFS, devendo ser elaborado de forma articulada pelas Pró-Reitorias, Diretorias, Coordenadorias Sistêmicas e os Campi". Dessa forma indica os representantes institucionais que estão diretamente vinculados aos objetivos estratégicos do IFS, aos quais convém estabelecer seus objetivos táticos no referido instrumento. Entretanto, a inserção destes no PDA ainda não é prática padronizada.

Vê-se que objetivos estratégicos norteiam a definição de objetivos táticos que por sua vez se desdobram em objetivos operacionais. A ausência dos operacionais no plano citado, não implica, necessariamente, em sua indefinição, aos objetivos informados no PDA (estratégicos e táticos) atribuem-se indicadores. Estes são traduzidos em metas, que são alcançadas em função de ações operacionais, entretanto, no referido plano nãocabe segmentar as ações; logo, não caberá informar objetivos operacionais.

Nesse aspecto, cumpre relembrar informação contida no PDA/2018, página 7, onde consta que no ano de 2016a PRODIN foi notificada pela Controladoria Geral da União – CGU por meio do Relatório de Auditoria n°201601456 por meio da constatação 3.1.1.1, que recomendou uma reavaliação do quantitativo de indicadores, afim de, entre outros aspectos, reduzir seu número para o mais próximo do gerenciável, o que limitou a 34 os188 preexistentes, cujo desdobramento tinha natureza operacional (detalhamento de metas. Ressalta-se que omonitoramento do número atual de indicadores é realizado por meio do software de gerenciamento deplanejamento estratégico (GEPLANES), ferramenta que está sendo utilizada com adaptações de forma aevidenciar a correlação dos objetivos táticos à respectiva estratégia indicada no PDA.

Diante do exposto, conclui-se que não convém registrar objetivos operacionais no PDA.

Evidência: Plano de Desenvolvimento Anual (PDA 2018). Disponível em: http://www.ifs.edu.br/images/prodin/2018/PLANO_DE_DESENVOLVIMENTO_ANUAL_2018_REV02.pdf

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

e) Análise da Manifestação:

A manifestação do gestor corrobora, em parte, uma vez que reconhece que não existe padronização no IFS quanto à necessidade de inclusão dos objetivos táticos no PDA. Sendo assim, alguns gestores incluem estes objetivos no PDA, enquanto outros não o fazem, conforme pode ser verificado no PDA 2018.

Ressaltamos a importância quanto à definição e inclusão dos objetivos táticos no PDA, uma vez a partir deste documento é realizado o acompanhamento da execução dos objetivos estabelecidos, possibilitando a realização de eventuais correções caso sejam identificadas dificuldades para atingimento dos objetivos.

f) Riscos e Efeitos:

Ausência de definição de objetivos táticos e operacionais por parte dos gestores do IFS pode dificultar a implementação da gestão de riscos, já que a fixação desses objetivos, alinhados à missão e à visão do IFS, é necessária para permitir a identificação de eventos que potencialmente impeçam a consecução.

Recomendação 001: (PRODIN)

Definir objetivos táticos no Plano de Desenvolvimento Anual– PDA, em conjunto com os setores competentes,alinhando-os aos objetivos estratégicos que permitam a consecução das metas estabelecidas no Plano de Desenvolvimento Institucional – PDI do IFS.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

2.2 Maturidade da Gestão de Riscos no IFS

Conforme detalhado no tópico Metodologia do trabalho, para avaliar o nível de maturidade da Gestão de Riscos no IFS, a equipe de auditoria respondeu ao questionário de avaliação da gestão de riscos (QAGR).

