PRESIDÊNCIA DA REPÚBLICA

SECRETARIA-GERAL

SECRETARIA DE CONTROLE INTERNO

PLANO ANUAL DE AUDITORIA INTERNA

PAINT 2019

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL

PRESIDÊNCIA DA REPÚBLICA

SECRETARIA-GERAL

SECRETARIA DE CONTROLE INTERNO

PLANO ANUAL DE AUDITORIA INTERNA

PAINT 2019

Brasília/DF, 2019

SUMÁRIO

1. APRESENTAÇÃO

1.1. Secretaria de Controle Interno

A Secretaria de Controle Interno da Presidência da República (CISET/SG-PR), unidade vinculada à Secretaria-Geral da Presidência da República, é responsável pelas atividades de auditoria (consultoria e assessoria), ouvidoria e corregedoria junto aos órgãos da Presidência da República, Vice-Presidência e entidades subordinadas.

No cumprimento de suas competências legais, a CISET realiza ações de auditoria e fiscalização nas unidades jurisdicionadas (UJ), buscando auxiliar na melhoria da gestão pública por meio do estímulo à governança, à gestão de riscos e ao incremento dos controles internos.

Além da área de auditoria, a CISET mantém, em sua estrutura, duas linhas de atuação estratégicas para o aprimoramento da gestão: Corregedoria e Ouvidoria. Nesse contexto, as ações da Corregedoria voltam-se, primordialmente, para coibir condutas irregulares de agentes públicos e privados na gestão da coisa pública. No âmbito da Ouvidoria, é responsável por gerir denúncias, reclamações, solicitações, elogios e sugestões encaminhados aos órgãos da Presidência e Vice-presidência da República.

O Decreto nº 9.670, de 2 de janeiro de 2019 alterou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Secretaria-Geral da Presidência da República e consequentemente houve alteração na estrutura da Secretaria de Controle Interno. As atividades de auditoria que eram exercidas por três unidades, a saber: Coordenação-Geral de Auditoria Contínua, Coordenação-Geral de Auditoria Operacional e Coordenação-Geral de Auditoria de Gestão, passaram a ser exercidas pela Coordenação-Geral de Avaliação e Coordenação-Geral de Consultoria.

A atividade de consultoria ganhou foco devido à necessidade identificada de assessoramento resultante do novo paradigma da gestão pública, a governança. Outra alteração foi a extinção da Coordenação-Geral de Planejamento e Governança e criação de uma Coordenação de Gestão Interna, com uma divisão específica para tratar de informações estratégicas.

A nova estrutura da CISET está representada pela figura 1.

Nova estrutura

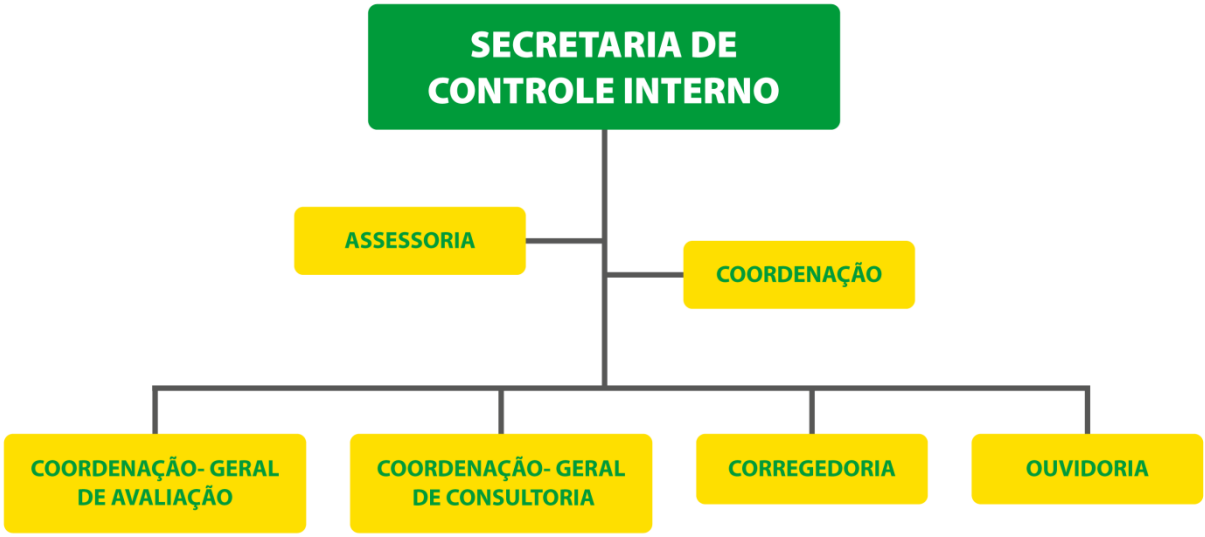


Figura 1 - Nova estrutura da CISET

No início desse ano de 2019, a CISET/Presidência priorizou a construção de seu mapa estratégico 2019-2022. O mapa foi fundamental para espelhar essa nova proposta de atuação da Secretaria - focada na prevenção e no alinhamento com os interesses da alta administração - para definir os valores da Secretaria, bem como para promover o alinhamento interno dos resultados a serem alcançados. O mapa estratégico tem impacto direto em todas as decisões da instituição. Ele cumpre a tarefa de orientar todos os demais planos. Foi, portanto, um direcionador para todas as ações definidas neste documento.

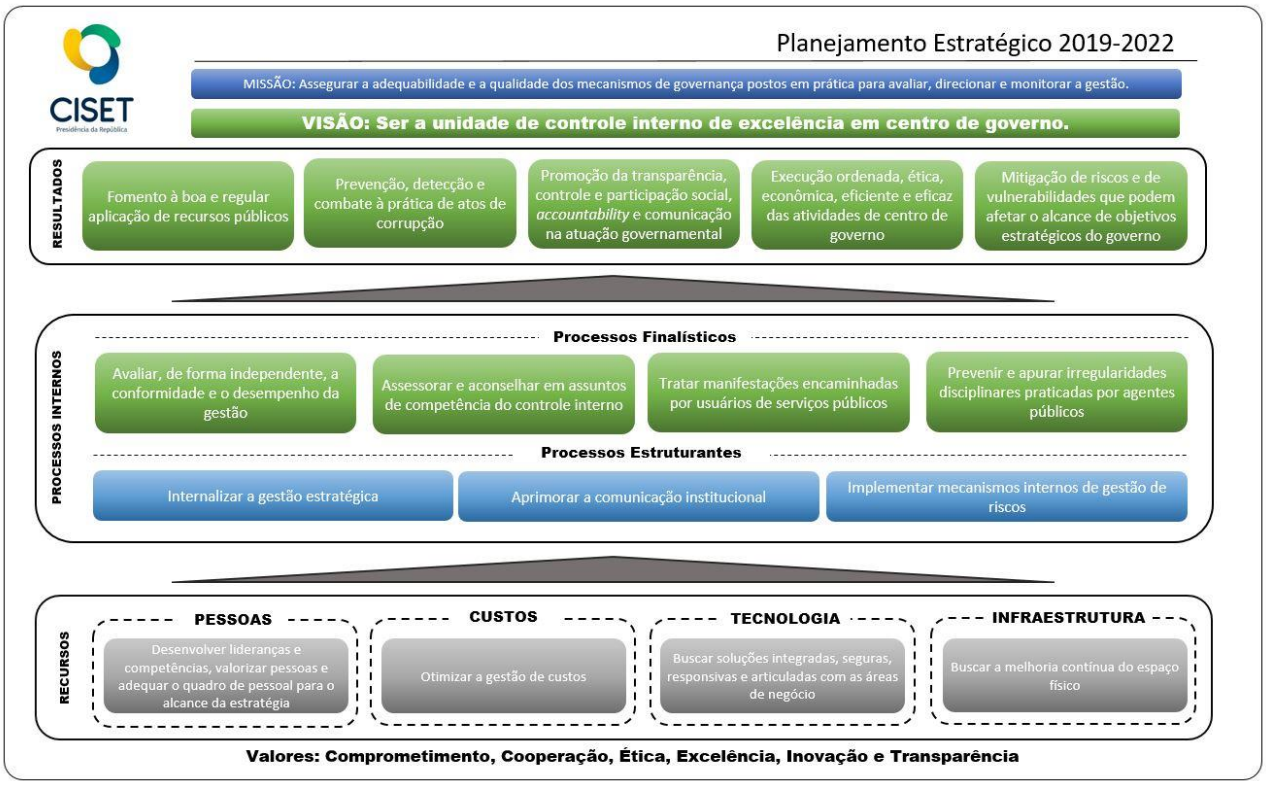


Figura 2 - Mapa estratégico da CISET

1.2. Competências

A Secretaria de Controle Interno da Presidência da República (CISET/Presidência) é o órgão setorial do Sistema de Controle Interno do Poder Executivo Federal responsável pelas ações de auditoria (avaliação e consultoria) nos órgãos integrantes da Presidência da República e da Vice-Presidência da República, nos termos da Lei n° 10.180, de 6 de fevereiro de 2001 c/c o Decreto n° 3.591, de 6 de setembro de 2000 e com o Decreto nº 9.670, de 2 de janeiro de 2019.

Ademais, exerce as atividades de unidade seccional do Sistema de Correição do Poder Executivo federal naqueles órgãos, nos termos do Decreto nº 5.480, de 30 de junho de 2005 c/c o Decreto nº 9.670, de 2 de janeiro de 2019; bem como as atividades de unidade de ouvidoria da Presidência da República.

Diante do novo decreto, as competências consolidadas no anexo VIII da Portaria SG/PR nº 7, de 14 de março de 2018, publicada no Diário Oficial da União de 15 de março de 2018, Seção 1, com retificação publicada em 6 de abril de 2018, Seção 1, que aprova o Regimento Interno da Secretaria-Geral da Presidência da República serão revistas.

1.3. Atuação

A atuação da Secretaria de Controle Interno abrange os órgãos integrantes da Presidência da República e da Vice-Presidência da República, conforme relação abaixo.

CASA CIVIL
Secretaria-Executiva
Secretaria Especial de Relações Governamentais
Secretaria Especial para o Senado Federal
Secretaria Especial para a Câmara dos Deputados
Subchefia de Ação Governamental
Subchefia de Articulação e Monitoramento
Subchefia para Assuntos Jurídicos
Imprensa Nacional – IN
Entidade vinculada à Casa Civil
Instituto Nacional de Tecnologia da Informação – ITI

GABINETE DE SEGURANÇA INSTITUCIONAL – GSI
Secretaria-Executiva
Secretaria de Segurança e Coordenação Presidencial
Secretaria de Coordenação de Sistemas
Secretaria de Assuntos de Defesa e Segurança Nacional
Agência Brasileira de Inteligência – ABIN

SECRETARIA-GERAL
Secretaria-Executiva - Secretaria de Administração
Secretaria Especial de Assuntos Estratégicos – SAE
Secretaria Especial de Modernização do Estado
Secretaria-Executiva da Comissão de Ética Pública

SECRETARIA DE GOVERNO

Secretaria Executiva
Secretaria Especial de Assuntos Federativos
Secretaria Especial de Relações Institucionais
Secretaria Especial de Articulação Social
Secretaria Especial do Programa de Parcerias de Investimentos – SEPPI
Secretaria Especial de Comunicação Social – SECOM
Entidade vinculada à Secretaria de Governo
Empresa Brasil de Comunicação – EBC

VICE-PRESIDÊNCIA DA REPÚBLICA

ADVOCACIA-GERAL DA UNIÃO – AGU

CONTROLADORIA-GERAL DA UNIÃO

1.4. Força de trabalho

A Secretaria conta atualmente com 57 servidores distribuídos conforme tabela 1 a seguir. Para o planejamento das ações de 2019, foi considerado a quantidade de homens hora disponíveis. O apêndice I detalha os parâmetros para cálculo do HH disponível.

	CGAVA		CGCON		COGIN		OUV		CORREG		GABIN	
Atividade	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro
Nº servidores	16	1	8	0	5	10	5	0	8	1	2	1
HH líquido	22.576		10.624		19.920		6.640		11.952		3.984	

Tabela 1 - Força de trabalho disponível para 2019

2. PLANO DE AUDITORIA

O plano de auditoria detalha as ações de consultoria e de avaliação da CISET/Presidência planejadas para 2019, bem como os critérios de seleção e os fatores limitadores. As ações foram divididas em três grandes grupos: trabalhos obrigatórios, definidos pela legislação como entregas obrigatórias da CISET; trabalhos prioritários, selecionados pela CISET a partir de critérios; e trabalhos de apoio estratégico, que subsidiam as ações anteriores.

