CGU

Controladoria-Geral da União

ORIENTAÇÃO PRÁTICA:

Plano de auditoria interna baseado em riscos

Brasília, 2020

SUMÁRIO

1. INTRODUÇÃO

Esta Orientação Prática tem por objetivo auxiliar as Coordenações-Gerais de Auditoria da Secretaria Federal de Controle Interno (SFC) e as Controladorias Regionais da União nos Estados a realizarem o Planejamento Anual da Atividade de Auditoria Interna Governamental.

De acordo com o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, aprovado pela Instrução Normativa (IN) SFC/CGU nº 3/2017, "a atividade de auditoria interna governamental tem como propósito aumentar e proteger o valor organizacional das instituições públicas, fornecendo avaliação, assessoria e aconselhamento baseados em risco".

Detalhando a referida diretriz normativa, o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal (MOT), aprovado pela IN SFC/CGU nº 8/2017, estabeleceu que o Plano de Auditoria deve ser baseado em riscos, direcionando os esforços da UAIG às questões que estejam com maior exposição a ameaças passíveis de afetar o alcance dos objetivos da organização auditada. Além disso, deve estar em harmonia com o plano estratégico da Unidade Auditada, com as expectativas de sua alta administração e com o seu processo de gestão de riscos, quando houver e for considerado confiável.

Nesse contexto, a presente Orientação Prática apresenta conceitos, procedimentos e práticas que, em conjunto, contribuem para que a Atividade de Auditoria Interna desenvolvida pela CGU possa, efetivamente, agregar valor à gestão, fomentando a melhoria dos processos de governança, de gerenciamento de riscos e de controles internos, mediante abordagem sistemática e disciplinada, baseada em risco[1].

[1] Segundo a norma ISO 31000:2018, "risco é o efeito da incerteza nos objetivos".

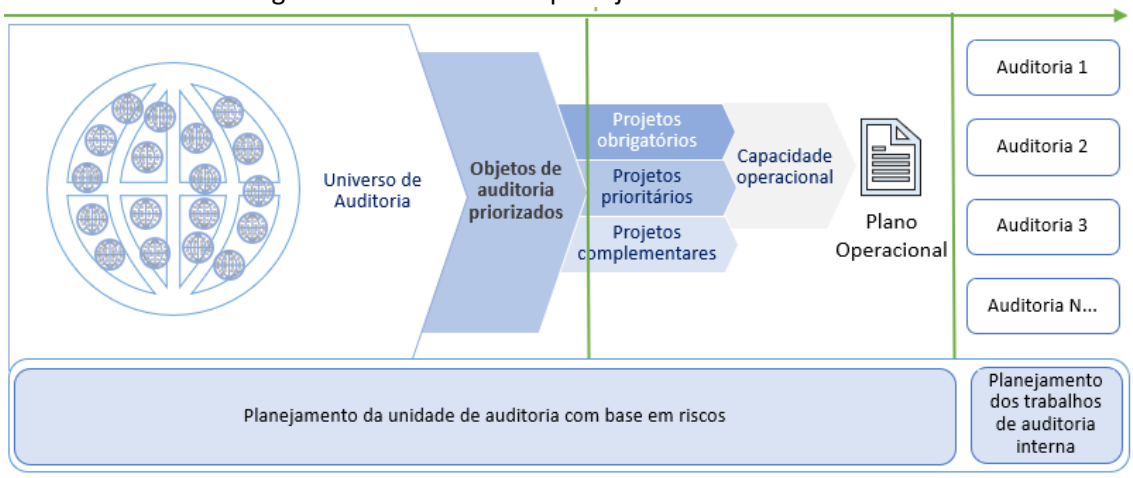
2. VISÃO GERAL DO PROCESSO

De acordo com o MOT, a expressão "Planejamento de Auditoria Baseado em Riscos" compreende, em termos gerais, as etapas de elaboração do Plano Anual de Auditoria Interna, denominado Plano Operacional (PO), na CGU, e de planejamento dos trabalhos individuais de auditoria, ambos com base em riscos.

Nesta Orientação Prática, serão abordados apenas os procedimentos relativos à fase de planejamento anual da atividade de auditoria interna, uma vez que as orientações relativas ao planejamento dos trabalhos individuais serão tratadas em Orientação Prática específica.

Em termos temporais, o processo de planejamento anual da atividade de auditoria interna é segregado em dois momentos distintos: no primeiro, são identificados, estudados e priorizados os objetos que compõem o Universo de Auditoria e, no segundo, estabelecem-se quais serão os objetos de auditoria que comporão o Plano Operacional da UAIG para cada exercício, mediante a consideração de outros fatores, como projetos de execução obrigatória, oportunidade de atuação e questões relativas à capacidade operacional.

Figura 1 – Momentos do planejamento anual da UAIG



Fonte: SFC/CGU

Relativamente ao processo de mapeamento e priorização dos objetos do Universo de Auditoria da UAIG, o MOT preconiza sua realização com base nas seguintes etapas:

Figura 2 – Processo de Planejamento da Unidade de Auditoria Interna Governamental

Fonte: SFC/CGU

A primeira etapa consiste no Entendimento da Unidade Auditada. No entanto, como a atuação da CGU compreende diferentes órgãos e entidades governamentais, bem como as diversas áreas de atuação do Governo Federal, para os fins desta Orientação Prática, a primeira etapa do processo de planejamento da UAIG será denominada "**Entendimento do Contexto**", de forma a contemplar tanto as instituições públicas (unidades) quanto as áreas de atuação do Governo Federal. O objetivo dessa etapa é produzir conhecimento e fornecer informações suficientes para possibilitar o desenvolvimento das etapas subsequentes.

Na segunda etapa, denominada "**Definição do Universo de Auditoria**", a equipe definirá o conceito a ser aplicado para definição dos objetos de auditoria e, então, realizará a identificação dos objetos constantes do Universo em estudo.