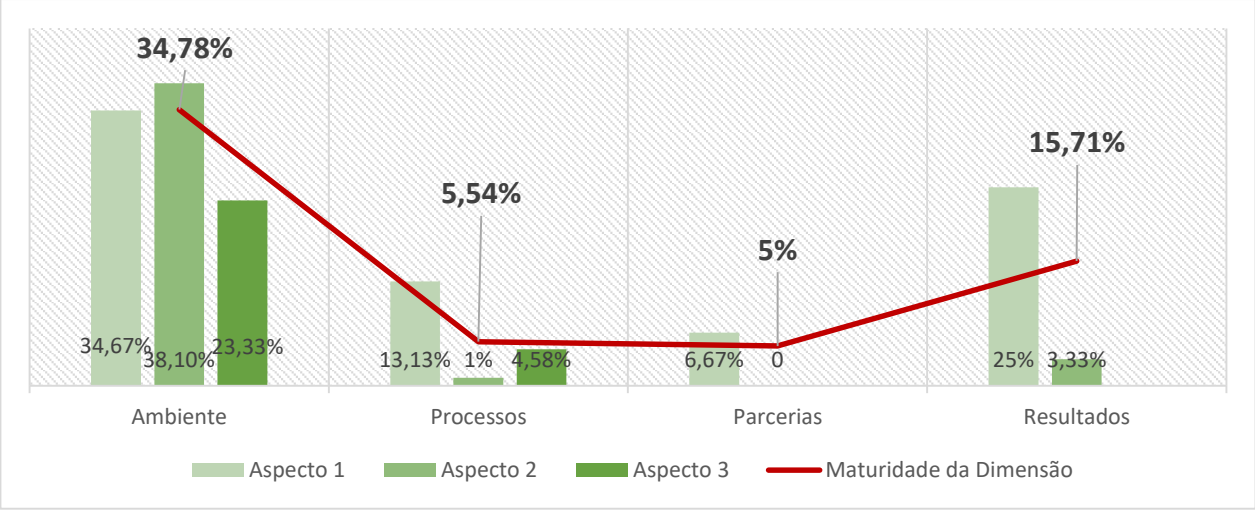
O Quadro e Gráfico a seguir apresentam, resumidamente, o resultado da avaliação da maturidade da gestão de riscos do IFS, por **dimensão** e seus respectivos **aspectos**:

***Quadro 3** - Resultado da avaliação da maturidade da gestão de riscos por dimensão e aspecto*

Dimensão	Maturidade por Dimensão	Aspectos	Maturidade por Aspecto
1. Ambiente	34,78%	1.1. Liderança	34,67%
		1.2. Políticas e estratégias	38,10%
		1.3. Pessoas	23,33%
2. Processos	5,54%	2.1. Identificação e análise de riscos	13,13%
		2.2. Avaliação e Resposta a riscos	1%
		2.3. Monitoramento e comunicação	4,58%
3. Parcerias	5%	3.1. Gestão de riscos em parcerias	6,67%
		3.2. Planos e medidas de contingência	0
4. Resultados	15,71%	4.1. Melhoria dos processos de governança	25%
		4.2. Resultados-chaves da gestão de riscos	3,33%

Fonte: Audint

***Gráfico 1** - Resultado da avaliação da maturidade da gestão de riscos por dimensão e aspecto*



Fonte: TCU

De posse dos índices de maturidade de cada dimensão, calculou-se a média ponderada levando em consideração os pesos estabelecidos no Modelo do TCU, conforme demonstrado na Tabela 2:

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

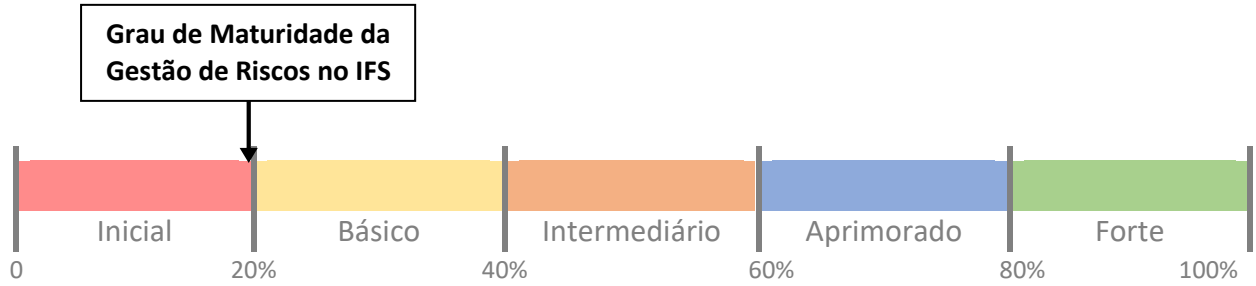
***Tabela 2** - Índice de Maturidade Global da Gestão do IFS*

Dimensão	Índices de Maturidade das Dimensões	Peso	Média Ponderada
Ambiente	34,78	0,4	13,91%
Processos	5,54	0,3	1,66%
Parcerias	5,0	0,1	0,50%
Resultados	15,71	0,2	3,14%
Índice de Maturidade Global			**19,22%**