2.1. Ações obrigatórias

As ações consideradas obrigatórias, para as quais não há que se falar em priorização, são aquelas determinadas pelo Tribunal de Contas União em decorrência do artigo 74 da Constituição Federal e de normativos do controle externo e interno, a saber: Decisão Normativa TCU nº 172 de 12 de dezembro de 2018, Instrução Normativa TCU 71/2012, Instrução Normativa SFC nº 03, de 09 de junho de 2017, Instrução Normativa Nº 9, de 09 de outubro de 2018. Como consequência, para o exercício de 2019, foram planejadas as seguintes ações obrigatórias:

Ação	Meta	Cliente	HH
Elaborar o Planejamento de Auditoria Interna	1 plano elaborado	CGU	160
Avaliação da conformidade e desempenho da gestão, para subsidiar o TCU no julgamento anual das contas.	5 unidades certificadas	TCU	6.400
Avaliar o planejamento e execução das ações das unidades de auditoria interna vinculadas à Presidência da República	2 Planos analisados	PR	32
Avaliar a adequação das medidas administrativas adotadas quanto aos processos de tomada de contas especial (artigo 10 da Instrução Normativa/TCU n° 71, de 28/11/2012)	100% dos processos recebidos analisados	TCU	96
Apurar as denúncias acerca da aplicação de recursos públicos federais	100% das denúncias recebidas analisadas	Órgão demandante	400
Avaliação dos atos de admissão e de concessão de aposentadorias e pensões	413 Processos Analisados	TCU	5.312
Relatório Anual de Atividades de Auditoria Interna	1 relatório elaborado	CGU	160

Tabela 2 - Ações obrigatórias da CISET

2.2. Ações prioritárias

A Secretaria de Controle Interno possui a particularidade de trabalhar essencialmente com órgãos de centro de governo, responsáveis por olhar a totalidade da ação governamental e assegurar coerência e coesão às diversas iniciativas propostas pelo governo. Sendo assim, atuação da CISET deve ser voltada para assuntos da alta administração.

Nesse sentido, a mudança de governo trouxe uma nova dinâmica para os trabalhos da Secretaria, com oportunidades de parcerias para a construção de modelo de governança mais eficiente e integrado.

A partir da análise da matriz SWOT elaborada pela Secretaria-Geral em 2017, por conta do planejamento estratégico, foram identificadas algumas oportunidades de atuação da CISET, que tem competência de, juntamente com o gestor, tratar a fraqueza de "Baixa governança corporativa" e a ameaça de "Gestão e governança tratada de forma setorial, na Presidência da República, com perda de sinergia no alcance de resultados para a sociedade", realizando avaliações e assessoramento diretamente nos órgãos de centro de governo.

Diante desse cenário, ressalta-se a visão definida no mapa estratégico da Secretaria de Controle Interno 2019-2022, que propõe "Ser a unidade de controle interno de excelência em centro de governo". Nesse contexto e tendo como direcionador alguns normativos recentes relacionados ao controle, foram definidas as ações prioritárias desta Secretaria.

Quanto às ações de consultoria, destaca-se que foram fundamentadas nas diretrizes do governo federal definidas a partir da publicação do Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional; da Portaria da CGU nº 57/2019, de 4 de janeiro de 2019, que trata da instituição do programa de integridade; da Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

Além disso, as ações de consultoria também buscam auxiliar os gestores no cumprimento das determinações e orientações constantes dos acórdãos do TCU, bem como no processo de prestação de contas anuais, em conformidade com a Decisão Normativa-TCU Nº 170, de 19 de setembro de 2018, que dispõe acerca das unidades cujos dirigentes máximos devem prestar contas de suas gestões ocorridas no exercício de 2018 e exige a preparação de relato integrado.

Quanto às ações prioritárias de avaliação, há previsão de ação contínua de avaliação dos atos da gestão, realizada a partir dos alertas diários gerados por trilhas de auditoria, ou por meio de análise baseada nos critérios de materialidade, criticidade e relevância, com potenciais riscos para a boa gestão da Presidência da República.

Há previsão também de avaliação da eficiência e dos resultados dos processos e temáticas prioritárias das unidades da PR. Essa ação está direcionada prioritariamente para atendimentos de demandas do gestor. A partir da demanda, será realizado um estudo das possíveis frentes de atuação e serão avaliados os principais riscos associados, para que seja definido, juntamente com o gestor, a linha de atuação da CISET.

Compete esclarecer que a metodologia utilizada na CISET/Presidência para a priorização das ações de controle a serem conduzidas encontra-se definida na Nota Técnica nº 42/2016/CGAP/CISET/SG-PR (Apêndice IV). Entretanto, a metodologia foi construída para um cenário de unidades gestoras de políticas públicas com critérios focados em materialidade, diferente do que ocorre na atual jurisdição da CISET/Presidência, que atua em unidades que exercem papéis estratégicos de governança de centro de governo.

Dessa forma, em virtude de uma atuação precípua da Ciset em consultoria ao Centro de Governo, deverá ser construída uma nova forma para priorização dessas ações.

Cabe ressaltar que os planos de auditorias das nossas unidades jurisdicionadas, tais sejam Empresa Brasil de Comunicações - EBC e Instituto Nacional de Tecnologia da Informação - ITI, foram recebidos, avaliados e compatibilizados com ações priorizadas na EBC devido demanda ministerial e também com ação obrigatória em decorrência da prestação de contas - Gestão 2018.

A seguir apresentam-se as ações prioritárias da CISET/PR.

Ação	Meta	Cliente	HH
Elaborar estratégia de atuação da CGCON, definindo as ações a serem conduzidas, as prioridades a serem implementadas, conciliando os interesses e necessidades dos órgãos da PR	2 Planos de Consultoria	PR	480
Identificar as estruturas de governança dos órgãos da Presidência da República, identificando fatores críticos de sucesso e oportunidades de melhoria.	4 Relatórios de Levantamento	PR	1280
Auxiliar os gestores na implementação de mecanismos de governança	8 estruturas implementadas	PR	1.536
Auxiliar os gestores na implementação de programa de Integridade	4 planos publicados	PR	640
Auxiliar os gestores na interlocução, atendimento de demandas e articulação de interesses junto ao TCU	15 comunicações estabelecidas	PR	480
Reportar às autoridades competentes as deliberações dos órgãos de controle e outras informações estratégicas de interesse das unidades.	40 informes	PR	640
Assessorar os gestores na implementação e funcionamento da política de gestão de riscos	4 políticas publicadas	PR	960
Orientar os gestores quanto a elaboração dos relatórios de gestão das Unidades Prestadoras de Contas (UPCs) da PR	9 UOC orientadas	PR	720

Promoção de oficinas para orientação técnica das unidades da PR nas temáticas de controle	4 oficinas realizadas	PR	512
Interlocução com a CGU e outras instâncias de controle para alinhamento de estratégias que possam auxiliar as unidades da PR a alcançar seus objetivos estratégicos.	4 interlocuções	PR	128
Auxiliar na apresentação de informações para a Prestação de Contas do Presidente da República (PCPR)	1 PCPR conduzida	Casa Civil	80
Avaliação continua dos atos da gestão (editais de licitação, adesões, dispensas e inexigibilidade de licitação, contratações, convênios ou outros instrumentos congêneres, etc.)	10 unidades monitoradas	PR	2.656
Avaliação das justificativas decorrentes das Trilhas de Auditoria de Pessoal	100% dos alertas analisados	Presidência da república	320
Avaliação da eficiência e dos resultados dos processos e temáticas prioritárias das unidades da PR	5 avaliações realizadas	PR	6.400

Tabela 3 - Ações prioritárias da CISET

2.3. Ações de apoio estratégico

Na reestruturação da CISET, foi criada uma divisão para subsidiar as ações das demais unidades da Secretaria. A divisão tem como objetivo principal produzir informações estratégicas sobre as unidades jurisdicionadas da Presidência da República, a partir de bases governamentais, identificando possíveis riscos e auxiliando assim na tomada de decisão do Secretário e no direcionamento das ações da Secretaria.

Ação	Meta	Cliente	HH
Mapear os sistemas utilizados pelos gestores no âmbito da PR.	Conhecimento dos sistemas utilizados pelas UJ	CISET	16
Produzir base de conhecimento acerca das unidades jurisdicionadas.	Relatório	CISET	3.200

Articular parcerias e acordos com outros órgãos e entidades para acesso a bases de dados governamentais.	Acesso a base de dados	Divisão	160
Produzir informações estratégicas para subsidiar as atividades da CISET.	Atendimento das demandas do Secretário	CISET	2.100
Manter e desenvolver sistemas internos.	Sistemas aprimorados	CISET	800
Realizar projeto piloto para implementação do sistema e-aud	Avaliação do sistema	CISET	320

Tabela 4 - Ações de apoio estratégico

2.4. Monitoramento das recomendações

O monitoramento das recomendações dar-se-á em dois momentos ao longo de 2019. As unidades que tiverem suas contas julgadas no ano (Secretaria-Geral, Secretaria de Governo, Empresa Brasil de Comunicação, Controladoria-Geral da União, Gabinete de Intervenção Federal) terão suas recomendações analisadas no momento do planejamento dos trabalhos de auditoria. Como resultado do trabalho de contas, as novas recomendações serão incluídas no sistema. No final do segundo semestre, será realizado um novo momento de acompanhamento das recomendações, com análises das providências tomadas pelo gestor. Para esse trabalho será reservado 160h.

Cabe destacar que o trabalho de monitoramento não se restringe à análise das providências ainda não acatadas, mas também no levantamento de possíveis riscos às unidades a partir da análise dos assuntos mais recorrentes, bem como consiste no aprimoramento das novas recomendações, de forma que seja evidenciado e atacado os principais riscos identificados e se pautando em “o quê” necessita ser feito, deixando para o gestor decidir “como” mitigar os riscos.

Atualmente, a Secretaria utiliza um sistema interno para acompanhamento dessas recomendações. Todo o processo - desde o cadastro de achado e recomendação, o registro da providência pelo gestor e a análise dos resultados - é realizado por meio do sistema. Com a mudança de governo e consequentemente a alteração de muitos de gestores na Presidência da República, será necessário realizar a capacitação desses novos gestores para o uso do sistema.

2.5. Fatores Limitadores

Cabe destacar alguns fatores que impactam diretamente no planejamento das ações da CISET ou que podem afetar a execução do plano.

A Presidência da República não possui quadro próprio e conta com a cessão de servidores de outros órgãos. Isso tem como consequência alta rotatividade do quadro de pessoal, necessidade de capacitação constante e dificuldade em manter equipes especializadas. Como exemplo, só nesse ano de 2019, nove servidores saíram da CISET.

Outra particularidade é a alteração constante da estrutura da Presidência da República, impactando na estrutura da própria CISET, além de alterar a abrangência de sua atuação, quando cria, funde ou extingue Secretarias e Ministérios.

A CISET sujeita-se à orientação normativa e à supervisão técnica da Controladoria-Geral da União e tem como uma de suas atribuições apoiar a supervisão ministerial e o Controle Externo nos assuntos de sua missão institucional. Sendo assim, sempre está se adequando às novas demandas.

3. DEMANDAS EXTRAORDINÁRIAS

As demandas extraordinárias podem ser originárias de demandas do gestor ou de demandas externas dos órgãos de controle – TCU e CGU, e de órgãos parceiros – MPU, Polícia etc.

A CISET tem buscado um alinhamento das suas ações às necessidades do Gestor. Nesse sentido, as demandas do gestor tendem a ter um peso maior frente as demais. Observa-se que, dentre as ações prioritárias, já existe margem para atendimento a algumas temáticas de demandas do gestor. Entretanto, caso seja uma ação não prevista no plano ou caso as demandas exijam mais recurso que o planejado, o Secretário, juntamente com os Coordenadores-Gerais, fará uma revisão do plano, definindo as novas prioridades pela criticidade. Essa análise levará em consideração a mensuração do risco, que estima a probabilidade e o impacto de sua ocorrência.

Ressaltamos o compromisso desta Secretaria em responder prontamente as demandas externas, entretanto, aquelas que implicarem ações de controle deverão ser avaliadas pela conveniência e oportunidade.

O apêndice III detalha o fluxo para tratamento das demandas externas.

4. AÇÕES DE DESENVOLVIMENTO

Com o objetivo de melhorar continuamente os processos internos e a qualidade das atividades dessa Secretaria, dois projetos devem ser destacados: Gestão do conhecimento e Gestão das capacitações.

O projeto de gestão do conhecimento tem como objetivo construir um modelo de gestão do conhecimento para a Ciset, utilizando as ferramentas disponíveis, de tal forma a aplicar os principais processos da gestão do conhecimento: identificação, criação, armazenamento, compartilhamento e aplicação do conhecimento; e, consequentemente, melhorar a capacidade de organização, permitir a correta utilização dos sistemas, fomentar a padronização, aumentar o desempenho e a qualidade dos produtos entregues.

O projeto de gestão das capacitações trata de proposta que engloba o planejamento das capacitações; criação de ferramenta para o gerenciamento do banco de talentos e para o controle das capacitações realizadas; definição de fluxograma; elaboração de diretrizes de afastamento para capacitação no âmbito da Secretaria.

Devido a alteração da estrutura, as novas Coordenações-Gerais precisam definir os novos processos e reavaliar os processos antigos, principalmente a Coordenação-Geral de Consultoria que propõe atividades que não eram realizadas. Nesse sentido, e por mais que os projetos citados tenham relação com essas necessidades, há também iniciativas de desenvolvimento dentro das próprias coordenações.

Ação	Meta	Cliente	HH

Gestão do conhecimento	Conhecimento identificado, organizado e compartilhado	CISET	1080
Gestão das capacitações	Definição de necessidades, criação de banco de talentos, monitoramento	CISET	600
Formar servidores especializados em matérias de controle e no negócio das unidades da PR.	Conhecimento compartilhado	CGCON	2560
Aprimoramento dos processos internos	Processo definido	CGCON	640
Gestão e aprimoramento de processos internos	Processo definido	CGAVA	600

5. CAPACITAÇÃO

O plano de capacitação 2019 da Secretaria de Controle Interno abrange congressos, cursos e certificações. A partir de uma percepção das competências necessárias para as atividades de auditoria, foi definido que todos os servidores que trabalham na área finalística deverão fazer o curso de gerenciamento de riscos. O curso previsto contempla 30h. Além desse curso básico, alguns servidores serão destacados para fazer um curso de gerenciamento de riscos em temas específicos.