A etapa seguinte consiste na **Avaliação da Maturidade da Gestão de Riscos** da Unidade (ou Unidades relacionadas à área de atuação governamental em estudo). Essa avaliação deve possibilitar à UAIG a tomada de decisão sobre em que medida ela poderá, ou não, valer-se dos riscos que eventualmente já tenham sido mapeados e avaliados pela gestão.

Finalmente, a UAIG deve proceder à **Seleção dos Trabalhos de Auditoria com Base em Riscos**, utilizando, para tanto, o cadastro de riscos da Unidade Auditada, se confiável, e, se não, o mapeamento de riscos realizado pela própria UAIG ou em fatores de risco.

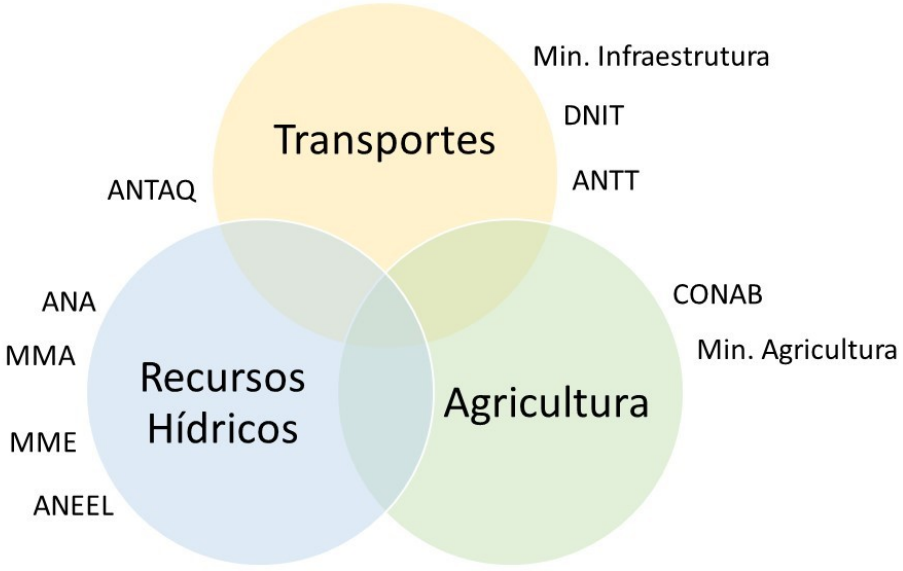
Dessa forma, o Plano Operacional deve corresponder a um portfólio de projetos de avaliação, consultoria e/ou apuração a serem realizados sobre objetos constantes do Universo de Auditoria previamente mapeado, considerados os riscos associados e demais fatores de priorização estabelecidos.

2.1. Universo de Auditoria

O MOT define Universo de Auditoria como o conjunto de objetos passíveis de serem priorizados para a elaboração do Plano de Auditoria Interna. Os objetos de auditoria podem ser processos, programas, políticas públicas, unidades de negócio, linhas de produtos ou serviços, sistemas, controles, operações, contas, divisões, funções, procedimentos etc. A definição do Universo de Auditoria deve ser lastreada em prévio entendimento sobre o contexto.

Com o Universo de Auditoria mapeado, a UAIG tem a possibilidade de definir sua estratégia de atuação, a extensão da cobertura de seus exames e as diretrizes para a rotação de ênfase[2] dos objetos de auditoria identificados.

Figura 3 – Exemplo de correlação entre unidades e áreas de atuação governamental cobertas pelo Universo de Auditoria CGU



Fonte: SFC/CGU

[2] A rotação de ênfase constitui um rodízio do foco da auditoria entre os objetos que compõem o Universo de Auditoria em determinado período, de modo a evitar, por um lado, a realização de diversos trabalhos de auditoria sobre um mesmo objeto; por outro lado, a inexistência de trabalhos sobre outros objetos associados a um menor risco (MOT, pág. 59).

No contexto da atuação da CGU, o Universo de Auditoria compreende o conjunto de Universos de Auditoria das diferentes áreas de atuação do Governo Federal, bem como dos Órgãos e Entidades do Poder Executivo Federal. Todavia, esses diferentes Universos de Auditoria coexistem de forma interrelacionada e interdependente, formando uma rede, a qual pode ser analisada sob diferentes perspectivas, conforme ilustrado.

2.2. Papéis e responsabilidades

Para que o processo de mapeamento e de atualização das informações relativas ao Universo de Auditoria da CGU seja estabelecido e opere de forma adequada, foram definidos papéis e responsabilidades, conforme disposto a seguir.

Compete aos diretores da SFC a responsabilidade pelo mapeamento do Universo de Auditoria da CGU. A definição das áreas de atuação do governo sob responsabilidade de cada diretor é estabelecida pelo colegiado de diretores da SFC. A definição das unidades seguirá a mesma estabelecida para o monitoramento de recomendações.

Cabe aos diretores, em suas respectivas áreas de atuação:

- definir a prioridade dos esforços de mapeamento;
- autorizar a realização dos projetos de mapeamento; e
- designar o gerente, o supervisor e a equipe de execução dos projetos de mapeamento.

Gerente

É o papel com a responsabilidade de conduzir os trabalhos de mapeamento de Universo de Auditoria e de dar a aprovação final sobre os conteúdos dos estudos realizadas pela equipe. Com a sua aprovação o estudo será incorporado ao Universo de Auditoria da CGU.

Supervisor

É responsável pelo acompanhamento e revisão geral dos trabalhos de mapeamento, zelando pela qualidade, tempestividade e adequação dos resultados em face dos objetivos estabelecidos.

Equipe

Cabe à equipe a responsabilidade por realizar os levantamentos de informações e as análises descritas nesta Orientação Prática.

A adequada definição da equipe é fundamental para o sucesso do processo. Para tanto, é necessário que a equipe reúna, coletivamente, conhecimento especializado sobre a Unidade ou a área de atuação governamental em estudo e, também, competências técnicas e interpessoais apropriadas, com destaque para habilidades de facilitação e de comunicação.