Fonte: Audint

A partir do índice de maturidade global de 19,22%, foi possível definir o nível de maturidade global da Gestão de Riscos no IFS como no nível Inicial, conforme demonstrado na escala a seguir:

***Gráfico 2** - Nível de maturidade global da Gestão de Riscos no IFS*



Fonte: Audint

Desta forma, o trabalho de auditoria permitiu concluir que há, no IFS, princípios e padrões documentados e treinamento básico sobre gestão de riscos, contudo, a implantação da política e prática de gestão de riscos esbarra na indefinição da Política de Governança e na ausência de desenho dos processos dos setores.

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

3 – CONSIDERAÇÕES FINAIS

A presente auditoria teve como objetivos principais determinar o nível de maturidade da gestão de riscos do IFS e identificar os aspectos da Gestão de Riscos que necessitam ser aperfeiçoados.

Em face dos exames realizados, foi possível concluir que maturidade da gestão de riscos no IFS encontra-se em níveis iniciais, conforme metodologia e classificação estabelecidos pelo Modelo de Avaliação da Maturidade Organizacional em Gestão de Riscos desenvolvido pelo TCU.

Apesar da existência de uma Política de Gestão de Riscos aprovada contendo princípios e padrões documentados, bem como a realização de treinamento básico sobre gestão de riscos para alguns gestores das áreas estratégicas e táticas do IFS, a implantação da política e a prática da gestão de riscos esbarra, dentre outros fatores relatados nas Constatações desse Relatório, na indefinição da estrutura de Governança do IFS, e consequentemente, na ausência de mapeamento dos processos dos setores e na insuficiência de recursos alocados no Departamento de Gestão de Riscos. Outros aspectos relevantes identificados durante o trabalho de auditoria foi a ausência de acompanhamento e supervisão, pelo Comitê de Governança, Riscos e Controles – CGRC e a falta de um cronograma para a realização das atividades de institucionalização da Gestão de Riscos.

Também foi possível detectar pontos positivos adotados pela gestão na temática de gestão de riscos: (1) a Ação de mobilização e sensibilização ao processo de gestão de riscos desenvolvida junto aos servidores da Reitoria e nos *campi* Itabaiana e Socorro pelo DGR em conjunto com a Coordenadoria de Planejamento (COPLAN), resultando em um diagnóstico da percepção dos gestores sobre a temática; (2) realização de revisão, em 2017, do Planejamento Estratégico e seus Indicadores utilizando como ferramenta a análise dos fatores do ambiente interno e externo (Ferramenta SWOT/FOFA) e (3) publicação, dentro do Plano Diretor de Tecnologia de Informação e Comunicação (DTI) 2014-2019, do Plano de Gestão de Riscos.

Diante das fragilidades apontadas, esta Audint sugere que os gestores envidem esforços para aperfeiçoar a implantação da gestão de riscos no IFS por meio da formalização do sistema de governança, do fortalecimento dos recursos humanos e tecnológicos do Departamento de Gestão de Riscos, do mapeando de processos da Instituiçãoe da atuação efetiva do Comitê de Governança, Riscos e Controles.

Faz-se necessário esclarecer que, apesar de os resultados da metodologia utilizada para avaliação da Maturidade da Gestão do Risco adotada neste trabalho evidenciarem aspectos críticos nas dimensões Processos, Parcerias e Resultados, entendemos que esta avaliação é consequência da fase atual implantação da gestão de riscos, a qual se encontra em fase inicial.

Neste sentido, as recomendações emitidas neste relatório têm por objetivo contribuir para a implementação da Política de Gestão de Riscos. Uma vez que entendemos que, após efetivamenteimplementada esta política, poderão ser reavaliados os aspectos relacionados as dimensões que nesta metodologia foram avaliadas com baixos índices, com a consequente

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

propositura de ações que tenham por objetivo o aumento de tais índices, caso estes não tenham sido elevados.Porém, a ausência de recomendações relacionadas as dimensões e aspectos avaliados com baixo índice neste trabalho, não impede que a gestão implemente as ações que julgarem pertinentes a qualquer momento.