O plano prevê a participação dos servidores da coordenação de avaliação no curso de auditoria baseada em riscos oferecido pelo TCU. Foi solicitado também um curso de gestão estratégica com foco em resultados, dentre outros para as áreas de auditoria, ouvidoria e gestão interna.

Ademais, o plano prevê certificação IIA e participação nos seguintes congressos:

- CONBRAI - Congresso Brasileiro de Auditoria Interna
- CLAI - XXIV Congresso Latinoamericano de Auditoria Interna
- 7º Congresso Internacional de Compliance

O plano garante as 40 horas mínimas de capacitação previstas na Instrução Normativa nº 9, de 09 DE outubro de 2018.

APÊNDICE I

Como parâmetro para a definição das ações da Secretaria de 2019, foi realizado um levantamento dos recursos com pessoal (HH) disponíveis. O cálculo levou em consideração os seguintes critérios:

Dias úteis 2019	
Total de dias no ano	365
Fim de semana	104
Feriados em dias de semana	11
Outros	0
Total de dias úteis	**250**

Tabela 5 - Cálculo dos dias úteis de 2019

Parâmetros definidos	
Férias	10% do total
Afastamento	4% do total de absenteísmo estimado
Capacitação	Média de 60h – baseada no plano de capacitações
Reserva técnica	20% do total

Tabela 6 - Critérios para o cálculo de HH

Além dos critérios citados, os servidores das unidades CISET foram divididos em dois grupos: aqueles que trabalham na atividade finalística de controle interno e aqueles que fazem as atividades meio. Essa divisão se faz necessário para que seja possível identificar o HH disponível para a realização das ações de controle interno.

	CGAVA		CGCON		COGIN		OUV		CORREG		GABIN	
Atividade	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro	Finalístico	Outro
Nº servidores	16	1	8	0	5	10	5	0	8	1	2	1
HH total	32000	2000	16000	0	10000	20000	10000	0	16000	2000	4000	2000
Férias	-3200	-200	-1600	0	-1000	-2000	-1000	0	-1600	-200	-400	-200
Afastamentos	-1280	-80	-640	0	-400	-800	-400	0	-640	-80	-160	-80
Capacitação	-960	-60	-480	0	-300	-600	-300	0	-480	-60	-120	-60
Reserva técnica	-5312	-332	-2656	0	-1660	-3320	-1660	0	-2656	-332	-664	-332
Total	21.248	1.328	10.624	0	-2656	13280	-2656	0	10.624	1.328	2.656	1.328
HH líquido	22.576		10.624		19.920		6.640		11.952		3.984	

APÊNDICE II – AÇÕES DE CORREIÇÃO E OUVIDORIA

Além das atividades de auditoria, a Secretaria de Controle Interno tem por competência realizar também as atividades de Corregedoria e de Ouvidoria. As tabelas 8 e 9 indicam as ações definidas para o período.

Ação	Meta	Cliente	HH
Acompanhamento gerencial das demandas da Corregedoria.	Demanda acompanhada	Corregedoria	240
Atendimento às demandas externas relativas à matéria da Corregedoria.	Demanda atendida	Órgão demandante	144
Realização de juízo de admissibilidade relativo à denúncias/representações correcionais.	Admissibilidade realizada	PR	832
Auxílio à autoridade instauradora e/ou julgadora para julgamento de procedimentos administrativos disciplinares.	Auxílio a julgamento realizado	PR	720
Supervisão dos procedimentos disciplinares no âmbito das Unidades Jurisdicionadas da Presidência da República.	Procedimentos supervisionados	PR	800
Instauração/Condução de Procedimento Administrativo Disciplinar - PAD	PAD concluído pela comissão	PR	5952
Instauração/Condução de Procedimento Administrativo Disciplinar - Sindicância	Sindicância concluída pela Comissão	PR	1920
Instauração/Condução de Procedimento Administrativo Disciplinar - Procedimento Celetista	Procedimento finalizado pela comissão	PR	480
Realização de visita técnica em Unidade Jurisdicionada da PR	Visita Técnica realizada	PR	32
Realização de inspeção correcional em Unidade Jurisdicionada da PR	Unidade Inspecionada	PR	48
Assessoramento na matéria disciplinar	Assessoramento realizado	PR	336

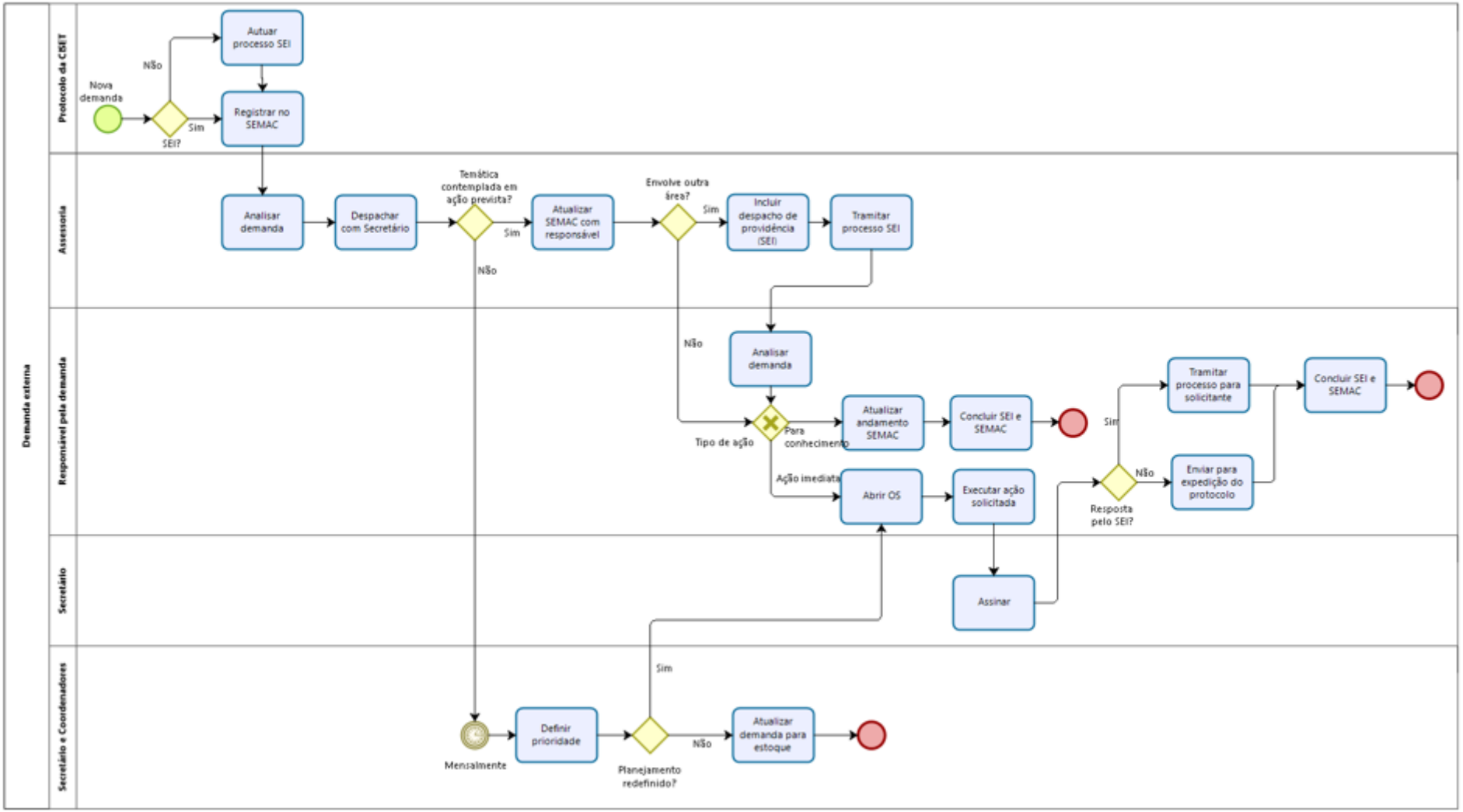
Promoção de evento de capacitação e/ou prevenção relativa à matéria correcional	Evento/Curso realizado	PR	96
Implementação do Painel da Corregedoria, com disponibilização de informações gerencias relativas às atividades disciplinares no âmbito da Presidência da República, extraídas do CGU-PAD, por meio do QlikView.	Painel implementado	PR	80
Elaboração de normativo relativo à matéria da Corregedoria.	Minuta de normativo apresentada	PR	220

Tabela 7 - Ações da Corregedoria

Ação	Meta	Cliente	HH
Promover o controle e a participação social	Inauguração da nova Ouvidoria e divulgação	PR	192
	Palestras e ações de sensibilização do público interno quanto à atuação da Ouvidoria como ambiente de participação e unidade de promoção da integridade	PR	1536
	Produção de materiais de apoio (folders, cartilhas e mídia digital	PR e público externo	640
Analisar e responder mensalmente todas as manifestações recebidas no e-OUV dentro do prazo.	Manifestações respondidas/encaminhadas	Manifestante	5000
Acompanhar trimestralmente a Pesquisa de Satisfação do Usuário	Análise das respostas à pesquisa de satisfação	PR e público externo	128
Produzir informações trimestrais em relação às atividades desempenhadas pela Ouvidoria	Relatório	PR	256
Produzir relatório anual de gestão da Ouvidoria	Relatório	PR e público externo	65

Tabela 8 - Ações da Ouvidoria

APÊNDICE III – DEMANDAS EXTERNAS



APÊNDICE IV – METODOLOGIA PARA O PLANEJAMENTO DAS AÇÕES DE CONTROLE BASEADAS EM RISCO

PRESIDÊNCIA DA REPÚBLICA

SECRETARIA DE GOVERNO

SECRETARIA DE CONTROLE INTERNO

NOTA TÉCNICA Nº 42/2016/CGAP/CISET/SG-PR

Apresentação dos resultados da Etapa I das atividades realizadas pelo Grupo de Trabalho responsável por elaborar a proposta de metodologia para o planejamento das ações de controle baseadas em risco.

Senhor Coordenador-Geral,

Faço referência às atividades do Grupo de Trabalho (GT) instituído inicialmente pela Portaria nº 2, de 8 de janeiro de 2016, e posteriormente retomado pela Portaria nº 12, de 28 de março de 2016, para realização de estudos e apresentação de proposta de metodologia a ser considerada, nesta Secretaria de Controle Interno, para o planejamento das ações de controle baseadas em risco.

2. O objetivo geral do trabalho consiste no estudo e na proposição de metodologia, elaborada em consonância com as técnicas de *risk assessment*[1], que possibilite a identificação e avaliação das situações de risco que devam ser consideradas pelas Coordenações-Gerais dessa Secretaria de Controle Interno para a definição de escopo das ações de controle realizadas no âmbito das entidades auditadas, estabelecendo-se um planejamento baseado em risco.

3. A presente nota técnica apresenta os resultados obtidos pelo GT na Etapa I, segundo a Nota Técnica nº 10/2016/CGAP/CISET/SG-PR, referente à realização de pesquisa bibliográfica e normativa a respeito de Gerenciamento de Riscos, Auditorias baseadas em risco e demais temas correlatos às áreas de planejamento, auditoria e riscos; e à proposição de esboço da referida metodologia.

[1] - Para os efeitos da Norma ABNT NBR ISO 31000:2009 o termo *risk assessment* foi traduzido como "processo de avaliação de riscos" (item 2.14 da norma) para evitar conflito com o termo *risk evaluation*, que foi traduzido como "avaliação de riscos" (item 2.24 da norma).

I - CONSIDERAÇÕES INICIAIS

4. Para alcançar os objetivos desse trabalho, o GT buscou aprofundar os conhecimentos sobre o tema e propor uma metodologia similar às praticadas pelo Tribunal de Contas da União (TCU) e Controladoria-Geral da União (CGU) e fundamentada nos princípios do Comitê das Organizações Patrocinadoras da Comissão *Treadway*[2] (COSO), bem como em normas nacionais e internacionais.

5. A pesquisa bibliográfica foi realizada em publicações disponíveis na internet, cursos, apresentações, manuais e normativos elaborados por órgãos de controle e entidades internacionais, visando à construção do arcabouço teórico necessário à proposição de uma metodologia.

6. Apresentam-se a seguir os principais conceitos que embasaram o trabalho de construção metodológica desse GT.

II - REVISÃO BIBLIOGRÁFICA

7. A revisão bibliográfica prevista nos trabalhos do GT teve como objetivo resgatar conceitos básicos e fundamentais para a atividade de planejamento e auditoria.

A) ACCOUNTABILITY

8. O termo *accountability* por diversas vezes é traduzido para a língua portuguesa como *responsabilização* ou *prestação de contas*. Contudo, essas definições restringem a amplitude real alcançada pelo termo.

9. Considerando a composição terminológica, observa-se que a palavra *accountability* refere-se à forma substantivada do termo da língua inglesa *account*, que em português significa *calcular*, *contar*. Logo, poderia ser traduzido como *aquilo que pode ser contado*, *calculado*.