Assim como na execução dos demais serviços de auditoria interna, é imperativo que, durante todo o trabalho, a equipe mantenha postura ética e profissional adequada, exercendo seu julgamento com o devido zelo e ceticismo profissional.

Nos casos em que a área de atuação governamental ou a Unidade a ser mapeada guarde relação com mais de uma UAIG, é recomendável que essas unidades sejam devidamente envolvidas nos esforços de mapeamento.

3. PROCESSO DE PLANEJAMENTO DA UNIDADE DE AUDITORIA INTERNA GOVERNAMENTAL COM BASE EM RISCO

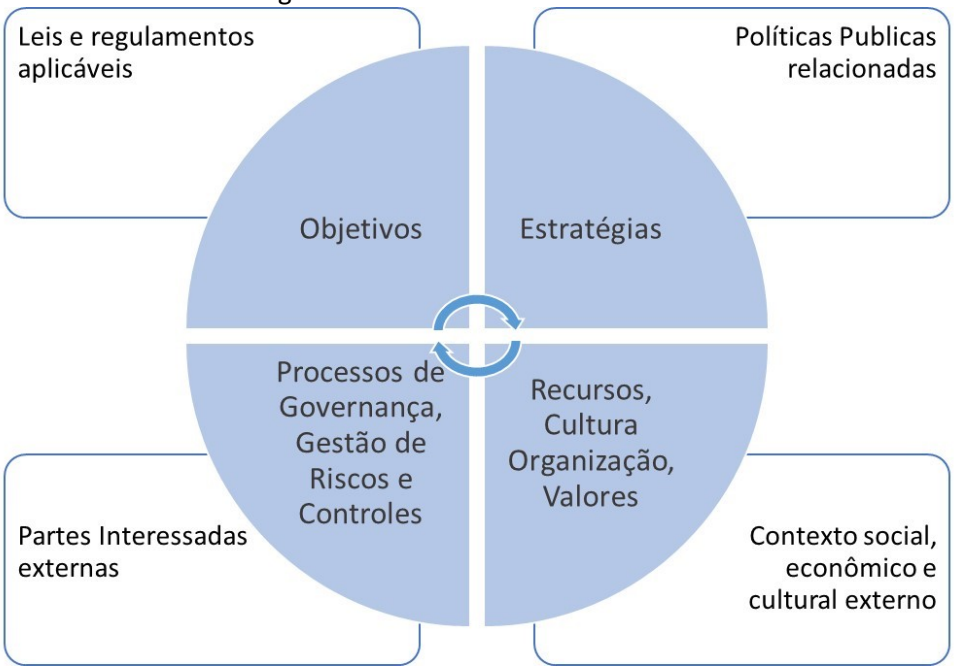
De forma a garantir que a UAIG agregue valor à gestão, concentrando seus trabalhos nas áreas e atividades cujo alcance dos objetivos pode ser mais fortemente impactado por eventos internos ou externos, ou seja, nas áreas de maior risco, são detalhadas a seguir as etapas a serem percorridas.

Destaca-se a necessidade de adequada documentação dos resultados alcançados em cada etapa, bem como sua tempestiva validação junto à gestão, de forma a garantir que o resultado final possa efetivamente corresponder à realidade da Unidade ou da área mapeada.

3.1. Entendimento do contexto

A finalidade dessa etapa é estabelecer o entendimento geral sobre o contexto interno (objetivos, estratégias, processos de governança, gerenciamento de riscos e controles internos, normativos, recursos – humanos, financeiros, tecnológicos etc.) e externo (leis e regulamentos aplicáveis, políticas públicas relacionadas, partes interessadas, ambiente de atuação, indicadores de desempenho etc.), relativos à Unidade ou à área a ser mapeada.

Figura 4 - Entendimento do contexto



Fonte: SFC/CGU

O devido conhecimento do contexto permite a identificação das áreas de maior relevância e dos principais riscos, os quais direcionarão as auditorias que, de fato, agreguem valor e contribuam para o aperfeiçoamento da gestão.

Para tanto, é necessário que a equipe mantenha um ambiente de forte interação e cooperação com as áreas de gestão e partes interessadas envolvidas, de forma a obter as informações necessárias para formar adequadamente seu entendimento. O uso de ferramentas de pesquisa e técnicas de levantamento de informações são particularmente úteis, a exemplo de pesquisas *on-line*, indagação escrita, entrevistas (gestores, servidores, clientes, usuários, beneficiários etc.) e *brainstorming*.

As principais fontes de informação que podem ser consideradas nesse processo[3], são:

- a alta administração, os gestores dos processos, profissionais com grande conhecimento sobre a Unidade ou área de atuação do Governo e as demais partes interessadas, com quem é possível coletar diversas informações, principalmente suas expectativas em relação à atividade de auditoria interna;
- áreas responsáveis pelo recebimento de denúncias relacionadas à Unidade ou outras instâncias públicas que detenham essa competência, a fim de subsidiar a elaboração do planejamento;
- documentos sobre planejamento organizacional (missão, visão, objetivos, valores, metas, indicadores etc.);
- estrutura organizacional e de governança, e as competências da unidade auditada e suas subunidades;
- sistemas de gestão empregados;
- marco legal e regulatório (leis, decretos, regimento interno, regulamentações externas incidentes sobre a Unidade Auditada e suas atividades, bem como políticas, procedimentos e manuais internos relevantes etc.);
- resultados de trabalhos de auditoria anteriores.

Com base no conhecimento estabelecido, a equipe deverá documentar as seguintes informações:

- **Qual é o objetivo da atuação governamental sobre a área estudada ou qual é o motivo de existência da instituição estudada?**

  Identificar o propósito da existência da instituição ou o papel do Governo Federal na área de atuação que está sendo estudada. Nesse momento, devem ser identificados a missão e os objetivos-chave, a visão de futuro, os valores fundamentais da organização ou do Governo Federal na área de atuação em análise.
- **Como acontece?**

[3] Lista adaptada do MOT, página 51.