Sobre os benefícios esperados desta auditoria pode-se mencionar, principalmente, a contribuição ao processo de implantação da gestão de riscos e no fortalecimento da estrutura de governança do IFS, cujas deficiências foram evidenciadas pelas impropriedades relatadas neste relatório, na conscientização quanto à importância da supervisão e monitoramento dos controles e na formalização, padronização e comunicação das rotinas e procedimentos, com o intuito de evitar problemas relacionados a interpretação e aplicação, bem como aperfeiçoar a atuação dos gestores e agentes públicos.

Ademais, independente das recomendações que serão objeto de monitoramento pela Audint, cabe aos atores envolvidos nos processos de implementação da política de gestão de riscos um acompanhamento mais efetivo dos processos vindouros.

Por fim, a equipe de auditores agradece a todos os servidores pela disponibilidade das informações requisitadas e se coloca à disposição para elucidar quaisquer inconsistências relatadas, visando, sobretudo, o aperfeiçoamento da Gestão de Riscos no IFS.

Aracaju/SE, 24 de abril de 2018.

Helanne Cristianne da Cunha Pontes
Auditora Interna

Wenia Ventura de Farias Caldas
Auditora Interna

Giulliano Santana Silva do Amaral
Chefe da Auditoria Interna

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Anexo I – Critérios para Avaliação da Maturidade em Gestão de Riscos

1. AMBIENTE

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.

1.1. 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, 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.

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**	**Pontuação**
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; COSO GRC 2004, 2; COSO GRC PublicExposure (PE) 2016, Princípios 3, 4 e 5; ISO 31000:2009, 3, "h" e 4.2; OCDE, 2011.	1,6
b) reforçando o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização;		1,6
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.		1,6
GOVERNANÇA DE RISCOS **Questão 1.1.2**	**Critério**	**Pontuação**
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.	1,6
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**	**Pontuação**
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.	0,8
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;		0,8
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;		0
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		1,6

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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.		1,6

1.2. Políticas e estratégias

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.

DIRECIONAMENTO ESTRATÉGICO **Questão 1.2.1**	**Critério**	**Pontuação**
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.	3,2

Questão 1.2.2	**Critério**	**Pontuação**
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.	0,8

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**	**Pontuação**
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, Princípios 9, 10 e 11; INTOSAI GOV 9130/2007, 1.3 e 2.2.	1,6
b) os objetivos de negóciosespecíficos 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.		0,8

Questão 1.2.4	**Critério**	**Pontuação**
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.	0,8

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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**	**Pontuação**
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.	4
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;	1,6
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;	4
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;	4
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;	1,6
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;	3,2
COMPROMENTIMENTO DA GESTÃO **Questão 1.2.6**	**Critério**	**Pontuação**
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.	0,8
ALOCAÇÃO DE RECURSOS **Questão 1.2.7**	**Critério**	**Pontuação**
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.	0,8
1.3. Pessoas 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.		
REFORÇO DA *ACCOUNTABILITY*		

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Questão 1.3.1	Critério	Pontuação
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.	0,8
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**	**Pontuação**
a) Naprimeira 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.	0,8
b) Nasegunda 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.	0,8
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. IIA IPPF Norma 2010, 2100, 2110 e 2210. RES CNJ 171/2013, Art. 10 e 12.	1,6
2. PROCESSOS		

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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.

2.1. 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.

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**	**Pontuação**
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.	0,8
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.	0
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.	0
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**	**Pontuação**
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	1,6
b) a análise de partes interessadas e seus interesses (por exemplo, análise de stakeholder, análise RECI, matriz de responsabilidades); e		0
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).		1,6
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**	**Pontuação**
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.	0,8
b) são utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de risco;	ISO 31000:2009, 5.4.2 .	0,8

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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.	0,8
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.	0,8
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".	0
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.	0,8
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**	**Pontuação**
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.	0,8
b) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise de riscos;		0
c) os participantes das atividades de identificação e análise;		0
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;		0
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;		0
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;		0
g) a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade; e	ISO 31000:2009, 5.5.1	0
h) o risco residual.	ISO 31000:2009, 5.5.1	0
2.2. 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.		
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**	**Pontuação**
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;	0

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

b) se uma atividade deve ser realizada, reduzida ou descontinuada; e	COSO GRC 2004, 6; COSO GRC PE 2016, Princípio 14.	0
c) se controles devem ser implementados, modificados ou apenas mantidos.		0
AVALIAÇÃO E SELEÇÃO DAS RESPOSTA A RISCOS		
Questão 2.2.2	**Critério**	**Pontuação**
A avaliação e a seleção das respostas a serem adotadas para reduzir a exposição aos riscos identificadosconsidera a relaçãocusto-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.	0
Questão 2.2.3	**Critério**	**Pontuação**
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;	0
PLANOS E MEDIDAS DE CONTINGÊNCIA		
Questão 2.2.4	**Critério**	**Pontuação**
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.	0
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**	**Pontuação**
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.	0,8
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;		0
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		0
d) os responsáveis pela aprovação e pela implementação do plano de tratamento de riscos, com autoridade suficiente para gerenciá-lo.		0
2.3. Monitoramento e comunicação 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		
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**	**Pontuação**
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.	0

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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.	0
SISTEMA DE INFORMAÇÃO **Questão 2.3.2** A gestão de riscos é apoiada por um registro de riscos ou sistema de informação que:	**Critério**	**Pontuação**
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.	0
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).	0
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**	**Pontuação**
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, Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.,	0
b) por meio de autoavaliações periódicas de riscos e controles (ControlandRisk Self Assessment – CRSA), que constam de um ciclo de revisão periódica estabelecido; e		0
c) a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança.		0
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**	**Pontuação**
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.,	0
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.		0,8
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**	**Pontuação**
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.	1,6

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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.	1,6
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.	0
Questão 2.3.6	**Critério**	**Pontuação**
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.	0
MONITORAMENTO DE MUDANÇAS SIGNIFICATIVAS **Questão 2.3.7**	**Critério**	**Pontuação**
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.	0
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**	**Pontuação**
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.	0
b) elaboração e devido acompanhamento de planos de ação para corrigir as deficiências identificadas e melhorar o desempenho da gestão de riscos.		0
3. PARCERIAS 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. *(Entende-se aqui por Parceria: contratos/convênios com Fundações de Apoio e outras entidades, tais como as parcerias como outras instituições de ensino.) -Texto retirado do trabalho da UFFS*		
3.1. Gestão de riscos em 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.		
AVALIAÇÃO DA CAPACIDADE DE GESTÃO DE RISCOS DE ENTIDADES PARCEIRAS **Questão 3.1.1**	**Critério**	**Pontuação**
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;	0
DEFINIÇÃO DE RESPONSABILIDADES, INFORMAÇÃO E COMUNICAÇÃO **Questão 3.1.2**	**Critério**	**Pontuação**
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.	0
PROCESSO DE GESTÃO DE RISCOS PARCERIAS **Questão 3.1.3**	**Critério**	**Pontuação**

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

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;	0
Questão 3.1.4	**Critério**	**Pontuação**
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.	0
Questão 3.1.5	**Critério**	**Pontuação**
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).	0
Questão 3.1.6	**Critério**	**Pontuação**
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	1,6
3.2. 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.		
Questão 3.2.1	**Critério**	**Pontuação**
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.	0
Questão 3.2.2	**Critério**	**Pontuação**
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.	0
4. 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.		
4.1. Melhoria dos processos de governança 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.		
INTEGRAÇÃO DA GESTÃO DE RISCOS AOS PROCESSOS ORGANIZACIONAIS **Questão 4.1.1**	**Critério**	**Pontuação**
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 da organização, tendo consciência do nível de maturidade atual e do progresso das ações em curso para atingir ao nível almejado.	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.	1,6

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br

Questão 4.1.2	Critério	Pontuação
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.	1,6
Questão 4.1.3	**Critério**	**Pontuação**
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.	0,8
Questão 4.1.4	**Critério**	**Pontuação**
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.	0
4.2. Resultados-chave da gestão de riscos 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.		
ENTENDIMENTO DOS OBJETIVOS, RISCOS, PAPÉIS E RESPONSABILIDADES **Questão 4.2.1**	**Critério**	**Pontuação**
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.	0
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**	**Pontuação**
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.	0
b) entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados;		0
c) a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável; e		0,8
d) as leis e os regulamentos aplicáveis estão sendo cumpridos.		0,8
EFICÁCIA DA GESTÃO DE RISCOS **Questão 4.2.3**	**Critério**	**Pontuação**
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.	0

Rua Francisco Portugal, 150, Salgado Filho. CEP: 49020-390 - Aracaju/SE
Tel.: (79) 3711-1880/1854, email: audint@ifs.edu.br