10. *DE ACORDO COM O DOCUMENTO* NORMAS DE AUDITORIA DO TRIBUNAL DE CONTAS DA UNIÃO, *O TCU CONCEITUA accountability COMO SENDO obrigação de responder por uma responsabilidade outorgada*, cuja definição foi extraída do Manual de Auditoria Integrada do Escritório do Auditor-Geral do Canadá (OAG).

11. Infere-se que o termo corresponde a algo mais amplo do que o ato de prestação de contas ou à possibilidade de responsabilização de alguém, consistindo, na verdade, em uma relação bilateral, sintagmática, em que existe uma reciprocidade entre as obrigações das partes*: uma que delega a responsabilidade e outra que a aceita, mediante o compromisso de prestar contas sobre como essa responsabilidade foi cumprida*[3].

---

[2] - *Committee of Sponsoring Organizations of the Treadway Commission*.

[3] NORMAS DE AUDITORIA DO TRIBUNAL DE CONTAS DA UNIÃO (NAT), FOLHA 11, NOTA DE RODAPÉ 1.

12. Nessa linha, a Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI)[4], quando da apresentação da norma *ISSAI 20 - Principles of transparency and accountability*[5], relacionou o conceito de *accountability* ao conceito de transparência[6], visto que ambos compreendem ações que possibilitem a transparência das informações e realizações do delegatário.

13. Em termos práticos, vislumbra-se uma instituição em que a alta administração delega responsabilidades a seus subordinados que aceitam e se comprometem a prestar conta de suas ações. Embora, inicialmente, essa relação tenha se firmado baseada em confiança, ela provoca dúvidas no delegante, que passa a buscar uma ferramenta que lhe forneça a segurança de que as ações do delegatário estão sendo realizadas da forma adequada para o alcance dos resultados esperados pelo delegante.

14. Surge então a figura do fiscalizador, atuando de forma independente, na relação de *accountability* para reduzir as incertezas do delegante.

B) *ACCOUNTABILITY* NO SETOR PÚBLICO

15. No setor público, a relação de *accountability* pode ser facilmente verificada na relação de delegação de poder estabelecida entre sociedade/cidadão e os agentes políticos eleitos, que por sua vez delegam a outros agentes da administração pública a realização de ações que visam atender aos anseios sociais, devendo esses prestar contas na forma do parágrafo único do artigo 70 da Constituição Federal, que dispõe:

> Prestará contas qualquer pessoa física ou jurídica, pública ou privada, que utilize, arrecade, guarde, gerencie ou administre dinheiros, bens e valores públicos ou pelos quais a União responda, ou que, em nome desta, assuma obrigações de natureza pecuniária.

16. Ocorre que a distância entre delegante e delegatário no setor público é ainda maior se comparado a qualquer instituição. Por isso, o legislador constituinte, visando fortalecer a relação de *accountability* do setor público brasileiro, estabeleceu na estrutura de governança da administração pública mecanismos de fiscalização, conforme artigo 70 da Constituição Federal, transcrito a seguir:

> Art. 70. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta,(...) será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder.

17. Nesse contexto, a atuação do controle externo e interno visa fornecer segurança aos delegantes do poder público, seja em nível de sociedade (controle externo), seja em nível de instituição (controle interno), sendo que a segurança em nível de instituição contribui para a em nível de sociedade.

C) CONTROLE INTERNO

[4] *International Organization of Supreme Audit Institutions*.

[5] Conceito apresentado na ISSAI 20 - *Principles of transparency and accountability*. As ISSAIs são Normas Internacionais das Entidades Fiscalizadoras Superiores (*International Standards of Supreme Audit Institutions – ISSAI*), emitidas pela INTOSAI.

[6] ISSAI 20 - *Principles of transparency and accountability*: *"Accountability and transparency are not easily separated: they both encompass many of the same actions, for instance, public reporting."*

18. Segundo COSO, em seu modelo *Controle Interno – Estrutura Integrada* (1992), controle interno é definido como *um processo realizado pela diretoria, por todos os níveis de gerência e por outras pessoas da entidade, projetado para fornecer segurança razoável quanto à consecução de objetivos nas seguintes categorias: a) eficácia e eficiência das operações; b) confiabilidade de relatórios financeiros; e c) cumprimento de leis e regulamentações aplicáveis.*

19. Esse modelo mudou o conceito considerado tradicional de "controles internos" e evidenciou o fato de que eles tinham de fornecer proteção contra eventos que viessem a ocorrer e afetassem de modo adverso o alcance dos objetivos da entidade. Assim, introduziu-se a noção de que controles internos deviam ser ferramentas de gestão e monitoramento de riscos em relação ao alcance dos objetivos, e não apenas dirigidos para riscos de origem financeira ou vinculados a resultados escriturais. De fato, ampliou-se o papel do controle interno.

20. Outros organismos internacionais incorporaram a ideia central desse novo conceito, conforme se observa na definição trazida pelo Comitê de Procedimentos de Auditoria do Instituto Americano de Contadores Públicos Certificados (AICPA)[7], de que controle interno consiste na atividade realizada para assegurar o cumprimento de algo de acordo com o planejado.

21. Contudo, com a ocorrência de escândalos econômico-financeiros e contábeis envolvendo organizações de todos os portes, houve um aprimoramento para um modelo que desse uma maior importância ao gerenciamento de riscos. Com isso, o COSO publicou em 2004 o Gerenciamento de Riscos Corporativos – Estrutura Integrada, também conhecido como ERM[8] ou COSO II.

22. Também em 2004, a INTOSAI publicou a revisão das *Diretrizes para as Normas de Controle Interno do Setor Público* (2004), alinhando-as ao COSO, e adotou a seguinte definição para controle interno:

> ... processo integrado efetuado pela direção e corpo de funcionários, estruturado para enfrentar os riscos e fornecer razoável segurança de que na consecução da missão da entidade os seguintes objetivos gerais serão alcançados:
>
> a. execução ordenada, ética, econômica, eficiente e eficaz das operações;
>
> b. cumprimento das obrigações de accountability;
>
> c. cumprimento das leis e regulamentos aplicáveis;
>
> d. salvaguarda dos recursos para evitar perda, mau uso e dano.

23. Alinhados também a esses conceitos, a CGU e o TCU publicaram as seguintes definições:

> **CGU (na Instrução Normativa SFC 1/2001, p. 67):**
>
> Controle interno administrativo é o conjunto de atividades, planos, rotinas, métodos e procedimentos interligados, estabelecidos com vistas a assegurar que os objetivos das unidades e entidades da administração pública sejam alcançados, de forma confiável e concreta,

[7] *American Institute of Certified Public Accountant*

[8] *Enterprise Risk Management – Integrated Framework.*

> evidenciando eventuais desvios ao longo da gestão, até a consecução dos objetivos fixados pelo Poder Público.
>
> **TCU (no Glossário de Termos do Controle Externo, 2012):**
>
> Processo efetuado pela administração e por todo o corpo funcional, integrado ao processo de gestão em todas as áreas e todos os níveis de órgãos e entidades públicos, estruturado para enfrentar riscos e fornecer razoável segurança de que, na consecução da missão, dos objetivos e das metas institucionais, os princípios constitucionais da administração pública serão obedecidos e os seguintes objetivos gerais de controle serão atendidos:
>
> I – eficiência, eficácia e efetividade operacional, mediante execução ordenada, ética e econômica das operações;
>
> II – integridade e confiabilidade da informação produzida e sua disponibilidade para a tomada de decisões e para o cumprimento de obrigações de *accountability*;
>
> III – conformidade com leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria instituição;
>
> IV – adequada salvaguarda e proteção de bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida".
>
> V – salvaguardar os ativos financeiros e físicos quanto à boa e regular utilização e assegurar a legitimidade do passivo;
>
> VI – permitir a implementação de programas, projetos, atividades, sistemas e operações, visando à eficácia, à eficiência e à economicidade na utilização de recursos; e
>
> VII – assegurar a aderência das atividades às diretrizes, planos e normas e procedimentos da unidade/entidade.

24. Observa-se que o controle interno consiste em um processo, um sistema, que envolve todos os setores e atividades de uma instituição, visando melhores resultados na busca de seus objetivos, considerados os riscos existentes.

25. A verificação da eficácia e eficiência desse sistema deve ser executada periodicamente, possibilitando segurança para a alta administração e clientes da instituição de que esta caminha para o alcance de seus objetivos. Essa atividade deve ser realizada por unidade interna à instituição, visando assessorar a alta administração no aprimoramento dos controles da gestão organizacional.

26. No Brasil, por vezes o conceito de controle interno como um sistema acima apresentado se confunde com o sistema de controle interno responsável pela fiscalização da administração pública nacional, em decorrência da tradição normativa e doutrinária brasileira, inclusive pelo estabelecido nos arts. 70 e 74 da Constituição Federal, transcritos a seguir: (grifos adicionados)

> Art. 70. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo **sistema de controle interno de cada Poder**.
>
> (...)

> Art. 74. Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, **sistema de controle interno** com a finalidade de:
>
> I - avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União;
>
> II - comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado;
>
> III - exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;
>
> IV - apoiar o controle externo no exercício de sua missão institucional.
>
> § 1º Os **responsáveis pelo controle interno**, ao tomarem conhecimento de qualquer irregularidade ou ilegalidade, dela darão ciência ao Tribunal de Contas da União, sob pena de responsabilidade solidária.
>
> § 2º Qualquer cidadão, partido político, associação ou sindicato é parte legítima para, na forma da lei, denunciar irregularidades ou ilegalidades perante o Tribunal de Contas da União.

27. Deve-se ter em mente que a expressão "**controle interno**" utilizado no §1º do art. 74 da CF refere-se aos **órgãos de controle** inseridos no Poder Executivo, Legislativo ou Judiciário, ou seja, às unidades que desempenham o papel de auditoria interna governamental dos Poderes[9]. Por isso o adjetivo "interno" é empregado para diferenciar do **controle externo** delegado aos tribunais de contas.

28. Por outro lado, a expressão "**sistema de controle interno**" utilizada nos arts. 70 e 74, caput, é mais abrangente, englobando tanto a atividade de controle exercida pelos órgãos de controle interno (atividades avaliativas), quanto o controle interno da gestão organizacional.

29. Para evidenciar essa diferenciação, a CGU utiliza as expressões **controle interno avaliativo**, a cargo dos órgãos de controle interno, e **controle interno administrativo**, de responsabilidade dos gestores.

30. Ressalta-se que as **unidades de controle interno de órgãos públicos e de auditoria interna** de entidades da administração indireta não são o próprio controle interno (ou um sistema de controle) das instituições em que estão inseridas, embora deles sejam parte. Ademais, segundo o Instituto dos Auditores Internos (IIA [10]), eles **desempenhem as atividades de auditoria interna**, auxiliando *a organização a manter controles efetivos a partir da avaliação sua eficácia e eficiência e da promoção de melhorias contínuas*.

31. Na publicação *Estrutura Internacional de Práticas Profissionais* – IPPF[11], o IIA apresenta ainda a seguinte definição para a atividade de auditoria interna:

---

[9] O Sistema de Controle Interno do Poder Executivo Federal é o único até então instituído formalmente, por meio do Decreto nº 3.591/2000, apesar de a Constituição prever, no artigo 74, que os demais poderes também devam manter um sistema.

[10] *Institute of Internal Auditors*. Normas Internacionais para a Prática Profissional da Auditoria Interna, 2010.

[11] INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK.

> A auditoria interna é uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma organização a realizar os 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.

32. O conceito também consta no Glossário das Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI)[12], publicado pela INTOSAI:

> Um meio funcional que permite aos administradores de uma entidade receber, de fontes internas, a segurança de que os processos pelos quais são responsáveis funcionam de modo tal que fiquem reduzidas ao mínimo as probabilidades de que se produzam fraudes, erros ou práticas ineficientes e antieconômicas. Possui muitas das características da auditoria externa, mas pode, corretamente, cumprir instruções do nível de direção a que responde.

33. Em âmbito nacional, o Conselho Federal de Contabilidade (CFC) e os órgãos federais de controle, CGU e TCU, apresentaram o conceito de auditoria interna, conforme transcrições a seguir:

> **CFC (na Norma Brasileira de Contabilidade - NBC TI 01)**
>
> A Auditoria Interna compreende os exames, análises, avaliações, levantamentos e comprovações, metodologicamente estruturados para a avaliação da integridade, adequação, eficácia, eficiência e economicidade dos processos, dos sistemas de informações e de controles internos integrados ao ambiente, e de gerenciamento de riscos, com vistas a assistir à administração da entidade no cumprimento de seus objetivos.
>
> A atividade da Auditoria Interna está estruturada em procedimentos, com enfoque técnico, objetivo, sistemático e disciplinado, e tem por finalidade agregar valor ao resultado da organização, apresentando subsídios para o aperfeiçoamento dos processos, da gestão e dos controles internos, por meio da recomendação de soluções para as não-conformidades apontadas nos relatórios.
>
> **CGU (na Instrução Normativa – SFC nº 01/2001)** (grifos adicionados)
>
> 1. A auditoria interna constitui-se em um conjunto de procedimentos, tecnicamente normatizados, que funciona por meio de **acompanhamento indireto de processos, avaliação de resultados e proposição de ações corretivas** para os desvios gerenciais da entidade à qual esta vinculada. Os trabalhos de auditoria interna são executados por unidade de auditoria interna, ou por auditor interno, especialmente designado para a função, e tem como característica principal assessoramento à alta administração da entidade, buscando agregar valor à gestão.
>
> 2. Para os fins desta Norma, considera-se que unidade de auditoria interna é aquela pertencente à estrutura organizacional de entidades da Administração Pública Federal Indireta ou aos entes paraestatais de cooperação com o Poder Público que realizam serviços sociais autônomos.
>
> **TCU (na Instrução Normativa nº 63/2010)** (grifos adicionados)
>
> Órgãos de controle interno: unidades administrativas, integrantes dos sistemas de controle interno da administração pública federal, incumbidas, entre outras funções, da **verificação da consistência e qualidade dos controles internos**, bem como do apoio às atividades de controle externo, exercidas pelo Tribunal.