Descrever o processo de funcionamento da organização ou da área de atuação do governo, incluindo, no que couber, informações sobre organograma, atores envolvidos, objetivos estratégicos e os macroprocessos[4] finalísticos e de apoio existentes, entre outras.

- **O que faz?**

  Detalhar o resultado entregue pela organização para cumprimento de seu propósito ou pelo Governo Federal na área de atuação em estudo, bem como as medidas de desempenho aplicáveis (metas, indicadores de desempenho e variações aceitáveis no desempenho) e o histórico dos resultados alcançados.

O Anexo I fornece um modelo de documento para apoiar o registro das informações e entendimentos firmados pela equipe sobre o contexto do Universo estudado.

3.2. Definição do Universo de Auditoria

Nessa etapa, a partir do entendimento geral formado sobre a Unidade ou área de atuação do governo será estabelecido o conceito de objeto de auditoria que será adotado e sua posterior aplicação.

Por definição, os processos[5] de negócio representam a atuação cotidiana das instituições e guardam estreita relação com as competências da Unidade ou do Governo Federal na área em estudo, possuindo certa perenidade organizacional, estando diretamente relacionados com os riscos e com os controles implementados pela organização (o que os torna passíveis de receberem trabalhos de auditoria), sendo, inclusive, mais detalhados do que os macroprocessos finalísticos. Dessa forma, as UAIG devem considerar os processos de negócio (ou grupo de processos correlatos) como o

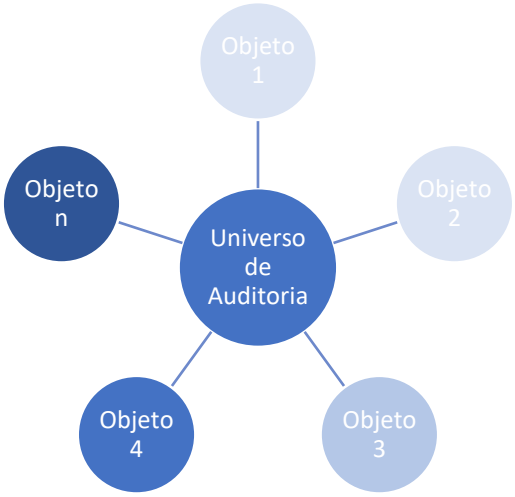
[4] É o meio pelo qual a organização reúne grandes conjuntos de atividades para gerar valor e cumprir sua missão institucional, de forma alinhada aos seus objetivos. Por exemplo, na CGU, guardam maior proximidade com a atuação da SFC os macroprocessos de "Gestão do Controle Interno Governamental" "Gestão do combate à corrupção". O primeiro macroprocesso citado é composto por 9 processos, a exemplo de "Gerenciar auditorias governamentais", "Desenvolver atividades de controladoria" e "Supervisionar órgãos de auditoria interna".

[5] Entende-se por processo um conjunto de atividades sequenciadas e relacionadas entre si que têm como finalidade transformar insumos em produtos e serviços, conforme o MOT, pág. 66

padrão preferencial de conceito para a definição dos objetos de auditoria no contexto do Universo em estudo.

Dessa forma, o Universo de Auditoria será constituído pelo conjunto de objetos mapeados pela equipe, sobre os quais a UAIG atuará, por meio de serviços de avaliação, consultoria e/ou apuração, de forma a apoiar o atingimento de seus objetivos, agregar valor, e promover a melhoria dos processos de governança, de gestão de riscos e de controles internos.

Figura 5 – Exemplo de ilustração da composição do Universo de Auditoria



Fonte: SFC/CGU

É necessário que o resultado da definição do Universo de Auditoria seja devidamente documentado, registrando, além da relação dos objetos de auditoria mapeados, uma visão geral sobre cada um dos objetos definidos, incluindo considerações sobre seus objetivos, atividades relacionadas, aspectos organizacionais, marco regulatório, e os arranjos orçamentários, financeiros, de pessoal e de tecnologia da informação existentes, entre outros.

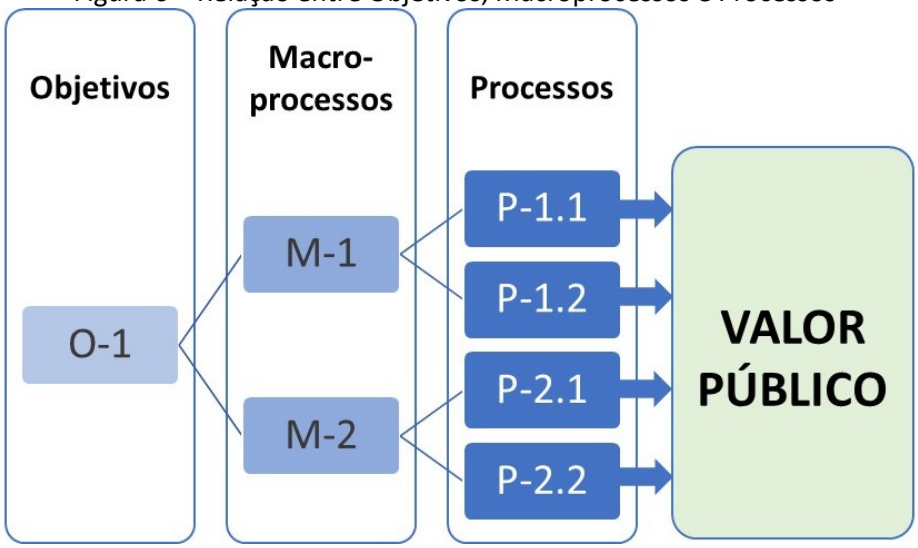
Aspectos relacionados a riscos ou criticidades identificados devem também ser documentados, de maneira a fornecer informações que podem ser consideradas no contexto dos trabalhos individuais de auditoria a serem realizados, além de outros insumos importantes para a posterior priorização dos objetos de auditoria.