[12] *International Standards of Supreme Audit Institutions.*

34. Diante dos conceitos apresentados, observa-se que o controle está diretamente ligado aos conceitos de objetivo (algo que se planejou atingir ou se estabeleceu para ser cumprido), de resultado (o que foi realizado em função dos objetivos estabelecidos) e, consequentemente, de risco, conforme detalhado a seguir.

D) RISCO

35. O conceito de risco foi definido por diversas instituições internacionais importantes para os estudos das atividades de auditoria:

> **IIA (*in* The Role of Internal Auditing in Enterprise-Wide Risk Management, 1999)**
>
> A possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade.
>
> **Committee OB-007, Risk Management (*in* AS/NZS ISO 31000:2009)** (adaptado)
>
> Efeito de incerteza nos objetivos, podendo ser positivo e/ou negativo, sendo caracterizado por potenciais eventos e consequências, ou sua combinação, e medido em termos de impacto e probabilidade.

36. O COSO[13] também traz o conceito de risco, definindo-o como a possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos. Este Comitê trata o conceito de evento como sendo um incidente ou uma série de incidentes resultantes de fatores internos ou externos à organização, que possam afetar a implementação da estratégia e o alcance dos objetivos.

37. Em âmbito nacional, cabe mencionar os conceitos estabelecidos pela Associação Brasileira de Normas Técnicas (ABNT) e pelo TCU:

> **ABNT (na NBR ISO 31000-2009)**
>
> Risco é o efeito da incerteza nos objetivos.
>
> NOTA 1 Um efeito é um desvio em relação ao esperado – positivo e/ou negativo.
>
> NOTA 2 Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).
>
> NOTA 3 O risco é muitas vezes caracterizado pela referência aos eventos (2.17) potenciais e às consequências (2.18), ou uma combinação destes.
>
> NOTA 4 O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade (2.19) de ocorrência associada.
>
> NOTA 5 A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

[13] No modelo Gerenciamento de Riscos Corporativos – Estrutura Integrada (2004), também conhecido como ERM (*Enterprise Risk Management – Integrated Framework*) ou COSO II.

TCU (na Instrução Normativa nº 63, de 01/01/2010)

Risco: possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades.

38. Todos os conceitos aqui apresentados carregam a noção de que os riscos estão relacionados aos objetivos de uma organização. Por conseguinte, a identificação dos riscos, sua avaliação e resposta exige necessariamente o conhecimento prévio dos objetivos a serem alcançados.

39. Do exposto, pode-se dizer que risco é um evento futuro e incerto ao qual toda instituição, pública ou privada, está sujeita e resulta de fatores internos ou externos à organização, podendo exercer forte efeito positivo ou negativo no alcance dos objetivos pretendidos e sendo medido em termos de impacto e probabilidade.

40. Sobre "impacto" o COSO o define como sendo o efeito da ocorrência de um determinado evento, de forma que esse efeito pode ser negativo, positivo ou neutro. Os impactos considerados negativos são os que representam ameaças ao cumprimento dos objetivos organizacionais, representando obstáculos à criação de valor ou desgastando o valor existente, originando-se até mesmo de condições aparentemente positivas, como nos casos de demanda por produto ou serviço superior à capacidade de atendimento.

41. Por outro lado, os impactos notadamente positivos podem contrabalancear os negativos e também representar oportunidades, influenciando favoravelmente o alcance das metas e sendo direcionados de volta para os processos de fixação de estratégias ou objetivos.

42. Portanto, o evento que gera influências positivas para a organização por vezes é denominado "oportunidade", e o que tem consequências negativas como "ameaça", sendo este um dos aspectos fundamentais a serem considerados quando se trata de planejamento de auditoria.

43. De acordo com o Escritório Geral de Contabilidade (GAO)[14], uma vez definidos os objetivos, o órgão deve identificar os riscos que poderiam impedir seu alcance e analisá-los em relação ao seu possível efeito. A direção do órgão deve, então, formular uma abordagem para a gestão de riscos e definir as atividades de controle interno necessárias para mitigá-los.

E) GERENCIAMENTO DE RISCOS

44. Primeiramente, cabe ressaltar que o enfrentamento aos riscos é de responsabilidade da entidade, prevenindo ou detectando sua materialização, conforme as *Diretrizes para as Normas de Controle Interno do Setor Público (2004)* publicadas pela INTOSAI, segundo a qual *controle interno é um processo integrado efetuado pela direção e corpo de funcionários estruturado para enfrentar os riscos e fornecer razoável segurança de que, na consecução da missão da entidade, os seguintes objetivos serão alcançados (...)*. (grifo adicionado)

45. Para o TCU, o gerenciamento de riscos consiste em um método sistemático de identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos, a fim de manter o grau de exposição

[14] *Government Accountability Office*, em GAO-01-1008G - Ferramentas de Gestão e Avaliação de Controle Interno, 2001.

da organização a riscos em nível aceitável, podendo-se gerenciar riscos com a redução da possibilidade de ocorrência do evento indesejado ou minimização do impacto sobre os objetivos.

46. Já a ABNT, conforme a NBR ISO 31000-2009, conceitua gestão de riscos como *atividades coordenadas para dirigir e controlar uma organização no que se refere aos riscos,* podendo ser aplicada a toda uma organização, a qualquer momento. Em termos gerais, *"**gestão de riscos**" refere-se à arquitetura (princípios, estrutura e processo) para gerenciar riscos eficazmente, enquanto que "**gerenciar riscos**" refere-se à aplicação dessa arquitetura para riscos específicos*. (grifos adicionados)

47. Diante desses conceitos, a administração do risco tem por diretiva que risco é uma opção e não um destino, portanto devem ser assumidos, mitigados (entende-se por alocados, controlados, compartilhados ou financiados) ou, simplesmente, evitados.

48. Esse risco pode ser classificado de duas formas distintas: **risco inerente**, que é aquele relativo ao risco do negócio, do processo ou da atividade, independente dos controles adotados; e **risco residual**, o que ainda permanece após a adoção dos controles necessários para combatê-lo. A assunção de um risco inerente pressupõe a tomada de medidas negociais ou de controle por parte da entidade visando reduzi-lo, podendo ou não remanescer o chamado risco residual.

49. O COSO [15] buscou estabelecer uma metodologia para um processo completo de gerenciamento de riscos, partindo da seguinte definição:

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicando no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

50. O modelo traz, no formato de uma matriz tridimensional (ilustração abaixo, conhecida como Cubo COSO II), os elementos que devem constituir um sistema de controle interno considerado eficaz, apoiado numa estrutura de gerenciamento de riscos, ampliando o alcance dos controles internos ao apresentar um enfoque maior ao tema.

[15] No modelo Gerenciamento de Riscos Corporativos – Estrutura Integrada (2004), também conhecido como ERM (*Enterprise Risk Management – Integrated Framework*) ou COSO II.

Figura 1: Elementos do COSO II

51. Para o COSO a relevância do gerenciamento do risco é apresentada da seguinte forma:

> A premissa implícita no gerenciamento do risco empresarial é que toda entidade, seja ela lucrativa, não-lucrativa ou pertencente ao governo, existe para prover valor a seus grupos interessados. Todas as entidades enfrentam incerteza, e o desafio da gerência é determinar quanta incerteza a entidade está preparada para aceitar na sua tentativa de crescer o valor provido a seus grupos interessados. A incerteza significa tanto riscos quanto oportunidades, com o potencial de corroer ou incrementar o valor. O gerenciamento de risco empresarial fornece um modelo para que a gerência efetivamente lide com a incerteza e seus riscos e oportunidades associados e, mediante isso, aumente sua capacidade de produzir valor.

52. Alinhada a esse modelo, a INTOSAI[16] menciona que o processo de avaliação e gerenciamento de riscos envolve os seguintes aspectos: (grifos adicionados)

> **Identificação do risco**: relacionado com os objetivos da unidade; abrangente; inclui riscos devidos a fatores externos e internos, tanto no nível da entidade, quanto de suas atividades;
>
> **Mensuração do risco**: estimativa da importância do risco; avaliação da probabilidade de ocorrência do risco;
>
> **Avaliação da tolerância da organização ao risco**;
>
> **Desenvolvimento de respostas**: quatro tipos de resposta ao risco devem ser considerados: transferência, tolerância, tratamento ou eliminação. Entre eles, o tratamento do risco é a mais relevante para essas diretrizes, porque um controle interno eficaz é o melhor mecanismo para tratar o risco.

53. Assim, a identificação de riscos pela administração tem como objetivo reconhecer os eventos potencialmente capazes de afetar a execução da estratégia ou o alcance dos objetivos, independente do impacto ser favorável ou não. Dessa forma, permite-se identificar não apenas eventos com potencial impacto negativo, mas também aqueles que representam oportunidades a serem aproveitadas.

[16] *Guidelines for Internal Control Standards for the Public Sector*, 2004, p.22.

54. Ademais, os eventos podem ser identificados independentemente da avaliação de sua probabilidade de ocorrência, pois os que representem elevado impacto devem ser considerados mesmo que tenha possibilidade de ocorrência relativamente baixa.

55. Como toda organização enfrenta uma série de riscos que podem afetar suas diversas áreas, o exame da relação entre a probabilidade e o impacto dos riscos representa uma peça fundamental para que as organizações desenvolvam, implementem e melhorem continuamente sua estrutura . Cabe então à administração não apenas gerir os riscos individuais, mas também entender os impactos inter-relacionados.

56. Logo, a gestão de riscos deve oferecer respostas eficazes aos impactos, além de respostas integradas aos diversos riscos, o que requer a avaliação destes em termos de sua probabilidade de ocorrência e impacto potencial de forma a determinar o modo pelo qual deverão ser administrados.

57. Ao determinar respostas a riscos, a administração deverá levar em conta seus efeitos em potencial sobre a probabilidade e o impacto, assim como seus **custos** e **benefícios**, optando pelas respostas compatíveis com a **tolerância a risco da organização** [17] , definida pela alta administração. As respostas adotadas podem englobar medidas para reduzir a probabilidade ou o impacto dos riscos, transferência da probabilidade ou do impacto dos riscos pelo compartilhamento de uma porção do risco (por exemplo, com a contratação de seguro) ou até mesmo aceitar o risco, não adotando nenhuma medida para enfrentar a probabilidade ou o grau de impacto dos riscos.

58. Para auxiliar esse processo de gerenciamento, principalmente para a primeira fase referente à identificação dos riscos, pode-se desenvolver uma matriz, na qual é possível visualizar graficamente a probabilidade de ocorrência de um risco e seu respectivo impacto aos objetivos, auxiliando na definição de quais são os riscos relevantes.

59. Essa matriz é elaborada a partir da aplicação da estrutura integrada de gerenciamento de riscos apresentada no modelo COSO II. Combinando algumas das técnicas da estrutura, é possível a categorização de eventos observados em trabalhos passados de auditoria, de forma a permitir a avaliação do risco que esses eventos representam para os processos e macroprocessos.

60. Segundo o supracitado modelo, *via de regra, as estimativas de probabilidade e grau de impacto de riscos são conduzidas utilizando dados de eventos passados observáveis, os quais fornecem uma base mais objetiva do que as estimativas inteiramente subjetivas.*

61. A avaliação dos riscos é inerentemente subjetiva, não se esperando que os mesmos sejam medidos independentemente da mentalidade, cultura, política e visão do mundo de quem os avalia. Dessa forma, em toda análise realizada existirá um grau de subjetividade, e isso não invalida seus resultados (HILL, 2006, apud Kochi, 2011)[18].

[17] A tolerância ao risco é a quantidade de riscos que uma entidade está preparada para assumir, antes de julgar sobre a necessidade de implementar uma ação. O desenvolvimento de respostas a riscos deve levar em consideração a quantidade de riscos que podem ser tolerados. Tanto riscos inerentes quanto aos riscos residuais devem ser considerados para determinar a tolerância ao risco (INTOSAI. *Guidelines for Internal Control Standards for the Public Sector*, 2004, p. 25).

[18] *Oportunidade de Aplicação de Matriz de Risco no Planejamento de Auditorias na SFC*, Brasília, 2011.

62. Essa avaliação pode se dar por meio de técnicas qualitativas, quantitativas ou pela combinação de ambas. No modelo COSO II, critérios subjetivos podem ser empregados em modelos não probabilísticos com o objetivo de prever impactos de eventos, baseando-se a avaliação do impacto em dados históricos ou simulações. Por exemplo, pode-se utilizar a técnica qualitativa de medição ordinal, na qual são relacionados os eventos em ordem de importância a partir da utilização de rótulos, como alto, médio ou baixo.

G) O PAPEL DA AUDITORIA INTERNA EM RELAÇÃO AOS RISCOS

63. No que se refere ao papel da auditoria com relação a riscos e controles, de acordo com o IIA, *os auditores internos devem exercer o zelo profissional devido levando em consideração*: (...) *a adequação e a eficácia dos processos de governança, gerenciamento de riscos e controles* (...) (ND 1220.A1 das IPPFs do IIA), *além de* (...) *estar alertas aos riscos significativos que poderiam afetar os objetivos, as operações e os recursos*. (ND 1220.A3 das IPPFs do IIA).

64. Ainda para o IIA, *a atividade de auditoria interna deve auxiliar a organização a manter controles efetivos a partir da avaliação da sua eficácia e eficiência e da promoção de melhorias contínuas*. (ND 2130 das IPPFs do IIA).

65. O TCU vem abordando o tema em Decisões Normativas[19], que orientam a atuação dos órgãos do controle interno no processo de prestação de contas anuais dos diversos órgãos da administração pública, com a seguinte determinação: *o órgão de controle interno deve utilizar abordagem baseada em risco para definição do escopo da auditoria e da natureza e extensão dos procedimentos a serem aplicados*.

66. Nessa mesma linha tem sido feitas recomendações como a do Acórdão nº 821/2014-Plenário, referente à auditoria operacional realizada por sua Secretaria de Controle Externo no Estado do Rio de Janeiro em Unidades de Auditoria Interna, Assessorias de Controle Interno e Unidades de Controle Interno das entidades e órgãos da Administração Pública Federal sob sua jurisdição, conforme transcritas a seguir:

> **à Companhia Docas do Rio de Janeiro (CDRJ)**:
>
> *estruture mais adequadamente as práticas de planejamento estratégico adotadas pela organização, com vistas à implementação futura de uma gestão orientada à governança e à gestão de risco;*
>
> *promova estudos com vistas a estruturar um sistema de controle interno que enseje a identificação dos riscos mais significativos para os objetivos da organização e o desenvolvimento de controles internos voltados à mitigação ou eliminação desses riscos;*
>
> **à unidade de auditoria interna da CDRJ:**
>
> *procure adequar os períodos de trabalhos de auditoria à complexidade dos trabalhos a serem realizados e com o risco, relevância e materialidade dos objetos fiscalizados;*
>
> *(...)*

[19] art. 9º, § 1º da Decisão Normativa-TCU 132/2013 e da DN-TCU 147/2015.

> *avalie o desempenho das suas atividades de fiscalização adotando as seguintes práticas dentre outras: avaliar a relação custo/benefício de seus trabalhos, monitorar a qualidade de suas auditorias e avaliar a economicidade e eficiência dos procedimentos de fiscalização adotados;*

67. Considerados todos os conceitos aqui expostos e a extensa bibliografia pesquisada, apresenta-se o esboço da metodologia a ser considerada para o planejamento das ações de controle baseadas em risco pela CISET/SG-PR.

III - PROPOSTA DE METODOLOGIA

68. O cerne da presente proposta metodológica é permitir às Coordenações-Gerais desta Secretaria de Controle Interno identificar **os temas relevantes, críticos** ou **de maior impacto** das entidades sob sua área de atuação por meio de uma avaliação de riscos, possibilitando, então, realizar o planejamento das ações de controle.

69. De acordo com o exposto, essa linha de atuação vai ao encontro das Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI), que dispõem sobre a necessidade de se *avaliar as respostas da administração aos riscos identificados, incluindo o desenho e a implementação de controles internos para tratá-los*[20], bem como da orientação do TCU, de que *o órgão de controle interno deve utilizar abordagem baseada em risco para definição do escopo da auditoria e da natureza e extensão dos procedimentos a serem aplicados*[21].

70. Conforme será detalhado a seguir, essa metodologia divide-se em quatro momentos, perfazendo a visão geral **da entidade** ou **de suas atividades (seja um projeto, processo, macroprocesso, programa ou objeto específico, independentemente de ser finalístico ou de apoio**), sua validação junto aos gestores, identificação dos riscos e definição dos temas mais propícios à execução de ações de controle.

1º MOMENTO – VISÃO GERAL DA ENTIDADE OU DE SUAS ATIVIDADES

71. O primeiro momento consiste em uma fase exploratória que propicie o conhecimento da entidade, do ambiente institucional, de suas atividades e dos controles internos a ela relacionados. Poderá ser realizado em nível de entidade, por meio do qual se busca compreender as características da instituição como um todo, ou em nível de atividade, que objetiva entender seus processos, projetos ou objeto específico.

72. De modo geral, deve-se considerar nessa fase exploratória a identificação de 6 (seis) elementos principais: a) fornecedores; b) insumos; c) requisitos; d) recursos de transformação; e) produtos; e f) clientes. Na figura a seguir são apresentados tais elementos e a forma como se relacionam:

[20] Item 46 da tradução, elaborada pelo Tribunal de Contas da União – TCU, do nível 3 das Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI), desenvolvidas pela INTOSAI.

[21] art. 9º, § 1º da Decisão Normativa - TCU 147/2015.

Figura 2: Visão sistêmica de um processo.

73. Na avaliação **em nível de atividades**, os **fornecedores** poderiam ser entendidos como o grupo de trabalho responsável pelo projeto, a área da instituição responsável por realizar o processo ou a instituição responsável pelas ações de um programa. Já os **clientes** seriam aqueles a quem são destinados os resultados dos projetos, dos processos ou dos programas.

74. Os **requisitos** dizem respeito ao marco regulatório (leis e regulamentos), normativos internos, procedimentos operacionais e padrões de desempenho (metas indicadores de resultados) que interferem diretamente nas ações ou atividades realizadas pela entidade. Por outro lado, os **recursos de transformação** consistem nas ferramentas utilizadas para processar os insumos em produtos.

75. Quanto à avaliação **em nível de entidade**, o qual naturalmente engloba diversos processos, projetos ou programas, deve-se também realizar uma leitura dos 6 (seis) elementos, mas de forma global, descendo ao nível de atividades, quando necessário ou possível, visando a amplitude da visão geral sobre o funcionamento da instituição, o ambiente em que ela atua e os controles internos de que ela se utiliza.

76. Nessa abordagem, no que diz respeito aos **recursos de transformação**, devem ser avaliados: a) colaboradores: a força de trabalho empregada; b) equipamentos: computadores, aparelhos, máquinas utilizadas para o desempenho de suas atividades; c) instalações: o ambiente físico onde são realizadas as atividades; e d) sistemas e *softwares*. Sobre os sistemas e *softwares*, cabe observar se são suficientes, seguros e de que forma impactam no alcance dos objetivos da instituição.

77. Quanto aos **requisitos**, devem ser identificados:

a) leis e regulamentos (as principais atribuições legais, constitucionais ou infraconstitucionais): norma de criação da instituição (e os objetivos de criação nela contidos), código de ética que se aplique a instituição, políticas de governo que envolvam a instituição;

b) normas internas: regimento interno ou estatuto, código de ética ou de conduta, planos estratégicos, organogramas (áreas/setores e suas atribuições, estrutura de governança);

c) procedimentos operacionais: manuais e procedimentos internos, relatórios de gestão, normas de execução, instrumentos de operacionalização, macroprocessos e processos mapeados; e

d) padrões de desempenho: metas e indicadores estabelecidos no PPA ou criados pela própria instituição.

78. Tanto em nível de entidade quanto de atividades, as informações relativas aos elementos mencionados podem ser obtidas em pesquisa nos portais das instituições, mediante indagação à administração (servidores e gestores), observação e inspeção *in loco*, procedimentos analíticos anteriores (análises realizadas pelas auditorias internas, órgãos de controles internos[22] e órgãos de controle externo), análises quantitativas (de informações históricas de atividades, resultados, indicadores, orçamentos), entre outros.

79. As avaliações nesses dois níveis geralmente são realizadas em trabalhos sequenciais, executando-se primeiramente em nível de entidade, a fim de ter uma base sólida do conhecimento da organização da instituição. A partir de então é que se parte para uma abordagem mais específica, no caso em nível de atividade. Tal forma de trabalho é conhecida como *top-down* (de cima para baixo), conforme recomenda a norma AS-2201 (or *Auditing Standard nº 5, Jul/2007)* da *Public Company Accounting Oversight Board* (PCAOB).

80. Entretanto, na prática observa-se que é mais comum a realização de avaliações em nível de atividades sem que tenha sido anteriormente empreendida uma avaliação global, ou seja, em nível de entidade.

81. Conforme dito anteriormente, esse 1º momento refere-se à fase exploratória, na qual geralmente se identifica se a instituição possui ou não seus macroprocessos e/ou processos mapeados. Na sua completa inexistência, o mapeamento deve ser feito mesmo que de forma superficial, visto ser o ponto de partida para a análise de riscos das atividades da instituição.

82. Isso porque os processos ajudam a implementar a estratégia de operação dos negócios e a produzir os resultados que serão entregues aos clientes, refletindo como, de fato, as empresas funcionam. Considerando que os processos são partes integrantes dos macroprocessos, suas falhas irão impactar também os macroprocessos, que, por sua vez, comprometerão o alcance dos objetivos mediatos e imediatos da entidade.

83. Dessa forma, o referido mapeamento auxilia a identificação de pontos fortes e fracos da entidade, dos quais os fracos correspondem aos aspectos que precisam ser melhorados, tais como: complexidade na operação, reduzir custos, gargalos, falhas de integração, atividades redundantes, tarefas de baixo valor agregado, retrabalhos, excesso de documentação e aprovações.

84. Para que se consiga realizar, minimamente, esse mapeamento, devem ser considerados os 6 (seis) elementos mencionados na Figura 2 anterior, quais sejam: fornecedores, insumos, requisitos, recursos de transformação, produtos e clientes. Para obtenção das informações necessárias à identificação desses elementos, as Coordenações-Gerais poderão se utilizar das mesmas técnicas listadas anteriormente:

[22] Análises de denúncias, relatórios de auditoria da gestão, Plano de Providências Permanente – PPP.

entrevistas, questionários, reuniões, workshops, observação de campo, análise da documentação existente e coleta de evidências.

85. Ao final desse primeiro momento, de posse da gama de informações acima mencionada, cada Coordenação-Geral deve identificar os principais pontos fortes e fracos do ambiente interno e externo da entidade ou de suas atividades, que pode ser, conforme ressaltado anteriormente, um projeto, processo[23], macroprocesso[24], programa ou objeto específico, independentemente de ser finalístico ou de apoio.

86. Nessa etapa sugere-se fazer uso da análise SWOT – *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças), que permite realizar uma avaliação do ambiente interno da organização ou de determinada atividade, visando identificar as forças e fraquezas, e do ambiente externo, para apontar as oportunidades e ameaças presentes.

87. De acordo com o TCU[25], *Strengths* (**Forças**) são as características positivas internas que uma organização pode explorar para atingir as suas metas. Referem-se às habilidades, capacidades e competências básicas da organização que atuam em conjunto para ajudá-la a alcançar suas metas e objetivos (Ex.: equipe experiente e motivada, recursos tecnológicos adequados).

88. Já *Weaknesses* (**Fraquezas**) são as características negativas internas que podem inibir ou restringir o desempenho da organização. Referem-se à ausência de capacidades e/ou habilidades críticas. São, portanto, deficiências e características que devem ser superadas ou contornadas para que a organização possa alcançar o nível de desempenho desejado. (Ex.: alta rotatividade de pessoal, sistemas de informação obsoletos, processos internos excessivamente burocratizados.)

89. Sobre *Opportunities* (**Oportunidades**), entende-se por características do ambiente externo, não controláveis pela organização, com potencial para ajudá-la a crescer e atingir ou exceder as metas planejadas. (Ex.: diretrizes governamentais favoráveis ao fortalecimento institucional, novas fontes orçamentárias, parcerias com outras instituições.).

90. Por fim, *Threats* (**Ameaças**) são características do ambiente externo, não controláveis pela organização, que podem impedi-la de atingir as metas planejadas e comprometer o crescimento organizacional. (Ex.: dispersão geográfica do público-alvo, disparidades regionais, conflito de competência.)

91. Ao final, será possível construir uma matriz, conforme exemplificada a seguir:

[23] Entende-se por processo o conjunto de atividades inter-relacionadas ou interativas que transforma insumos (entradas) em produtos (saídas), de acordo com a Associação Brasileira de Normas Técnicas (2005, N. 3.4.1). Sob esse prisma, toda organização pode ser vista como uma coleção de processos que, de forma integrada, atuam para alcançar os objetivos.

[24] Os macroprocessos podem ser finalísticos ou de apoio, sendo finalísticos aqueles relacionados aos objetivos de criação da instituição, na maioria das vezes produzem resultados para o público externo à instituição. Os processos de apoio são os que dão suporte aos processos finalísticos e estão diretamente relacionados à gestão dos recursos necessários ao desenvolvimento de todos os processos da instituição.

[25] - Para maiores informações sobre a técnica de análise SWOT, sugere-se a leitura do documento *Análise SWOT e Diagrama de Verificação de Riscos aplicados em Auditoria*, de autoria do TCU e anexo à Portaria-SEGECEX nº 31, de 9 de dezembro de 2010.