A relação completa dos objetos de auditoria identificados no Universo de Auditoria em estudo deve ser devidamente registrada no sistema de gestão da atividade de auditoria. O objeto identificado deve ser cadastrado mesmo que não seja objeto de estudo mais aprofundado no momento do mapeamento do Universo.

O Anexo II apresenta modelo de documento para apoiar o registro das informações e entendimentos da equipe sobre cada um dos objetos de auditoria mapeados.

Seguindo a abordagem sugerida de conceituação dos objetos nos processos, deve-se, a partir do conhecimento dos objetivos (chave e estratégicos), identificar os macroprocessos existentes e, para cada um deles, o conjunto de processos finalísticos e de apoio (os objetos de auditoria), responsáveis pela entrega de valor pela Unidade ou área de atuação governamental em estudo, conforme ilustrado.

Figura 6 – Relação entre Objetivos, Macroprocessos e Processos

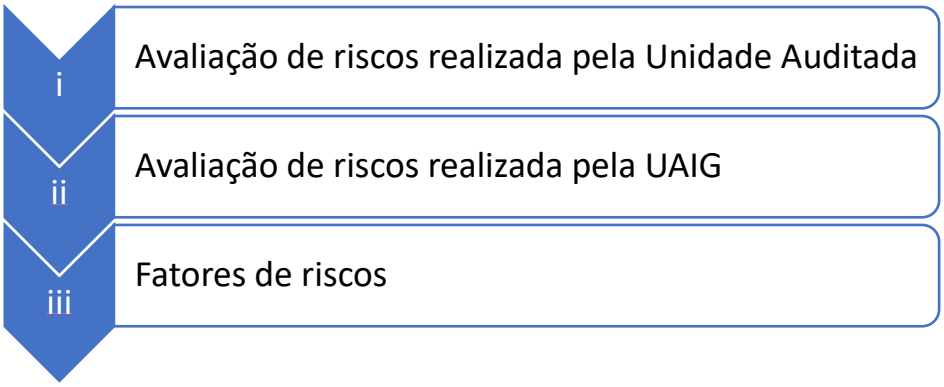


Fonte: SFC/CGU

3.3. Avaliação da maturidade da gestão de riscos

Segundo a IN SFC/CGU nº 3/2017, existem diferentes bases que podem ser utilizadas para a elaboração do Plano de Auditoria com base em riscos. A seleção da base a ser utilizada deve considerar as condições do contexto e as competências técnicas disponíveis na UAIG.

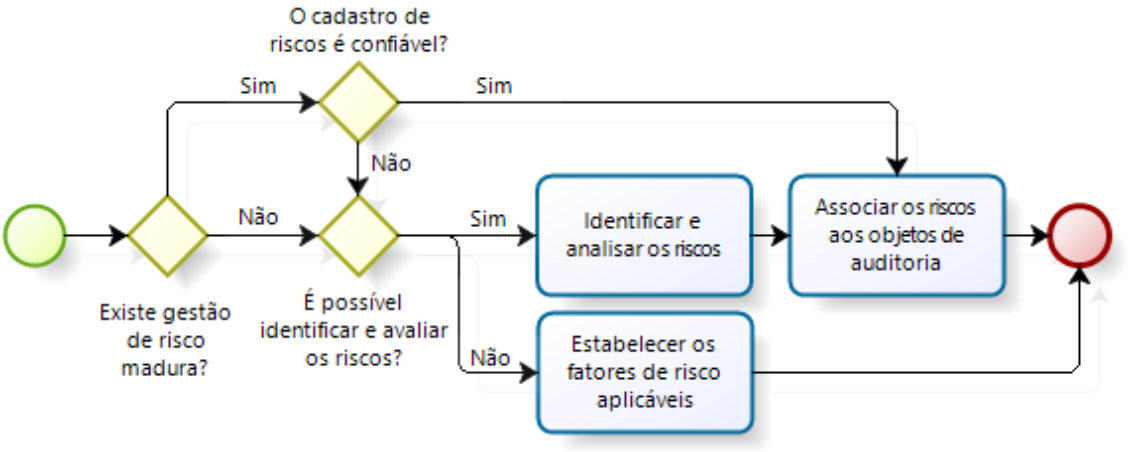
Figura 7 – Bases para seleção dos trabalhos de auditoria



Fonte: MOT

No âmbito da CGU, a elaboração do Plano Operacional deve seguir, de forma prioritária, a ordem acima exposta. Assim, os trabalhos serão priorizados com base em fatores de riscos (por exemplo: materialidade, relevância e criticidade) apenas se a avaliação de riscos da própria Unidade Auditada não existe ou não é confiável, e, não é possível ou aplicável a realização de uma avaliação de riscos pela própria UAIG.

Figura 8 – Fluxo de decisões relacionadas com a maturidade da gestão em gestão de riscos



Fonte: SFC/CGU

Dessa forma, o primeiro passo para essa definição é a avaliação da maturidade da gestão de riscos do contexto em estudo. Nos casos em que for considerada madura, deverá servir de referência para a priorização dos objetos de auditoria. Não havendo gestão de riscos madura, é necessário que a própria equipe identifique e analise os riscos do contexto para a posterior priorização de objetos de auditoria.

Para apoiar a avaliação de maturidade da gestão de riscos, é recomendada a utilização da planilha modelo, constante no Anexo III desta Orientação Prática, onde são dispostos

os quesitos para avaliação. Constatado o nível de maturidade “Aprimorado” ou “Avançado”, os riscos mapeados pela gestão devem ser apropriados pela UAIG como variáveis de classificação dos objetos de auditoria definidos.

No caso de não haver maturidade suficiente ou de inexistir gestão de riscos no contexto avaliado, a equipe deve então realizar a identificação e a avaliação os riscos, de forma a permitir a priorização e a seleção de trabalhos de auditoria sobre objetos que representam maior nível de risco inerente[6].

Ressalta-se não haver expectativa de que esse estudo inicial avance sobre a consideração dos controles implementados e a avaliação dos riscos residuais[7]. No entanto, caso disponível, esse detalhamento fortalece e traz maior assertividade ao processo de priorização que será realizado em seguida.

Por fim, nas situações em que for constatada a inadequação da maturidade da gestão de riscos do contexto e não for aplicável ou viável a identificação e avaliação dos riscos pela UAIG, poderão ser utilizados critérios de priorização, chamados de fatores de risco, para priorização e seleção dos objetos de auditoria do Universo em estudo.

Conforme preconizado pelo MOT, nessas situações, é necessária a definição prévia dos critérios de priorização a serem utilizados, adaptados ao contexto sob estudo, devidamente validados junto ao gerente do trabalho de mapeamento do Universo de Auditoria.

3.4. Seleção dos objetos de auditoria com base em riscos

Finalizada a etapa de avaliação da maturidade da gestão de riscos e definida a base a ser utilizada para priorização dos objetos, dá-se início ao processo de seleção dos objetos de auditoria com base em riscos. Esse processo observará procedimentos específicos, a depender da forma de seleção definida pela equipe.

---

[6] Risco inerente: segundo a Metodologia de Gestão de Riscos da CGU, é o risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

[7] Risco residual: segundo a Metodologia de Gestão de Riscos da CGU, é risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

Seleção com base na avaliação de riscos realizada pela Unidade Auditada

Como essa forma de priorização se baseia no cadastro de riscos da Unidade Auditada, é possível que não haja uma correspondência direta entre os riscos identificados pela gestão e o Universo de Auditoria mapeado pela equipe.

Nesses casos, será necessário primeiramente realizar a associação entre os objetos de auditoria mapeados e os objetos da gestão de riscos (macroprocessos, processos, unidades de negócio etc.) e, somente então, vincular os riscos (ou conjunto de riscos) aos objetos do Universo de Auditoria.

Na sequência, a UAIG deve classificar os objetos de auditoria com base nos riscos associados a cada um deles.

Seleção com base na avaliação de riscos realizada pela UAIG

Para a classificação dos objetos de auditoria, no caso de não haver maturidade suficiente ou em face da inexistência de gestão de riscos na Unidade ou área em estudo, é necessário que a própria UAIG realize a identificação e a avaliação dos principais riscos do negócio.

De forma a equilibrar os aspectos de efetividade, qualidade e viabilidade operacional, foi definido o seguinte modelo padrão[8], a ser aplicado no âmbito da CGU, para priorização dos objetos de auditoria do Universo em estudo com base em riscos:

i) identificação e avaliação dos riscos-chave[9] relacionados aos objetos de auditoria identificados;
ii) associação dos riscos dos macroprocessos aos processos (objetos de auditora);
iii) priorização dos objetos de auditoria com base em riscos.

[8] O procedimento padrão foi adaptado do modelo proposto por Santos (2019), considerando que o conceito de objeto de auditoria estabelecido foi por processo. Caso seja estabelecido entendimento diverso, o procedimento deve ser adaptado.
[9] Os riscos-chave são os principais riscos aos quais uma organização está exposta ou o Governo Federal está exposto em sua atuação na área em estudo.

Como visto anteriormente, nas etapas de entendimento do contexto e de definição do Universo de Auditoria, são identificadas, entre outras informações, os objetivos da Unidade/área em estudo, os macroprocessos e seus respectivos processos (finalísticos e de apoio). Por questões de viabilidade operacional, o modelo preconiza a identificação e avaliação dos riscos apenas no nível dos macroprocessos, com posterior associação aos processos relacionados.

Dessa forma, o primeiro passo consiste na identificação e avaliação dos riscos-chave relacionados aos objetos de auditoria definidos. Para tanto, é recomendado o uso de técnicas como Matriz SWOT, *Brainstorming*, Diagrama *Bow-Tie*, entre outras. A norma ABNT ISO 31010:2009 apresenta e explica o uso dessas e de outras técnicas no contexto dos trabalhos de Gestão de Riscos.

Por exemplo, com a aplicação da Matriz SWOT em cada macroprocesso mapeado, é possível identificar forças e fraquezas do ambiente interno e oportunidades e ameaças do ambiente externo ao contexto em avaliação. Com base nas fraquezas e nas ameaças levantadas, podem ser identificados riscos por meio de resposta à questão: "*Quais riscos podem decorrer das fraquezas e das ameaças relacionadas ao macroprocesso?"*.

A partir de então, cada risco identificado deve ser avaliado em relação ao seu potencial impacto (I) e à sua probabilidade (P) de ocorrência, conforme quadro ilustrativo a seguir:

Quadro 1 – Exemplo de identificação e avaliação de riscos dos macroprocessos

Macroprocessos	**Riscos-Chave**	**Nível de Risco[10] (I x P)**
M1. Macroprocesso 1	R1. Risco 1 R2. Risco 2 R3. Risco 3	NR1. 10 x 6 = 60 NR2. 6 x 6 = 36 NR3. 6 x 8 = 48
M2. Macroprocesso 2	R1. Risco 1 R4. Risco 4 R5. Risco 5	NR1. 10 x 6 = 60 NR4. 8 x 8 = 64 NR5. 8 x 6 = 48
M3. Macroprocesso 3	R4. Risco 4 R6. Risco 6 R7. Risco 7 R8. Risco 8	NR4. 8 x 8 = 64 NR6. 10 x 4 = 40 NR7. 6 x 6 = 36 NR8. 8 x 6 = 48

[10] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação de suas consequências e sua probabilidade (ABNT ISO GUIA 73:2009)

Fonte: Adaptado de Santos (2019)

O Anexo IV apresenta planilha de apoio ao processo de identificação e análise dos riscos.

O segundo passo consiste na associação dos riscos identificados e avaliados nos macroprocessos a cada um dos seus processos relacionados, que representam os objetos de auditoria mapeados. Essa associação pode ser feita a partir da resposta à seguinte questão, a ser aplicada a cada um dos processos: "*Que riscos relacionados aos objetivos do macroprocesso estão presentes no processo em análise?"* Concluída a associação dos riscos dos macroprocessos a cada um dos processos, é calculada a magnitude dos riscos dos processos, por meio do somatório do nível de risco de cada um dos riscos associados. O quadro a seguir ilustra esse passo:

Quadro 2 – Exemplo de associação dos riscos dos macroprocessos aos processos

Macroprocessos	Processos	Riscos Associados	Σ Nível dos Riscos Associados
M1. Macroprocesso 1	P1. Processo 1.1	R1; R2	60 + 36 = **96**
	P2. Processo 1.2	R1; R2; R3	60 + 36 + 48 = **144**
	P3. Processo 1.3	R1; R3	60 + 48 = **108**
	Magnitude do Macroprocesso 1		**348 (24,7%)**
M2. Macroprocesso 2	P4. Processo 2.1	R4; R5	64 + 48 = **112**
	P5. Processo 2.2	R1; R4; R5	60 + 64 + 48 = **172**
	P6. Processo 2.3	R4	**64**
	P7. Processo 2.4	R1; R4	60 + 64 = **124**
	P8. Processo 2.5	R1; R4; R5	60 + 64 + 48 = **172**
	Magnitude do Macroprocesso 2		**644 (45,7%)**
M3. Macroprocesso 3	P9. Processo 3.1	R4; R6	64 + 40 = **104**
	P10. Processo 3.2	R7; R8	36 + 48 = **84**
	P11. Processo 3.3	R4; R6; R7; R8	64 + 40 + 36 + 48 = **188**
	P12. Processo 3.4	R4; R6; R7	64 + 40 + 36 = **140**
	Magnitude do Macroprocesso 3		**416 (29,6%)**

Fonte: Adaptado de Santos (2019)

Por fim, no terceiro passo, a partir da aferição do valor de magnitude dos riscos associados a cada processo, é possível definir a ordem de prioridade dos processos com base em riscos, de forma a subsidiar a elaboração do Plano Operacional.

Quadro 3 – Exemplo de priorização de objetos de auditoria com base em riscos

Prioridade	Processos	Riscos Associados	Σ Nível dos Riscos Associados
1	P11. Processo 3.3	R4; R6; R7; R8	188
2	P5. Processo 2.2	R1; R4; R5	172
3	P8. Processo 2.5	R1; R4; R5	172
4	P2. Processo 1.2	R1; R2; R3	144
5	P12. Processo 3.4	R4; R6; R7	140
6	P7. Processo 2.4	R1; R4	124
7	P4. Processo 2.1	R4; R5	112
8	P3. Processo 1.3	R1; R3	108
9	P9. Processo 3.1	R4; R6	104
10	P1. Processo 1.1	R1; R2	96
11	P10. Processo 3.2	R7; R8	84
12	P6. Processo 2.3	R4	64

Fonte: Adaptado de Santos (2019)

Seleção com base em fatores de riscos

No caso de opção pela priorização dos objetos de auditoria com base em fatores de riscos, devem ser definidos os fatores de priorização dos objetos considerando a adequação à realidade da Unidade Auditada e a disponibilidade de dados para aferição dos fatores, sempre com foco nos processos de governança, de gerenciamento de riscos e de controles internos da Unidade Auditada, bem como a possibilidade de ocorrência de erros, fraudes ou não conformidades significativas.[11]

Após a definição e aprovação dos fatores (e eventuais pesos atribuídos) a serem utilizados, a equipe deverá proceder à avaliação de cada um dos objetos com base nos critérios determinados e, a partir de então, promover a hierarquização dos objetos.

Conforme destacado pelo MOT, deve-se evitar a utilização de fatores que não possam ser associados a todos os objetos de auditoria (a exemplo da materialidade, quando nem todos os objetos possuírem um valor monetário). Caso isso não seja possível, a UAIG

[11] Para acessar mais detalhes e exemplos sobre a definição de fatores de riscos quantitativos e qualitativos, acesse o MOT nas páginas 56 e 57.

deve cercar-se de cuidados metodológicos de normalização cabíveis, que permitam a comparabilidade com base nas premissas estabelecidas.

Elaboração do Plano Operacional

Finalmente, no momento de elaboração do PO, além da priorização estabelecida no *ranking* acima, a Unidade de Auditoria deverá considerar, por exemplo:

- a oportunidade de realização de cada trabalho, considerando o contexto político/institucional;
- a expectativa agregação de valor e de geração de benefícios financeiros e não financeiros;
- trabalhos que devem ser realizados em função de obrigação normativa, por solicitação da Alta Administração ou por outros motivos (decisões judiciais, demandas externas etc.);
- trabalhos de auditoria realizados anteriormente sobre o objeto (criticidades e rodízio de ênfase);
- a disponibilidade dos recursos necessários à realização dos trabalhos;
- a capacidade operacional e técnica da UAIG para realizar os trabalhos.

Nesse sentido, o Plano Operacional da UAIG será estabelecido com a inclusão dos objetos de auditoria mais relevantes e oportunos, que possam efetivamente agregar valor à gestão pública.

Importante destacar que, além da relação de trabalhos de auditoria a serem executados no período, devem ser consideradas outras atividades a serem cobertas pelo PO, conforme requisitos constantes em normativos específicos, a exemplo de:

- previsão de, no mínimo, 40 horas de capacitação para cada auditor interno governamental, incluindo o responsável pela UAIG;
- monitoramento das recomendações emitidas em trabalhos anteriores e ainda não implementadas e em acompanhamento pela UAIG a que se refere o PO;
- atividades de gestão e melhoria da qualidade da atividade de auditoria interna governamental.

4. DISPOSIÇÕES GERAIS

4.1. Validação dos resultados com a gestão

Como forma de assegurar a adequação dos entendimentos e das conclusões dos auditores acerca do Universo de Auditoria, é necessário que tais resultados sejam devidamente validados junto aos responsáveis pela gestão da Unidade ou tema em estudo.

Portanto, é essencial que os trabalhos sejam desenvolvidos com base em um ambiente de colaboração e de interlocução permanente entre as partes, considerando os objetivos mútuos envolvidos e o potencial de agregação de valor à gestão.

4.2. Compartilhamento de informações com a gestão

De acordo com o Instituto dos Auditores Internos, a estrutura de gestão é a

> "responsável pelo estabelecimento e operação da estrutura de gerenciamento de riscos (...). O papel fundamental do auditor interno em relação ao GRC deveria ser o de prover avaliação (*assurance*) à administração e ao conselho quanto à eficácia do gerenciamento de riscos. Quando a auditoria interna estende suas atividades além deste papel fundamental, deveria aplicar determinadas salvaguardas (...). Desta forma, a auditoria interna irá proteger a sua independência e objetividade dos seus serviços de avaliação (*assurance*). Dentro destas restrições, o GRC (gerenciamento de riscos corporativos) pode auxiliar a ampliar o perfil e aumentar a eficácia da auditoria interna" (IIA, 2009).

Como se pode ver, o processo de gerenciamento de riscos é de responsabilidade da gestão e, portanto, não deve ser realizada pela Atividade de Auditoria Interna. Entretanto, em se tratando de unidades com baixo nível de maturidade em gestão de riscos, é esperado que os levantamentos realizados pela auditoria tenham grande valor como fator impulsionador dessa importante atividade de gestão.

Nesse contexto, é oportuno que o processo de identificação e avaliação dos riscos (para fins de seleção dos objetos do Universo de Auditoria) seja elaborada pelo próprio Gestor, com apoio e facilitação realizada pela UAIG, o que permitirá, simultaneamente,

a utilização dos resultados pela equipe de mapeamento e o fortalecimento da capacidade da Gestão para gerir seus próprios riscos.

Caso isso não seja possível, visando o apoio à elevação da maturidade em gestão de riscos da Unidade auditada, a UAIG pode compartilhar os resultados alcançados, desde que adote as devidas salvaguardas. De acordo com o IIA (2009), algumas importantes salvaguardas são:

- deixar claro que a Administração permanece como a responsável pelo gerenciamento de riscos;
- a auditoria interna não deve gerenciar nenhum dos riscos em nome da Administração;
- a auditoria interna deve dar suporte ao processo de tomada de decisão da Administração, sendo responsabilidade da gestão a tomada de decisões sobre o gerenciamento de riscos.

4.3. Periodicidade de reavaliação

Esforços de atualização das informações do Universo de Auditoria devem ser realizados, pelo menos, a cada quatro (4) anos.

Todavia, os estudos de entendimento de contextos e de seus riscos devem ser atualizados sempre que ocorrerem mudanças significativas no ambiente que possam comprometer a adequação dos resultados e sua utilidade para fins de definição do Plano Anual de Auditoria Interna.

Mudanças como, por exemplo, modificações no direcionamento estratégico, alterações na política pública, alterações de estrutura organizacional das Unidades envolvidas, novas demandas da sociedade, crises econômicas, entre outras, podem ser indicativos da necessidade de início de um projeto de atualização do Universo de Auditoria.

Importa ressaltar que, após o mapeamento inicial, atualizações tendem a consumir menores esforços e recursos.

4.4. Mapeamento de Universo de Auditoria em Unidades da Administração Indireta

Pelo fato de as instituições públicas federais da administração indireta contarem com unidades próprias de auditoria interna, os esforços de mapeamento de Universo de Auditoria da CGU devem ser concentrados, primeiramente, em instituições da administração direta e nas áreas de atuação do governo.

Mapeamentos de Universo de Auditoria realizados em instituições da administração indireta devem considerar os conhecimentos gerados pela unidade de auditoria interna atuante na organização. Portanto, caso já exista Universo de Auditoria ou estudos sobre os riscos institucionais e essas informações sejam consideradas maduras e de boa qualidade pela equipe da CGU, devem ser adotados e incorporados ao Universo de Auditoria da CGU.

5. REFERÊNCIAS

ABNT. **ISO GUIA 73:2009 – Gestão de Riscos – Vocabulario**. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Rio de Janeiro. 2009.

ABNT. **ISO 31010: Gestão de riscos: Técnicas para o processo de avaliação de risco**. ISO/IEC. [S.l.]. 2012.

CGU. **Instrução Normativa SFC/CGU nº 3, de 09 de junho de 2017**. Controladoria-Geral da União. Brasília. 2017. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal.

CGU. **Instrução Normativa SFC/CGU nº 8, de 6 de dezembro de 2017**. Controladoria-Geral da União. Brasília. 2017. Aprova o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal.

CGU. **Metodologia de Gestão de Riscos da CGU**. Controladoria-Geral da União. [S.l.]. 2018.

IIA. **Declaração de Posicionamento do IIA: Declaração de Posicionamento IIA: O Papel da Auditoria Interna no Gerenciamento de Riscos Corporativo**. The Institute of Internal Auditors - IIA. [S.l.]. 2009.

SANTOS, P. R. M. R. D. **Planejamento de auditoria baseado em riscos: Proposta de aplicação da metodologia de planejamento de auditoria baseada em riscos na seleção de objetos de auditoria relacionados à mobilidade urbana**. Instituto Serzedelo Corrêa. Brasília. 2019. Trabalho de Conclusão de Curso apresentado ao Instituto Serzedello Corrêa como requisito parcial para a obtenção do grau de especialista em Auditoria do Setor Público.