Figura 2: Exemplo de matriz SWOT (fonte: Gestão da Estratégia com uso do BSC. ENAP, 2013)

92. Nesse momento, já será possível ter uma **visão geral da entidade ou de determinada atividade**, inclusive identificando os fatores críticos (fraquezas e ameaças) a ela relacionados. Na sequência, faz-se necessário identificar a estrutura de controle interno utilizada em função do objeto da auditoria, particularmente quanto à existência de política gerenciamento de riscos formalmente instituída, seu grau de atualização e os resultados de sua aplicação.

93. Vale ressaltar que a existência e a qualidade dos controles internos administrativos poderão impactar a matriz SWOT, visto que compõem as forças da organização e muitas vezes equilibram as fraquezas existentes. Caso inexista uma política gerenciamento de riscos, faz-se necessário estabelecer situações mais críticas na construção das fraquezas.

94. A fim de assegurar que a visão construída até o momento sobre a entidade ou de determinada atividade corresponde à realidade, passa-se ao 2º momento correspondente à validação junto aos gestores.

2º MOMENTO – VALIDAÇÃO

95. Nesse 2º momento é primordial que a Coordenação-Geral solicite à entidade reunião com interlocutores que detenham conhecimento sobre os principais macroprocessos ou sobre a atividade objeto do momento anterior, de modo a avaliarem todos os levantamentos realizados na fase exploratória (mapeamento, matriz SWOT, etc.).

96. No caso da visão geral em nível de entidade, a validação deverá ser feita juntamente com o gestor da instituição. Vale ressaltar que, nos casos em que o mapeamento de processos já tiver sido realizado formalmente pela instituição, faz-se necessário avaliar a necessidade de se validar os levantamentos realizados pela Coordenação-Geral. Em se tratando de avaliação em nível de atividade, esta deve ser validada com a autoridade competente pela condução e supervisão do projeto, processo, etc..

97. Com base nas informações levantadas e validadas até então, dá-se sequência à presente metodologia pela identificação dos riscos correspondentes.

3º MOMENTO – IDENTIFICAÇÃO DOS RISCOS

98. O 3º momento caracteriza-se pela identificação dos riscos para a entidade ou relativas à determinada atividade objeto da fase exploratória (pode ser um projeto, processo, macroprocesso, programa ou objeto específico), certificando-se junto à instituição quais são os eventos a ela relacionados.

99. Segundo COSO, *eventos são incidentes ou ocorrências originadas a partir de fontes internas ou externas que afetam a implementação da estratégia ou realização dos objetivos.* Uma das técnicas que podem ser utilizadas para identificação de eventos proposta na metodologia COSO (Santos, 2012) é o inventário de eventos:

> *Inventário de eventos – trata-se da relação detalhada de eventos em potencial comuns às organizações de um cenário industrial, ou para um determinado tipo de processo, ou atividade, comum às indústrias. Alguns softwares podem gerar listas de eventos relevantes originárias de uma base geral de potenciais eventos, que servirão como ponto de partida para se identificar eventos. Por exemplo, uma organização envolvida em um projeto de desenvolvimento de software utiliza-se de uma relação detalhada de possíveis eventos referentes a projetos desse tipo.*

100. Assim, percebe-se que nesse momento é fundamental identificar quais são ou podem ser os principais eventos com potencial de gerar impacto no andamento dos temas já estudados e que, até agora, se mostraram, em tese, relevantes e/ou críticos[26] para que a organização alcance seus objetivos.

101. Essa identificação é realizada por meio de aplicação de metodologia de mapeamento e qualificação dos eventos, os quais podem ser avaliados mediante a atribuição de notas para os critérios de probabilidade, materialidade e relevância. Nessa metodologia, a relevância é definida a partir da observação de que, caso o risco se materialize, qual seria o impacto no alcance dos objetivos de determinada atividade (por exemplo, um macroprocesso) e, consequentemente, da entidade. Leva-se

[26] Abordou-se como sendo uma percepção preliminar quanto à identificação de temas relevantes e/ou críticos em decorrência da própria metodologia aqui apresentada, que busca justamente trazer elementos mais objetivos para tal julgamento. Portanto, trata-se apenas de um julgamento inicial com base na experiência da Coordenação-Geral, associado ao levantamento realizado.

em consideração se o risco seria elevado o suficiente para causar dano significativo, inclusive afetando a imagem da instituição.

102. Para isso pode-se utilizar ferramentas que busquem facilitar a interação da Coordenação-Geral com os gestores e operadores dos processos. Essas ferramentas são as escalas de probabilidade e de impactos, que serão utilizadas posteriormente para a elaboração da Matriz Impacto x Probabilidade. Primeiramente, apresenta-se a seguir a escala de probabilidades.

ESCALA DE PROBABILIDADES		
Frequência	**Descrição**	**Grau**
Muito Baixa	Evento extraordinário para os padrões conhecidos da gestão e operação do processo, praticamente impossível. Embora possa assumir dimensão estratégica para a manutenção do processo, **não há histórico disponível da sua ocorrência**.	1
Baixa	Evento casual, inesperado. É uma surpresa quando ocorrer. **Muito embora raro, há histórico de ocorrência conhecido** pelos principais gestores e operadores do processo.	2
Média	Evento esperado, porque se reproduz com frequência reduzida, porém constante. **Seu histórico de ocorrência é de conhecimento da maioria dos gestores** e operadores do processo.	3
Alta	Evento usual e corriqueiro. Devido à sua **ocorrência habitual ou conhecida em uma dezena ou mais de casos**, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo.	4
Muito Alta	Evento que se repete seguidamente, de maneira assídua, numerosa e não raro de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo. **Quando não ocorre, é uma surpresa**.	5

103. Na elaboração da escala de probabilidades, realizada em colaboração entre a Coordenação-Geral e os representantes da unidade, **não devem ser considerados os controles já existentes**. Nessa atividade **avalia-se o risco inerente ao evento** e, caso os controles instituídos sejam levados em consideração, a avaliação pode ser enviesada ao se considerar que a probabilidade de ocorrência de um evento seria mais baixa do que a realidade.

104. Na ocorrência do evento, o impacto pode ser percebido em diferentes dimensões nos objetivos da entidade ou de determinada atividade. Como exemplo, um risco pode ter maior impacto financeiro, mas não necessariamente um importante impacto na qualidade. Outro aspecto importante para percepção do impacto é a análise das ameaças e das oportunidades de forma separada, conforme tratado anteriormente na técnica SWOT.

105. Assim, as primeiras dimensões de impacto[27] a serem avaliadas são:

a) **Impactos no tempo e nos prazos:** corresponde ao nível de impacto na conclusão da atividade. É positivo no caso de antecipação e negativo quando houver atrasos. Tendo em vista que cada atividade difere em tamanho, complexidade e diversos outros fatores, faz-se necessário confirmar o grau de tolerância considerado apropriado para cada nível de impacto, conforme exemplo abaixo:

ESCALA DE IMPACTO NO TEMPO E NOS PRAZOS		
Impacto	**Descrição**	**Grau**
Muito Baixo	Menos de 15 dias corridos de atraso ou antecipação.	1
Baixo	Atraso/antecipação entre 15 a 60 dias corridos.	2
Médio	Atraso/Antecipação entre 60 a 120 dias corridos.	3
Alto	Atraso/Antecipação entre 120 a 180 dias corridos.	4
Muito Alto	Atraso/Antecipação acima de 180 dias corridos.	5

b) **Impactos nos custos:** trata-se do impacto econômico-financeiro, sendo positivo quando se gera economia e negativo para os eventuais prejuízos. Nos moldes do apresentado para os impactos no tempo e nos prazos, é necessário destacar o grau de tolerância considerado apropriado para cada nível de impacto nos custos, a exemplo da seguinte escala:

ESCALA DE IMPACTO NOS CUSTOS		
Impacto	**Descrição**	**Grau**
Muito Baixo	Variação abaixo de R$ 500 mil	1
Baixo	Variação entre R$ 500 mil e R$ 1 milhão	2
Médio	Variação entre R$ 1 milhão e R$ 2 milhões	3
Alto	Variação entre R$ 2 milhões e R$ 5 milhões	4

[27] - Baseado na publicação *Adopting the quadratic mean process to quantify the qualitative risk analysis* (Vargas, 2013 PMI Global Congress Proceedings).

ESCALA DE IMPACTO NOS CUSTOS		
Impacto	**Descrição**	**Grau**
Muito Alto	Variação acima de R$ 5 milhões	5

c) **Impactos na qualidade:** corresponde ao nível de impacto na qualidade requerida pela atividade. Pode ser positivo ou negativo para forças/oportunidades ou fraquezas/ameaças, respectivamente. Conforme apresentado anteriormente, deve-se considerar o nível de tolerância apropriado, a exemplo da escala para eventos negativos de risco a seguir:

ESCALA DE IMPACTO NEGATIVO NA QUALIDADE		
Impacto	**Descrição**	**Grau**
Muito Baixo	Impacto imperceptível (na maior parte das vezes sequer é percebido pelos gestores)	1
Baixo	Cliente percebe, mas releva e nenhuma ação é necessária.	2
Médio	Cliente percebe e demanda ações/informações.	3
Alto	Cliente demanda por ações corretivas imediatas.	4
Muito Alto	Cliente rejeita a entrega ou produto.	5

d) **Impactos na saúde e segurança organizacional:** esse grupo de impacto pode incluir aspectos referentes ao ambiente de trabalho, à segurança dos dados, à reputação institucional, entre outros. Apresenta-se a seguir exemplo de escala para avaliar os impactos em questão:

ESCALA DE IMPACTO NEGATIVO NA SAÚDE E SEGURANÇA ORGANIZACIONAL		
Impacto	**Descrição**	**Grau**
Muito Baixo	Sem impacto no ambiente/reputação da organização.	1

ESCALA DE IMPACTO NEGATIVO NA SAÚDE E SEGURANÇA ORGANIZACIONAL		
Impacto	**Descrição**	**Grau**
Baixo	Impacto perceptível no ambiente/reputação, mas irrelevante.	2
Médio	Impacto é percebido e surgem preocupações.	3
Alto	Impacto evidente no ambiente/reputação da organização.	4
Muito Alto	Crise. Impacto é tão evidente e público que o processo pode não prosseguir como planejado.	5

e) **Outros impactos:** esse grupo é opcional e objetiva incluir outros impactos de risco que não foram contemplados nos grupos anteriores. É importante ressaltar que o grau desses outros impactos, se existirem, deve variar entre 1 e 5 como os demais grupos.

106. Outra dimensão de impacto a ser considerada é o horizonte de tempo ou proximidade do evento, ou seja, um evento que pode ocorrer em algumas horas requer diferentes ações do que outro evento que pode causar impacto daqui a anos. Assim, se um evento está próximo de ocorrer, este tem maior prioridade se comparado com eventos futuros (neste caso sob o aspecto da proximidade).

107. A escala de proximidade pode ser compatível com outros grupos de impactos (de 1 a 5 pontos para diferentes horizontes de tempo), conforme exemplo adiante. É importante ressaltar que se faz necessário definir o que são eventos imediatos e de curto, médio, longo e longínquo prazo, de forma a se ajustar a escala ao caso concreto.

ESCALA DE IMPACTO DEVIDO À PROXIMIDADE DO EVENTO		
Impacto	**Descrição**	**Grau**
Longínquo	Evento pode ocorrer posterior a 1 ano.	1
Longo prazo	Evento pode ocorrer entre 6 meses a 1 ano.	2
Médio prazo	Evento pode ocorrer entre 3 a 6 meses.	3
Curto prazo	Evento pode ocorrer entre 15 dias a 3 meses.	4
Imediato	Evento pode ocorrer a qualquer tempo nos próximos 15 dias.	5

108. Do exposto, as escalas de impactos, também conhecidas como escalas de consequências, apresentam os efeitos decorrentes de um determinado evento. Como há diferentes aspectos a serem avaliados, sua estimativa final dá-se por meio do cálculo da média quadrática (raiz quadrada da média aritmética dos quadrados dos impactos), conforme a seguinte fórmula:

$$Impacto = \sqrt{\frac{(Impacto\ no\ tempo)^2 + (Impacto\ nos\ custos)^2 + (Impacto\ na\ qualidade)^2 + (Impacto\ na\ segurança)^2 + (outros)^2 + (proximidade)^2}{6}}$$

109. A decisão pela média quadrática ao invés da média aritmética simples dos graus dos impactos baseia-se no conceito de que diferentes níveis de impactos geram exposição adicional ao processo e sua variância pode ser considerada como um fator de risco.

110. Cabe ressaltar que o conceito de variância está diretamente relacionado à dispersão dos diferentes grupos de impactos. Se há grande variação no impacto, a variância será também alta e a diferença entre a proposta pela média quadrática e a tradicional média aritmética aumentará, influenciando o impacto de determinado risco.

111. Os impactos decorrentes de eventos oriundos de fraquezas/ameaças e forças/oportunidades podem ser calculados por meio da mesma fórmula, mas com diferentes sinais ("+" para forças/oportunidades e "–" para fraquezas/ameaças).

112. Do exposto, é possível atribuir o binômio *probabilidade* e *impacto* a todos os eventos relacionados a uma atividade, com cada fator variando de 1 a 5 conforme apresentado anteriormente. Ao se combinar essas duas escalas, é possível determinar uma medida de risco para avaliação e priorização desses eventos, denominada de ***valor esperado***, que é calculada pela multiplicação entre os valores de probabilidade e impacto.

113. Em resumo, apresenta-se a seguir a tabela de identificação de riscos de uma atividade, contemplando as avaliações quanto à probabilidade e impacto para determinação da medida de risco.

EVENTOS ATRELADOS À *SWOT* DA ATIVIDADE		ESCALA DE PROBABILIDADE	DIMENSÕES DE IMPACTO							VALOR ESPERADO (risco)
DESCRIÇÃO	Origem SWOT		Tempo / Prazo	Custos	Qualidade	Saúde / Segurança	Outros	Proximidade	TOTAL	
Evento 1	S_1									
Evento 2	W_1									
Evento 3	O_1									
Evento 4	T_1									
Evento 5	W_2									
Evento ...	T_2									

S – Força; W – Fraqueza; O – Oportunidade; T – Ameaça.

114. No caso de ter sido realizada mais de uma avaliação para um mesmo evento, seja pela equipe de auditores e/ou por integrantes da unidade, sugere-se determinar um único *valor esperado* a partir da aplicação da média quadrática, a exemplo da fórmula indicada anteriormente.

115. Para melhor visualização dos resultados, pode-se construir a matriz de risco, na qual são plotadas as duas variáveis, sendo a probabilidade indicada no eixo das ordenadas (eixo x) e o impacto[28] total no eixo das

28

coordenadas (eixo y). O quadrante indica a medida de risco correspondente, a qual é classificada em baixo, médio, alto e extremo, conforme exemplificado a seguir.

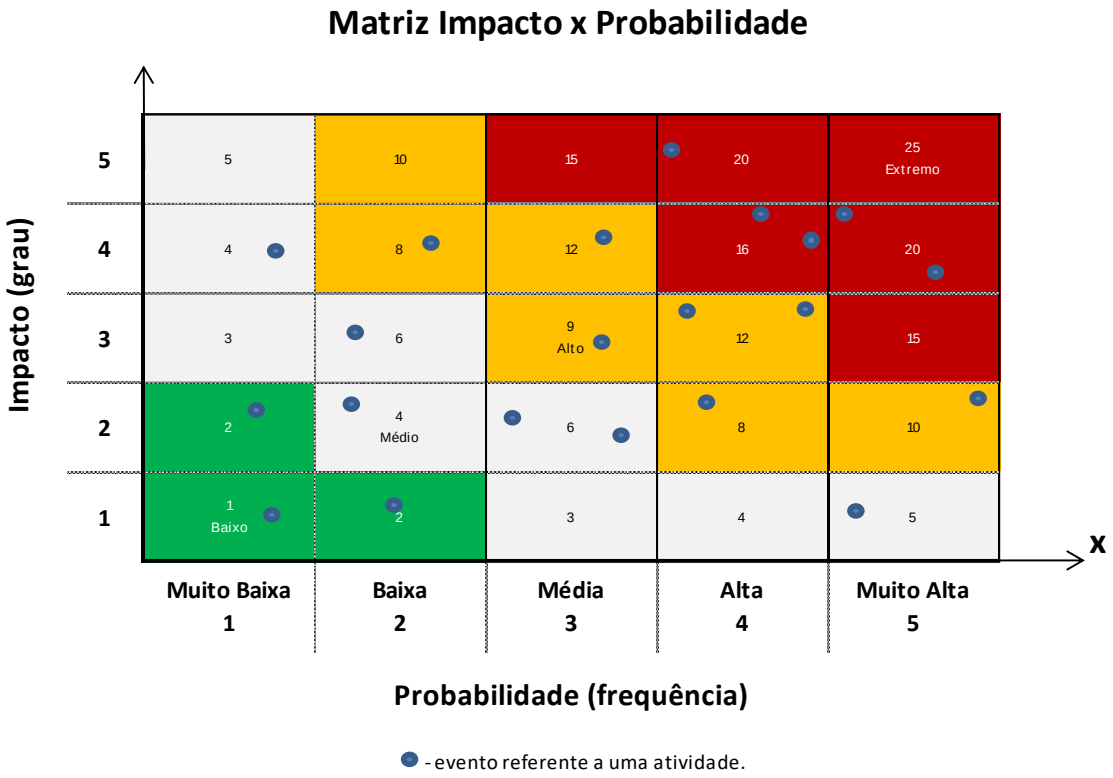


Figura 3: Exemplo de uma matriz de risco.

116. Percebe-se do exemplo acima que a ocorrência de uma gama de **eventos relacionados a uma determinada atividade** pode gerar certa dificuldade na priorização dos riscos segundo a simples interpretação visual da matriz ou mesmo em forma tabular.

117. Outro complicador é a necessidade de se avaliar diversas atividades de uma entidade, o que requer proceder à identificação de riscos aqui apresentada, obtendo assim outras relações de eventos ponderados segundo o binômio *probabilidade* e *impacto*.

118. Ao final do processo busca-se naturalmente identificar quais atividades representam maior exposição ao risco para fins de planejamento das ações de controle.

4º MOMENTO – PRIORIZAÇÃO DOS RISCOS

119. No momento anterior foi apresentada uma série de ferramentas e parâmetros destinados a quantificar uma análise qualitativa de risco dos eventos relacionados às forças/oportunidades e às fraquezas/ameaças no âmbito de uma entidade ou atividade a ela relacionada, seja macroprocesso, processo, projeto, etc.

120. Em se tratando de apenas uma atividade, as medidas de risco (*valores esperados*) calculadas no momento anterior já possibilitam identificar os eventos com maior exposição ao risco, bastando ordená-las de forma descrente e classificá-las em baixo, médio, alto e extremo, segundo a matriz de risco.

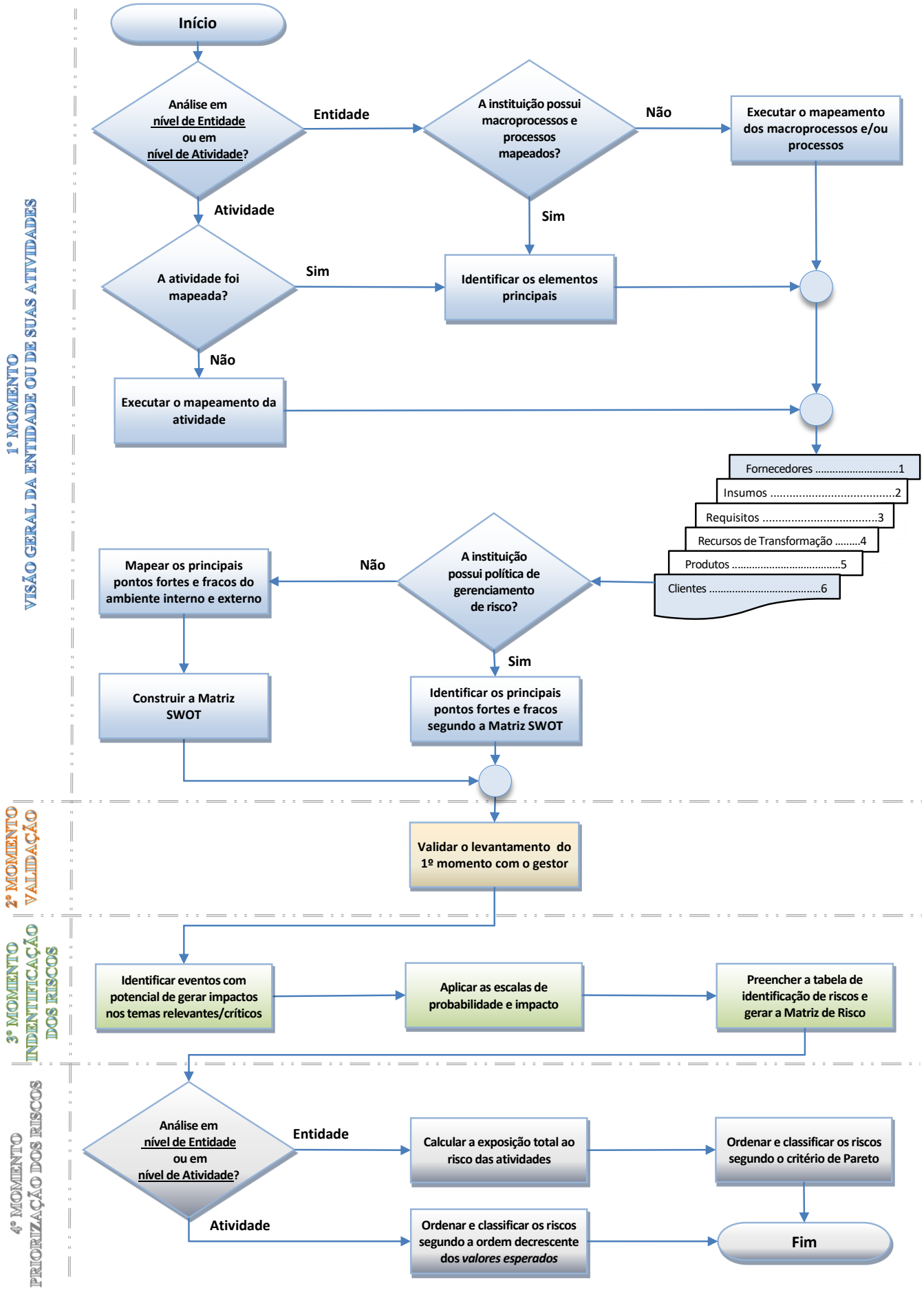
121. No caso de uma avaliação em nível de entidade, onde se analisa mais de uma atividade e, por conseguinte, se identifica uma variedade de eventos com diferentes probabilidades e impactos[29], faz-se necessário determinar uma exposição total ao risco de cada atividade em questão. Tal medida é calculada como sendo a soma dos *valores esperados* (probabilidade x impacto) de todos os eventos relacionados àquela atividade.

122. É interessante destacar que, como os impactos decorrentes de eventos oriundos de fraquezas/ameaças e forças/oportunidades apresentam diferentes sinais ("+" para forças/oportunidades e "–" para fraquezas/ameaças), o cálculo da exposição total ao risco por meio da soma aritmética conjuga esses efeitos, representando assim uma medida confiável.

123. Após a determinação dos valores de exposição total ao risco de todas as atividades em análise, deve-se ordená-los de forma decrescente e classificá-los segundo o critério de Pareto, atribuindo a classificação de *risco alto ou extremo* a 20% dos valores mais altos, de *médio* a 30% dos valores seguintes e de *baixo* a 50% restante.

124. Diante do exposto, é possível identificar quais as atividades são efetivamente relevantes, críticas ou de maior impacto para as entidades segundo essa avaliação da exposição ao risco. A presente metodologia pode ser visualizada no fluxograma apresentado a seguir.

[29] Nesta situação de identificação de riscos referentes a diversas atividades de uma entidade, deve-se considerar as mesmas escalas de impacto definidas para cada uma das seis dimensões.


1° MOMENTO
VISÃO GERAL DA ENTIDADE OU DE SUAS ATIVIDADES
Início
Análise em nível de Entidade ou em nível de Atividade?
Entidade
A instituição possui macroprocessos e processos mapeados?
Não
Executar o mapeamento dos macroprocessos e/ou processos
Atividade
Sim
A atividade foi mapeada?
Sim
Identificar os elementos principais
Não
Executar o mapeamento da atividade
Fornecedores 1
Insumos 2
Requisitos 3
Recursos de Transformação 4
Produtos 5
Clientes 6
A instituição possui política de gerenciamento de risco?
Não
Mapear os principais pontos fortes e fracos do ambiente interno e externo
Sim
Identificar os principais pontos fortes e fracos segundo a Matriz SWOT
Construir a Matriz SWOT
2° MOMENTO
VALIDAÇÃO
Validar o levantamento do 1º momento com o gestor
3° MOMENTO
IDENTIFICAÇÃO DOS RISCOS
Identificar eventos com potencial de gerar impactos nos temas relevantes/críticos
Aplicar as escalas de probabilidade e impacto
Preencher a tabela de identificação de riscos e gerar a Matriz de Risco
4° MOMENTO
PRIORIZAÇÃO DOS RISCOS
Análise em nível de Entidade ou em nível de Atividade?
Entidade
Calcular a exposição total ao risco das atividades
Ordenar e classificar os riscos segundo o critério de Pareto
Atividade
Ordenar e classificar os riscos segundo a ordem decrescente dos valores esperados
Fim

IV - CONCLUSÃO

125. De acordo com os conceitos apresentados e a proposta de metodologia aqui trazida, buscou-se prover as Coordenações-Gerais desta Secretaria de Controle Interno de ferramental capaz de identificar os temas relevantes, críticos ou de maior impacto das entidades sob sua área de atuação por meio de uma avaliação de riscos, possibilitando, então, balizar o planejamento de suas ações de controle.

126. Conforme se depreende das exposições da presente nota técnica, essa metodologia se apresenta, a princípio, versátil, de fácil compreensão e aplicação. No entanto, conforme consta no planejamento das atividades deste GT, a próxima etapa do trabalho será sua aplicação em uma unidade-piloto para fins de validação.

127. De antemão, entende-se como primordial que os levantamentos de informações aqui delineados e os resultados então previstos sejam retroalimentados a cada exercício, de modo a engrandecer o conhecimento sobre o negócio das entidades e aprimorar a identificação de temas de maior relevância e/ou sensíveis para atuação pela CISET/SG-PR ou mesmo pelas próprias auditorias internas.


CISET
Presidência da República
SECRETARIA-GERAL DA
PRESIDÊNCIA DA REPÚBLICA
PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL