VIGÊNCIA
INÍCIO: 12/04/2022 FIM:

TÍTULO
MANUAL DE PROCEDIMENTOS DA AUDITORIA INTERNA DO SERPRO

REFERÊNCIAS

TEMA: AU – Auditoria Interna

PALAVRAS-CHAVE: auditoria, procedimentos, diretrizes, controle interno, fiscalização, CGU, IIA, IPPF

PROCESSO
12.04 - Gerenciar Auditoria Interna

CÓDIGO DE CLASSIFICAÇÃO
010.01

CLASSIFICAÇÃO DA INFORMAÇÃO
Ostensivo

1.0 FINALIDADE

Instituir o Manual de Procedimentos da Auditoria Interna do Serviço Federal de Processamento de Dados – Serpro, que detalha procedimentos afetos ao processo Gerenciar Auditoria Interna e seus subprocessos, de forma a padronizar seus métodos de trabalho, sistemas e modelos, observando os elementos obrigatórios da Estrutura Internacional de Práticas Profissionais (IPPF), que incluem a Definição de Auditoria Interna, o Código de Ética, os Princípios Fundamentais e as Normas Internacionais para a Prática Profissional de Auditoria Interna definidos pelo *The Institute of Internal Auditors* (The IIA), assim como a orientação e regulamentação estabelecida pela Controladoria-Geral da União – CGU, no exercício da supervisão técnica.

2.0 ÂMBITO DE APLICAÇÃO

Auditoria Interna.

3.0 DETERMINAÇÃO

A Auditoria Interna, no âmbito de suas atribuições estabelecidas no Estatuto Social do Serpro, e observando os elementos obrigatórios da IPPF citados, assim como a conformidade com as diretrizes e normas técnicas que regem as ações de controle do Sistema de Controle Interno do Poder Executivo Federal, estabelece o Manual de Procedimentos da Auditoria Interna com o intuito de sistematizar e padronizar conceitos, técnicas e práticas a serem observadas e seguidas pelos empregados da Auditoria Interna do Serpro.

4.0 DISPOSIÇÕES FINAIS

4.1 A versão mais atual do Manual de Procedimentos será publicada na página da Auditoria Interna na Intranet, acompanhada das versões anteriores para consulta, mantido controle de versionamento.

4.2 Com base nos resultados do Programa de Gestão e Melhoria da Qualidade – PGMQ e visando sustentar as práticas de qualidade, o titular da Auditoria Interna analisará ao

menos anualmente a necessidade de revisar o Manual de Procedimentos, consolidando nova versão.

4.3 Os casos omissos ou as dúvidas que porventura surjam serão tratados pelo titular da Auditoria Interna ou pelo colegiado de gerentes no âmbito do PGMQ.

12 de abril de 2022

Auditor Interno

DP/AUDIN/AUDIE/mjlmm

Manual de Procedimentos Operacionais

Auditoria Interna (Audin)

Abril/2022 - Versão 1.0

Vigência: 12 de abril de 2022

serpro.gov.br

Controle de Revisões

Versão	Data	Autor/Revisor	Alterações da Versão
1.0	12/04/2022	Carlos Moraes de Jesus	Versão 1.0

EQUIPE TÉCNICA

Auditor Interno

Carlos Moraes de Jesus

Departamento de Departamento de Assessoramento a Auditoria Interna e Externa (AUDIE)

Maria Juliane Leite Mendonça Macedo

Departamento de Auditoria Contínua (AUDCN)

Rennis Sousa de Oliveira

Departamento de Auditoria em Gestão de Aquisições, Contratos e Logística (AUDAC)

Marcos José Perini

Departamento de Auditoria em Gestão Contábil e Financeira (AUDCF)

Renata Nunes Lazzarini

Departamento de Auditoria em Gestão Empresarial e Pessoas (AUDEP)

Nilson Romero Michiles Junior

Departamento de Auditoria na Entidade de Previdência Complementar (AUDPC)

Fabiano de Moura

Departamento de Auditoria em Tecnologia da Informação e Negócios (AUDTN)

Ângela Maria Cristina Clara

Sumário

1 Introdução

Conforme previsto no Regimento Interno da Auditoria Interna, esta Auditoria Interna (Audin) atua como órgão auxiliar ao Sistema de Controle Interno do Poder Executivo Federal (SCI) e apoia o controle externo por previsão constitucional, estando sujeita à orientação normativa e à supervisão técnica pelo órgão central do SCI, atribuição exercida pela Secretaria Federal de Controle Interno (SFC) da Controladoria-Geral da União (CGU), reconhecendo a natureza mandatória dos elementos obrigatórios da Estrutura Internacional de Práticas Profissionais (IPPF), que incluem a Definição de Auditoria Interna, os Princípios Fundamentais e as Normas Internacionais para a Prática Profissional de Auditoria Interna e o Código de Ética definidos pelo *The Institute of Internal Auditors* (The IIA).

Este Manual de Procedimentos Operacionais da Auditoria Interna detalha os procedimentos afetos ao processo Gerenciar Auditoria Interna e seus subprocessos: Realizar Auditoria Interna e Assessorar Auditoria Interna e Auditoria Externa, observando os instrumentos acima descritos.

Em relação à legislação da SFC/CGU - PR, este Manual considera o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal e a Instrução Normativa SFC que dispõe o Plano Anual (PAINT) e Relatório Anual (RAINT) das UAIG do Poder Executivo Federal, os quais podem ser acessados diretamente na página da CGU ou por meio dos links indicados na página da Audin (link).

2 Tipos de Serviços

A avaliação e a consultoria são os serviços típicos prestados pela Auditoria Interna e estão definidos tanto no Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal quanto na Estrutura Internacional de Práticas Profissionais de Auditoria Interna (IPPF).

2.1 Avaliação

A avaliação corresponde ao serviço de asseguração prestado pelo auditor interno, que emite opinião objetiva e independente sobre o objeto auditado, com base em critérios estabelecidos e no resultado dos testes de auditoria.

2.2 Consultoria

A consultoria prestada pela Auditoria Interna possui regulamentação interna no Serpro, que em resumo a define como o assessoramento prestado à alta administração por solicitação específica dos Conselhos ou da Diretoria Executiva, sendo requisito a natureza estratégica e voltada a adicionar valor aos sistemas de governança, de gestão de riscos e de controles internos. Como todo assessoramento, cabe ao gestor decidir pela adoção ou não, sem que a Auditoria Interna assuma qualquer responsabilidade que seja da Administração.

3 Etapas da avaliação - Subprocesso: Realizar Auditoria

O Plano Anual de Auditoria Interna (PAINT) contém os trabalhos individuais de auditoria que serão executados no ano. Desta forma, após a aprovação do PAINT pelo Conselho de Administração e, antes do

início do exercício correspondente à execução do Plano, a equipe do Departamento de Assessoramento a Auditoria Interna e Auditoria Externa (Audie) realizará o cadastramento do PAINT no sistema de Auditoria. Após 1º de janeiro do ano correspondente, os gerentes dos departamentos de auditoria poderão realizar a abertura dos trabalhos conforme objetivos, escopos, prazos e recursos previstos no PAINT.

3.1 Planejamento

Os trabalhos de avaliação e consultoria iniciam-se com o planejamento individual do trabalho. Nesta etapa são realizados os levantamentos preliminares (incluindo legislação e demais normativos, referenciais de boas práticas, histórico de controle, contexto de negócio) e análises do objetivo, principais riscos e controles existentes, processos envolvidos, testes de auditoria a serem executados e as técnicas que serão utilizadas.

Estas informações compõem o programa de trabalho individual e devem ser registradas no Sistema de Auditoria (Sisaudit) com base nas informações constantes do Documento de Análise Preliminar do Objeto Auditado (DAP) (link) e Matriz de Riscos (MR) - Auditoria (link).

Para todas as tarefas (testes) do Programa de Auditoria, deve ser registrado quem da equipe ficou responsável pela sua realização. Para isso, no campo 'Resultado' do teste no Sisaudit deve ser referenciado o #Atribuído para: <responsável> - #Complexidade: <nível>.

3.1.1 Procedimento: Elaborar Documento de Análise Preliminar (DAP)

Descrição: Levantamento de informações relevantes e contexto do objeto auditável, visando subsidiar o planejamento com foco no objetivo do trabalho. Nessa etapa deve ser preenchido o Documento de Análise Preliminar do Objeto Auditado (DAP) (link). Atribuir um responsável e informar a complexidade.

3.1.1.1 Revisar as abas "Dados gerais" e "Cronograma" do trabalho

Com base no Plano Anual de Atividade de Auditoria Interna - PAINT vigente (link) e informações preliminares já apuradas, revisar no Sisaudit, as informações relativas a cada trabalho, nas abas "Dados gerais" e "Cronograma". Devem ser revisados, sobretudo, os campos: Objetivo, Escopo, Conhecimentos específicos, Cronograma de início e fim previsto, equipe e respectivos papéis. Feito isso, encaminhar Planejamento Tático para aprovação pelo CAE. Toda tarefa deve ser #Atribuído para: <responsável> - #Complexidade: <nível>. Por exemplo, essa tarefa pode ser atribuída a quem ficar responsável por facilitar essa dinâmica na equipe, provavelmente o Supervisor ou o Auditor responsável.

3.1.1.2 Elaborar Planejamento Tático da Auditoria

No Sisaudit, na aba "Dados gerais" relativo ao trabalho em curso, elaborar Planejamento Tático da Auditoria, alocando a equipe de auditoria, submetendo a aprovação pelo Supervisor. O Planejamento Tático deve ser aprovado pelo Supervisor e submetido à aprovação pelo Titular da Auditoria Interna, após o que passará ao Status 'Planejamento tático aprovado'. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.3 Coletar, da equipe e do supervisor, as Declarações Individuais para Início do Trabalho

Em conformidade com as IPPFs 1120 - Objetividade individual, 1130 - Prejuízo à Independência ou à Objetividade, 1200 - Proficiência e Zelo Profissional Devido e 2230 - Alocação de recursos para o trabalho da auditoria, deve-se coletar, da equipe e do supervisor, as Declarações Individuais para Início do Trabalho, conforme modelo disponível (link). Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.4 Atribuir o nº da Auditoria e colocá-la 'Em planejamento'

Para que o Sisaudit atribua o número da Auditoria, deve ser informado pelo administrador do Sisaudit o número do Memorando de Apresentação. Por padrão, inicialmente será informado o número '0001' e a data atual. Após expedição do Memorando no próximo passo, a equipe deve atualizar os campos de número e data, conforme Siscor expedido. No Sisaudit, na aba "Dados Gerais" relativo ao trabalho em curso, nesse estágio o 'Status' da Auditoria será automaticamente alterado pelo sistema para 'Em planejamento'. #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.5 Encaminhar Memorando de apresentação da Equipe de auditoria

Elaborar Memorando de Apresentação da Equipe de Auditoria, conforme modelo disponível (link). Atentar para necessidade de revisão de normativos citados no referido modelo (versão do Estatuto, data de aprovação da Assembleia, etc). O memorando assinado e encaminhado pelo Auditor Interno deve ser salvo tanto no Siscor quanto no Sisaudit, como papel de trabalho. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.6 Ajustar aba "Cronograma", informando início da execução do DAP

No sistema de auditoria - Sisaudit, na aba "Cronograma", informar a 'Data início realizado' da tarefa do DAP. O sistema alterará automaticamente a Situação da tarefa do DAP para 'Em andamento'. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

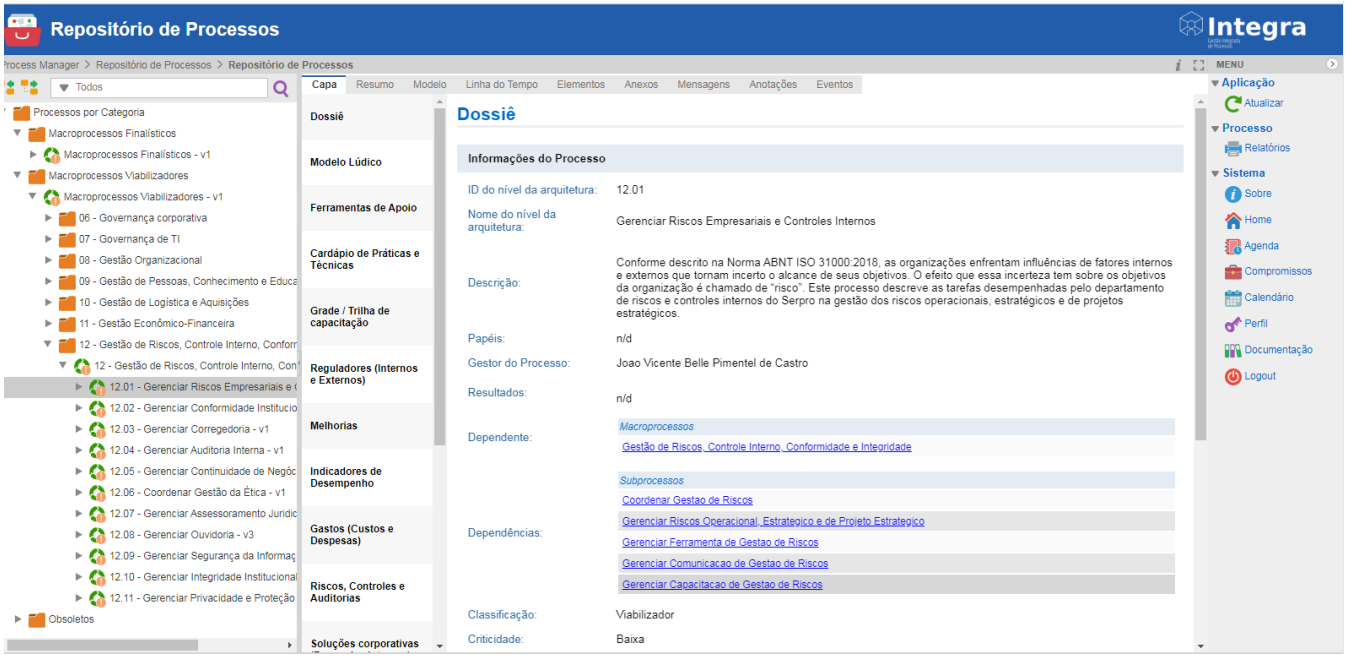
3.1.1.7 Identificar Objetivo da Auditoria e Justificativa para realização do trabalho

Antes de iniciar o planejamento, a equipe de auditoria precisa ter claro porque fazer aquele trabalho, qual o objetivo e escopo dele. Essas diretrizes devem guiar o planejamento como um todo e a definição macro da abordagem. Essas informações devem ser consultadas na aba 'Dados Gerais' da Auditoria no Sisaudit e no PAINT vigente (link), considerando as informações preliminares já levantadas. O 'Resultado' dessa discussão na equipe sobre os objetivos do trabalho deve ser registrado no sistema de auditoria - Sisaudit, na aba "Programa de auditoria", tarefa: Elaborar Documento de Análise Preliminar - DAP, sequencial 7, identificar Objetivo da Auditoria e Justificativa para realização. Esse registro pode ser um simples relato do alinhamento discutido na equipe ou até referenciar algum documento que tenha sido produzido nessa etapa, como por exemplo uma memória de reunião da equipe. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.8 Identificar Objetivo do objeto de auditoria e Metas (operacionais ou estratégicas) associadas

Para que a equipe possa conduzir um bom planejamento de Auditoria Baseada em Riscos (ABR), deve inicialmente identificar se o objeto de auditoria possui objetivos declarados, formalmente registrados. Se

houver metas operacionais ou estratégicas definidas, isso facilita orientar a boa seleção de riscos com potencial impacto sobre aquela métrica, inclusive possibilitando quantificação. Para avaliação das informações relacionadas ao objeto auditável, um dos caminhos é utilizar o sistema integra (link), módulo: Repositório de Processos, escolher o processo afeto e no item Capa/Dossiê, consultar as informações disponíveis.



Devem ser pesquisados também, eventuais políticas, normas, manuais ou outros documentos internos que declarem o objetivo do objeto de auditoria. O sistema de Informações Normativas do Serpro (Sinor) (link) também deve ser consultado. Na intranet - aba Estratégia Empresarial, constam o Planejamento Estratégico vigente (link), bem como, as metas estratégicas, Resultados-Chave, etc. Os indicadores corporativos encontram-se disponíveis no Painel de Indicadores Corporativos (link). Instrumentos como Plano Estratégico de TI (PETI) e Plano Diretor de TI (PDTI), podem ser encontrados na intranet - Governança de TI

(link). O 'Resultado' juntamente com a fonte de referência devem ser registrados no sistema de auditoria - Sisaudit, na aba "Programa de auditoria", tarefa: Elaborar Documento de Análise Preliminar (DAP), sequencial 8, identificar Objetivo do objeto de auditoria e Metas (operacionais ou estratégicas) associadas. É importante que esse entendimento quanto aos objetivos e metas seja validado com os gestores nas etapas iniciais de interlocução para o trabalho. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.9 Identificar a cobertura prevista no PAINT: Processos, Objetivos Estratégicos, Metas Estratégicas, Riscos Estratégicos, Riscos Operacionais

Os objetivos do processo (objeto auditável), respectivos riscos (estratégicos e operacionais) e controles devem estar diretamente associados, a fim de permitir a confirmação se as principais ameaças foram identificadas e se os controles existentes são suficientes para mitigação. Quando da elaboração do PAINT, cada auditoria já nasce com uma primeira associação estruturada de processos, objetivos e riscos que pretende cobrir. No Redmine (link) - "projetos" - PAINT - Auditoria - escolher o item do trabalho em questão, no campo "Tarefas relacionadas" já consta uma primeira vinculação de principais riscos e objetivos estratégicos relacionados ao objeto auditável. Identificar a cobertura prevista no PAINT: Processos, Objetivos Estratégicos, Metas Estratégicas, Riscos Estratégicos, Riscos Operacionais. O planejamento deve buscar assegurar a cobertura prevista no PAINT ou devem ser revisadas as vinculações no Redmine, se necessário. Este processo é importante pois esta vinculação alimentará o indicador de cobertura de riscos e processos do PAINT. O 'Resultado' dessa primeira revisão de cobertura deve ser informado no sequencial 9 do procedimento do DAP. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.10 Identificar na Matriz de Riscos do PAINT os fatores de risco que mais impactaram a avaliação do nível de riscos, inclusive riscos emergentes e expectativas da alta administração

Essa etapa visa que a equipe, no início do processo de planejamento, tenha clareza dos principais aspectos de riscos que justificaram a inclusão daquele trabalho no PAINT do ano, de modo a orientar a abordagem para cobrir esses aspectos. Com base na Matriz de Riscos que embasou o PAINT vigente, disponibilizado como papel de trabalho padrão na abertura de todos os trabalhos no Sisaudit, analisando nas abas 'I. Avaliação de riscos (GESTOR)', 'II. Avaliação de riscos (AUDIN)' e 'III. Avaliação riscos (Alta Adm)' os fatores de risco que mais impactaram a avaliação do nível de riscos. Ex: *há pontuação expressiva para denúncia, pad e sindicância? Qual a criticidade da relação de sistemas (sistemas internos que suportam o processo e/ou sistemas de clientes relacionados com a atividade fim? Como foi a rotação de ênfase deste objeto auditável? O que houve de registro de expectativa da Alta Administração em relação ao objeto auditável? Há riscos emergentes, regulatórios e mudança no processo associados ao objeto auditável? Como o gestor avaliou este processo? Há avaliação RCSA pela Audin?* Avaliar os critérios acima direcionará os esforços para o que há de mais significativo no objeto auditável. Lembrando que a chance de ocorrência de erros significativos e/ou fraude deve ser avaliada em todos os trabalhos de auditoria, sendo considerada para inclusão no escopo. Toda tarefa deve ser #Atribuído para: <inserir> - #Complexidade: <inserir>.

3.1.1.11 Levantar a Materialidade do objeto de auditoria: custos, gastos, despesas, receitas, orçamento ou reflexo contábil

O objetivo dessa etapa é mapear onde está o dinheiro do objeto que está sendo auditado, para auxiliar no enfoque de aspectos relevantes e em uma análise custo benefício dos testes planejados. Por exemplo, um processo de cobrança de débitos tributários para o cliente pode envolver bilhões em débitos tributários em prescrição, milhões em faturamento para o Serpro pelo contrato de receita para cobrança e outros tanto milhões em custos incorridos com a folha de pagamento e demais custos operacionais. A depender do escopo do trabalho é possível adotar diferentes enfoques sobre esse objeto, para buscar potencializar o valor agregado pela auditoria. Inicialmente, vale avaliar as informações de Gastos (Custos e despesas) disponíveis no sistema integra (link), módulo: Repositório de Processos, escolher o processo afeto e no item capa/Dossiê, consultar as informações disponíveis. Uma outra fonte de informação é o painel Gestão de Gastos - Diretoria, disponível no Qlik (link). Para solicitação de acesso ao painel, deve ser usado o link abaixo, seguindo as instruções (link). Valores relativos a contratos de receita e de despesas; orçamentos; dentre outras fontes também podem ser consideradas.

3.1.1.12 Levantar Normativos Internos e legislação aplicável

Para consulta de normativos internos, utilizar o Sinor (link) e os sites de cada Diretoria, a exemplo deste (link). Para consulta de legislação aplicável, utilizar o Portal da Legislação (link), Diário Oficial da União (link); TCU (link) e demais fontes inerentes a cada tema.

3.1.1.13 Levantar referenciais de boas práticas, manuais e bibliografia especializada

Para preenchimento deste item do DAP devem ser observados guias ou conjuntos de boas práticas tais como: COBIT, COSO, TOGAF, Normas ISO, Orientações Suplementares do IIA (link), Fontes Autoritativas no Archer, Manuais publicados, dentre outros. Em acórdãos do TCU relacionados ao tema também pode haver menção do Tribunal a referenciais de boas práticas.

3.1.1.14 Levantar notícias internas e externas sobre o tema

Na caixa de pesquisa da intranet do Serpro e em site de busca na internet, realizar consulta por palavras-chave relacionadas ao objeto da auditoria e ao seu escopo, buscando identificar eventuais notícias internas ou externas relevantes para subsidiar o processo de planejamento da auditoria. Por exemplo, a notícia da conquista de novos clientes internacionais pelos serviços de biometria, a depender do escopo do trabalho, pode trazer um ponto relevante sobre eventuais transferências internacionais de dados pessoais segundo a LGPD, atração da GPDR ou aspectos dos controles financeiros para recebimento no exterior e regras de tributação.

3.1.1.15 Levantar Sistemas internos (seus manuais e controles, considerando mapeamento do GTAG 11 no PAINT), repositórios, painéis, página da unidade e outras fontes de informação relevante

Um primeiro mapeamento dos sistemas internos envolvidos já deve ser informado na aba 'Programa de Auditoria', 'Dados gerais', 'Aplicativos utilizados nas operações'. Nessa tarefa do DAP deve ser buscado detalhamento sobre informações de interesse registradas no sistema, Manuais, controles de perfis, fluxo no sistema e outras informações que auxiliem a utilizá-lo como fonte de informações ou planejar testes específicos (integridade das informações, confirmação dos fluxos, controle de acessos, etc).

3.1.1.16 Levantar processos correlatos, partes interessadas, mecanismos de supervisão/governança, metas e indicadores operacionais, serviços de clientes, contratos de receita e de despesa envolvidos, projetos estratégicos/setoriais e iniciativas PETI/PDTI envolvidas

Essa etapa do levantamento é importante para mapear os processos na empresa impactados pelo objeto da auditoria e que impactam nele, as partes interessadas internas e externas à empresa (inclusive para mapear expectativas) e conexões diretas daquele objeto com metas e iniciativas estratégicas no Serpro. Essas informações são relevantes para subsidiar o planejamento da abordagem da Audin.

3.1.1.17 Levantar Denúncias e outras Demandas Externas sobre o tema

O Levantamento de denúncias, representações ou outras demandas externas ajuda a extrair uma visão pela auditoria sobre possíveis vulnerabilidades no objeto da auditoria, devendo ser aproveitado diretamente da análise de riscos à integridade (fraude, corrupção ou desvios de conduta ética) ou riscos de erros significativos. Os referidos riscos devem ser considerados na Matriz de Riscos do planejamento da auditoria individual.

3.1.1.18 Analisar outros Relatórios da 1ª, 2ª ou 3ª linhas, com respectivos planos de ação

Esse levantamento auxilia a identificar concretamente relatórios e documentos similares produzidos por outros prestadores internos ou externos de serviço de avaliação ou consultoria, que possam trazer conhecimento útil para a etapa de planejamento da auditoria individual. Para além disso, a Auditoria pode optar por depositar confiança no trabalho realizado por terceiros e aproveitar parte dos resultados ou conclusões. Para isso deve adotar prudências adicionais para assegurar a consistência do trabalho realizado, conforme detalhado em item específico desse Manual.

3.1.1.19 Analisar Atas da Diretoria Executiva e respectivos processos decisórios sobre o tema

Essa etapa objetiva mapear concretamente, para aquele objeto específico, eventuais itens de discussão em Diretoria sobre o tema, Notas Técnica elaboradas no âmbito do processo decisório ou outras instruções relevantes para a tomada de decisão gerencial. Eles elementos auxiliam a contextualizar melhor o ambiente e as condições de contorno em que está inserido o objeto de auditoria.

3.1.1.20 Analisar plano de trabalho, pautas, Atas e follow-up sobre o tema no Conselho Fiscal e no Conselho de Administração

Da mesma forma que o item anterior, para mapear expectativas da alta administração é importante conhecer eventuais discussões precedentes sobre o objeto, se há item previsto em plano de trabalho de colegiado (para alinhar cronograma de entrega), se há registro em Ata ou acompanhamento em follow-up do Colegiado. Os planos de trabalho dos colegiados estão refletidos na 'Agenda mandatória' no Archer e as pautas de reuniões são geridas pela Secretaria dos colegiados e a Ata publicadas na Internet. Ainda não houve a consolidação em repositório único, podendo ser aproveitado o conhecimento mantido pela equipe de assessoramento da Audin.

3.1.1.21 Analisar Relatórios e Atas do COAUD sobre o tema, com respectivos planos de ação

Na mesma linha do item anterior, enfocando especificamente a pauta do COAUD, que costuma buscar maiores aprofundamentos de governança, gestão de riscos e controles internos. Além disso, o COAUD elabora relatório anual dos trabalhos, aprovado pelo CA.

3.1.1.22 Analisar Relatórios da Audin e histórico de recomendações

Também é natural que esse levantamento considere eventuais trabalhos anteriores da Audin sobre o tema, inclusive na lógica de rotação de ênfase. O histórico de fragilidades identificadas, recomendações atendidas ou pendentes e de abordagens anteriores deve auxiliar a equipe a propor nova abordagem sobre o tema, com foco no valor adicionado aos clientes da auditoria.

3.1.1.23 Analisar Relatórios (e solicitações) da CGU e histórico de recomendações

Para o caso em que houve trabalhos realizados por órgãos de controle, O histórico de fragilidades identificadas, recomendações atendidas ou pendentes e de abordagens anteriores deve auxiliar a equipe a propor nova abordagem sobre o tema, com foco no valor adicionado aos clientes da auditoria. Nesses casos, a equipe deve se orientar por evitar a sobreposição de esforços ou simplesmente confirmar o que os avaliadores externos já apontaram. Por exemplo, o esforço pode estar mais concentrado em aprofundar causas intermediárias, causa raiz e consequências para apoiar a gestão na solução efetiva das falhas.

3.1.1.24 Analisar Acórdãos (e ofícios de requerimento) do TCU e histórico de determinações ou recomendações

Para o caso em que houve trabalhos realizados por órgãos de controle, O histórico de fragilidades identificadas, recomendações atendidas ou pendentes e de abordagens anteriores deve auxiliar a equipe a propor nova abordagem sobre o tema, com foco no valor adicionado aos clientes da auditoria. Nesses casos, a equipe deve se orientar por evitar a sobreposição de esforços ou simplesmente confirmar o que os avaliadores externos já apontaram. Por exemplo, o esforço pode estar mais concentrado em aprofundar causas intermediárias, causa raiz e consequências para apoiar a gestão na solução efetiva das falhas.

3.1.1.25 Analisar Relatórios de outros avaliadores (ou consultores) externos e respectivos planos de ação

Conforme antes destacado, esse levantamento auxilia a identificar concretamente relatórios e documentos similares produzidos por outros prestadores externos de serviço de avaliação ou consultoria, que possam trazer conhecimento útil para a etapa de planejamento da auditoria individual. Para além disso, a Auditoria pode optar por depositar confiança no trabalho realizado por terceiros e aproveitar parte dos resultados ou conclusões. Para isso deve adotar prudências adicionais para assegurar a consistência do trabalho realizado, conforme detalhado em item específico desse Manual.

3.1.1.26 Analisar outros documentos relevantes

Geralmente nas interlocuções iniciais com os gestores ou do levantamento realizado a equipe toma conhecimento de outros documentos relevantes para realizarem um bom planejamento da abordagem de auditoria, por exemplo: Planos de negócios, análises de viabilidade, atas de comitês de riscos das Diretorias ou COGRS, *benchmarks* realizados, entre outros.

3.1.1.27 Apresentar Processos e áreas envolvidas

No DAP deve ser registrado um diagrama mais visual dos processos da cadeia de valor relacionados e áreas envolvidas, ilustrando artefatos gerados, interfaces críticas, repartição de competências e segregações de funções. Essa visão auxilia a posicionar testes de controle com uma visão corporativa ponta a ponta, enfocando pontos críticos para o sucesso do processo.

3.1.1.28 Apresentar Fluxograma dos (macro)processos

Esse fluxo pode ser simplificado em macroprocessos, justamente para buscar uma visão integrada dos processos, artefatos gerados e evitar apresentar detalhes desnecessários para a abordagem de auditoria, inclusive para evitar o viés de posicionar os testes de auditoria em detalhes operacionais de menor relevância para o trabalho. Ou seja, a partir dos fluxos registrados no Integra para os processos da cadeia de valor, a equipe de auditoria pode apresentar Fluxograma próprio que auxilie a obter uma visão integrada pontos críticos do objeto de auditoria.

3.1.1.29 Submeter ao Supervisor os Pontos críticos dos processos

Os pontos críticos do processo são entendidos como aquelas etapas determinantes para o atingimento dos objetivos e, caso não sejam executadas conforme previsto, possuem impacto relevante no resultado. Pontos críticos não são necessariamente fragilidades, embora também as incluam, mas etapas-chave para o sucesso da execução do processo. Como uma etapa de qualidade do planejamento, é importante validar junto ao Supervisor os pontos críticos mapeados, tendo em vista que concentrarão o foco do planejamento e dos testes de auditoria.

3.1.1.30 Submeter ao Supervisor as Questões de Auditoria propostas, acompanhadas dos métodos e técnicas de auditoria

Para evitar que o Relatório da auditoria perca a visão do todo e se transforme no simples relato de resultados de testes individuais que não se conectam, é importante que a equipe de auditoria desenvolva Questões de Auditorias agregadoras, em que o conjunto de testes traga evidências suficientes, relevantes e úteis para suportar a conclusão apresentada para a respectivas questões. Para que o suporte de evidências seja consistente, é importante que a equipe debata sobre métodos e técnicas de auditoria adequados para obtê-las, inclusive como forma de realizar avaliação preliminar da viabilidade de responder a determinada questão proposta. As respostas às Questões de Auditoria representarão as grandes conclusões obtidas ao final do trabalho. Nesse sentido, como etapa de qualidade, devemos questionar se responder a aquela questão gera interesse no leitor e agrega conteúdo relevante para as partes interessadas. Como boa prática, as Questões de Auditoria devem adotar redação direta, objetiva, positiva, evitando linguagem excessivamente técnica. São exemplos: "*O serviço tal oferecido aos clientes está aderente à LGPD, atendendo à ISO 27701?*" e "*Os riscos críticos e controles-chave estão claramente definidos e são monitorados, resguardando o atingimento das metas e objetivos*". Nesse mesmo sentido, devem ser evitadas redações negativas, por comunicarem um viés de buscar evidências de funcionamento inadequado: "*O serviço prestado está desconforme à norma tal?*" e "*A definição de riscos e controles é insuficiente para assegura o atingimento dos resultados?*" Outro ponto de boa prática na definição das Questões de Auditoria é evitar respostas binárias, de simples 'sim' ou 'não'. A redação deve permitir explorar nuances da resposta, para que mantenha a objetividade e ao mesmo tempo permita explorar eventuais ressalvas. Senão vejamos:

"*Com base nos testes realizados e evidências coletadas pela auditoria, é possível concluir que o serviço tal prestado ao cliente está aderente à LGPD nos aspectos detalhados na metodologia, salvo quanto à privacidade by design, por ter sido construído sobre bases de dados e sistemas legados, sem maiores adequações posteriores. Já no que se refere à conformidade com a ISO 27701 como referencial de boa prática, foram identificadas não conformidades relevantes nas áreas tal e tal, o que <prejudica / não prejudica> a conformidade geral com a norma>*". Do mesmo modo, as Questões de Auditoria também devem evitar questões exploratórias, voltadas a relatar como é executada determinada etapa do processo. Essas questões devem ser respondidas na etapa de planejamento, não no Relatório. Por exemplo: "*Os gestores aprovam planejamento anual explicitando os objetivos e respectivas metas?*" e "*Como é realizada a etapa de levantamento de demanda e planejamento das contratações?*"

3.1.1.31 Defender para o Supervisor a consistência do Objetivo da Auditoria com o Escopo e o Não Escopo da Auditoria, assim como o custo de auditoria (hh, perfis da equipe) registrado no Painel do Qlik <link>

Nessa etapa de conclusão do DAP, realizados os levantamentos de aspectos relevantes a serem testados e delineadas as principais frentes de auditoria refletidas nas Questões de Auditoria, é possível debater junto ao Supervisor e defender a abordagem proposta. Por exemplo, ao consultar o Painel do Qlik pode ser identificado que, com base na equipe alocada, aquela auditoria custará R$ 600 mil para o Serpro. Ao analisar a materialidade levantada, pode ser observado que representa R$ 2 milhões de receita para o Serpro e de R$ 500 milhões em débitos tributários do cliente. Nesse caso, a equipe pode chegar à conclusão que pode ser relevante trazem uma dimensão de clientes para a abordagem do trabalho, buscando maior potencial de gerar impacto positivo relevante com o trabalho. Nesse aspecto a discussão sobre Escopo e Não Escopo da Auditoria devem ocorrer naturalmente como um controle de qualidade para atingimento do Objetivo pretendido com o trabalho, buscando validar se aspectos relevantes ficaram de fora quando poderiam ser abordados ou se detalhes desnecessários foram incluídos e consumirão recursos, mas sem conexão significativa com o Objetivo da auditoria nem impacto relevante projetado no objeto.

3.1.1.32 Revisão do DAP pelo gerente par

Na Audin, a revisão técnica dos trabalhos foi delegada para os Gerentes de Auditoria. Foi criada a figura do Gerente par, inclusive como uma estratégia no âmbito do PGMQ para que temas com interface mantenham um fluxo natural de comunicação e sinergia entre abordagens de auditoria em áreas correlatas, conforme segue:

Gerência de Auditoria	Gerente par
AUDCF	AUDEP
AUDEP	AUDPC
AUDPC	AUDCF
AUDAC	AUDTN
AUDTN	AUDAC
AUDCN	Conforme escopo

O Gerente par deve revisar os principais artefatos do trabalho, incluindo DAP, Matriz de Riscos e Relatório de Auditoria, para que possa realizar as revisões conhecendo o contexto precedente. Embora exista essa alocação ordinária, a depender do escopo do trabalho, de abordagens precedentes, pode ser mais efetivo definir outro Gerente par para um trabalho específico, que deve ser comunicado pelo gerente da equipe responsável pelo trabalho.

3.1.1.33 Na aba 'Cronograma', informar a 'Data fim realizado' da tarefa do DAP, alterando Situação para 'Concluída'

Para fins de acompanhamento de produtividade, assim que concluída a revisão da DAP deve ser informada a 'Data fim realizado' para que essa macroentrega seja considerada concluída naquela data.

3.1.2 Procedimento: Elaborar a Matriz de Riscos da auditoria individual

Apresentar o mapeamento de Objetivos, respectivos Riscos e Controles identificados pelo gestor e complementados pela Audin, explicitando os Testes de Controle planejados e a distribuição deles na equipe de auditoria. Nessa etapa deve ser preenchido o Documento Matriz de Riscos da Auditoria Individual (link). Atribuir um responsável e informar a complexidade.

3.1.2.1 Na aba 'Cronograma', informar a 'Data início realizado' da tarefa da Matriz de Riscos, alterando Situação para 'Em andamento'

Para fins de acompanhamento da produtividade, deve ser informado na aba 'Cronograma' a 'Data início realizado' da Matriz de Riscos, indicando o início dessa etapa da fase de planejamento.

3.1.2.2 Selecionar, do conjunto de informações levantadas no DAP, aquelas relevantes e úteis para orientar o planejamento da Auditoria Baseada em Riscos (ABR)

Tendo em vista a quantidade de informações levantadas na etapa do DAP, para início da elaboração da Matriz de Riscos é interessante revisitar o DAP e selecionar o conjunto de informações e documentos considerados relevantes para orientar as diretrizes do planejamento de ABR.

3.1.2.3 Preencher a Matriz de Riscos com o Objetivo do objeto de auditoria, acompanhado das Metas (operacionais ou estratégicas) associadas e respectivos resultados

A partir do artefato padrão de Matriz de Riscos disponibilizado na página da Audin (link), informar no campo próprio o Objetivo do objeto de auditoria, Metas (operacionais e estratégicas) associadas e respectivos resultados. Na aba 'Programa de Auditoria' no Sisaudit, deve ser incluído um procedimento não padrão na fase de execução para registrar o Objetivo. Dentro dele as metas operacionais ou estratégicas devem ser registradas como testes, incluindo os testes de qualidade detalhados a seguir neste Manual.

3.1.2.4 Preencher a Matriz de Riscos com a Extração de Riscos e Controles no Archer, conforme link disponibilizado

Consta do modelo de Matriz de Riscos - Auditoria o link para acesso a extração padronizada do Archer apresentando Riscos (operacionais, de projetos e de segurança da informação) aprovados, acompanhados dos níveis de riscos atual e final, assim como dos respectivos controles, seus estágios de implantação e processos da cadeia de valor envolvidos. Para facilitar filtrar pelos processos de interesse, a equipe deve primeiro filtrar pela unidade organizacional gestora, filtrar os processos selecionados e na sequência desmarcar a unidade (para que sejam apresentados riscos transversais de outras unidades que impactem aqueles processos). O resultado dessa extração deve ser incluído da Matriz de Riscos como ponto de partida para a reavaliação pelos auditores.

3.1.2.5 Considerando histórico de denúncias, sindicâncias e PADs no PAINT, representações no TCU e pontos críticos do processo no DAP, triângulo da fraude no RCSA, riscos de integridade já mapeados pelo gestor na extração no Archer, apresentar reflexão crítica da Audin sobre Risco de Integridade (fraude, corrupção ou desvio de conduta ética) ou de erros significativos no objeto de auditoria

Segundo a IPPF Norma 2120.A2 - A atividade de Auditoria Interna deve avaliar o potencial de ocorrência de fraude e a forma como a organização gerencia o risco de fraude. Essa etapa visa materializar a visão da Audin sobre riscos de fraude ou de erros significativos. Nele devem ser considerados tanto os riscos de integridade já meados pelos gestores, quanto as tipologias levantadas no DAP a partir de denúncias, sindicâncias e PAD. Se houver análise específica sobre o triângulo (diamante ou pentágono) da fraude (link) no RCSA, também pode ser aproveitada. Caso contrário, como boa prática é recomendável que essa análise seja conduzida pela própria equipe da Audin, explorando hipóteses no processo que reúnam pressão (financeira do indivíduo, por resultados), racionalização (autoconvencimento de que o ato desonesto é justificável) e oportunidade (fragilidade dos controles, conjugada com capacidade para praticar o ato e o cálculo mental de risco/retorno). O risco de fraude ou de erros significativos selecionado pela equipe deve ser avaliado por ela quanto a probabilidade e impacto, justificando na matriz a realização (ou não) de testes de controle específicos, considerando também o objetivo e escopo do trabalho.

3.1.2.6 Considerando o conjunto de tipologias extraídas das informações levantadas no DAP, em especial pontos críticos do processo, demandas de órgãos de controle, riscos emergentes e visão de riscos da alta administração no PAINT, complementar os riscos já mapeados pelo gestor com a visão de riscos pela Audin, analisando causas, consequências e identificando respectivos controles

Na Auditoria Baseada em Riscos (ABR), tão importante quanto consumir da visão de riscos já mapeada entre 1ª e 2ª linhas, é essencial que a Auditoria Interna, atuando como 3ª linha, traga sua reflexão crítica sobre os riscos que incidem no objeto de auditoria. Assim, no exercício do julgamento profissional, os auditores internos devem reavaliar a probabilidade e impacto dos riscos já mapeados, assim como propor novos riscos não mapeados a partir dos seus próprios levantamentos. Essa abordagem reforça a independência e objetividade da abordagem pela Audin, contribuindo para estruturar novas visões sobre o mesmo objeto. Nesse sentido, a equipe deve aproveitar tipologias levantadas no DAP, em especial pontos críticos do processo, demandas de órgãos de controle, riscos emergentes e visão de riscos da alta administração no PAINT, para orientar seu julgamento profissional e realizar análise adequada de causas, consequências e respectivos controles.

3.1.2.7 Realizar reavaliação de probabilidade e impacto dos riscos extraídos do Archer e avaliação daqueles identificados pela Audin, hierarquizando pelo Nível de Riscos. Aproveitar propostas de Questões de Auditoria do DAP para agrupar os conjuntos de riscos (e respectivos controles) pertinentes para aprofundar, dentro do Escopo planejado da auditoria

Feita a revisão crítica quanto a probabilidade e impacto dos riscos mapeados pelos gestores ou pela própria Audin, os riscos devem ser hierarquizados por Nível de Risco, podendo ser aproveitadas as Questões de Auditoria para agregá-los em blocos temáticos ou de aspectos impactados. Essa hierarquização é essencial para o sucesso da ABR e para compensar o esforço de planejamento realizado. Essa ordenação deve orientar a seleção de testes e técnicas de auditoria, a alocação de recursos para realizá-los, assim como a

definição de critério de parada (a partir do qual as evidências são suficientes, sendo dispensáveis testes adicionais).

3.1.2.8 Realizar reunião de Abertura dos trabalhos, Apresentando objetivo e cronograma previsto da auditoria, equipe de auditoria e papéis, responsabilidades do auditado, tratativas para acesso a ativos e informações necessárias para realizar o trabalho, etapas básicas do processo de auditoria, formas de comunicação, e Debatendo questões de auditoria e respectivos critérios de auditoria, assim como dúvidas ou sugestões do auditado

A reunião de Abertura dos trabalhos deve ser realizada a partir do momento que a equipe de Auditoria possua clareza quanto à abordagem pretendida, isso inclui a apresentação das questões e dos critérios de auditoria, assim como cronograma previsto. A depender do objeto da Auditoria, por exemplo em assuntos de atuação recorrente, é possível antecipar a apresentação, visto que a abordagem já é conhecida pelos envolvidos. Por outro lado, em abordagens novas que envolvam um esforço adicional de planejamento, pode ser o caso de antecipar a reunião de apresentação para facilitar o levantamento de informações junto aos gestores para subsidiar o processo de planejamento.

3.1.2.9 Facilitar a autoavaliação pelos gestores da Autoavaliação da Maturidade de Riscos e Controles (RCSA), baseada no COSO ICIF, aproveitando as informações levantadas no DAP e na extração de riscos e controles para orientar a entrevista e explorar outros temas relevantes para complementar a Matriz de Riscos

Essa etapa de facilitar a autoavaliação no RCSA é geralmente realizada junto com a reunião de Abertura, preferencialmente com a participação do Superintendente responsável e do titular da Auditoria Interna ou o gerente de auditoria. É recomendável que essa interlocução com foco em riscos e controles, conforme 5 componentes e 17 princípios do COSO-ICIF, seja aproveitada para explorar junto ao gestor aspectos de interesse já mapeados nas etapas de planejamento, buscando identificar fontes relevantes e validar a compreensão sobre o objeto de auditoria. Ao final da facilitação, deve ser alinhado junto ao gestor o envio por Solicitação de Auditoria, com prazo de até 5 dias úteis, para conclusão da autoavaliação e inclusão das evidências ou comentários.

3.1.2.10 Incluir na Matriz de Riscos testes voltados a subsidiar a opinião da Audin, baseada no COSO ICIF, sobre a Autoavaliação da Maturidade de Riscos e Controles (RCSA) pelos gestores. A opinião da Audin, juntamente com a Autoavaliação pelos gestores, será consolidada no Relatório de Riscos e Controles Internos - RRC e subsidiarão eventuais recomendações de melhorias de GRC

Feita a facilitação da autoavaliação pelos gestores no RCSA, a equipe possuirá mais elementos para incluir na Matriz de Riscos do trabalho a precisão de testes específicos para avaliar o estágio de maturidade de riscos e controles, consolidando a opinião do RRC. A depender do resultado da avaliação, a equipe verificará a necessidade de elaborar recomendação correspondente, voltada a melhorias de GRC. Como aspecto de qualidade da auditoria, é importante que a equipe enxergue que os aspectos mais relevantes identificados no levantamento voltado ao RRC possuem testes de auditoria correspondentes para suportar a opinião da Audin ao final do trabalho.

3.1.2.11 Feita a priorização de Riscos inerentes críticos e Controles-chave, desenvolver Testes de Controle a serem aplicados para coletar evidências suficientes, adequadas e úteis acerca do funcionamento efetivo dos controles e da gestão de riscos, explicitando os critérios de auditoria adotados como parâmetro (sejam normas ou referenciais de boas práticas)

A auditoria deve enfocar nos riscos inerentes críticos e nos controles-chave. Para fins de auditoria, o conceito de riscos inerentes engloba dois aspectos: riscos puros, sem considerar o efeito dos controles; riscos inerentemente críticos ao negócio auditado (e.g: segurança da informação, cybersegurança, infraestruturas críticas, atendimento de incidentes, sustentação do serviço, continuidade de negócios, são exemplos de riscos inerentemente críticos para uma empresa de TI). O primeiro aspecto é importante para evitarmos o viés de consideramos efetivos os controles para reduzir o nível de risco ao apetite e o segundo aspecto visa validar que o risco tem o potencial de impactar de modo relevante as operações. Os controles-chave são aqueles controles determinantes para trazer o nível de risco para a faixa de apetite e nesse sentido devem ter seus testes de controle priorizados, devido à relevância para a efetividade da gestão de riscos e asseguração dos objetivos. Para os testes devem ser indicados os critérios de auditoria (sejam normas ou referenciais de boas práticas) que representação a situação que se espera encontrar, a ser confrontada com a situação encontrada após a realização dos testes.

3.1.2.12 Realizar análise custo vs. benefício dos Testes de Controle, priorizando aqueles de menor custo de aplicação e a maior nível de asseguração sobre os Riscos e Controles mais relevantes (maior Nível de Risco) para o Escopo planejado. Atualizar na Matriz de Riscos as 'Horas Previstas' para cada Teste planejado, que orientará as referências '#Complexidade' no Sisaudit

Essa análise custo vs. Benefício consiste em etapa natural de revisão de qualidade, a partir do momento em que a equipe possui clareza dos riscos inerentes críticos, controles-chave, testes de controle planejados e respectivas complexidades, é natural a reflexão quando ao esforço vs. Retorno. Nessa etapa a equipe pode concluir que os testes estão bem dimensionados/posicionados, que estão subdimensionados ou sobredimensionados, realizando ajustes, redefinindo prioridades e promovendo os devidos registros no Sisaudit. O registro do 'Resultado' no Sisaudit pode ser desde um breve relato das ponderações e conclusões entre equipe e supervisor, até um artefato estruturado, com mapa de calor, mostrando que a maior parte do esforço de testes da auditoria está dimensionada e posicionada conforme controles-chave e riscos críticos. Os riscos críticos e os controles-chave priorizados devem ser registrados cada um como um procedimento não padrão na aba 'Programa de Auditoria' no Sisaudit, conforme padrão definido. Uma vez definidos e registrados no Sisaudit os procedimentos para cada risco crítico e controle-chave, os testes de controle devem ser registrados dentro dos respectivos procedimentos, referenciando o '#Complexidade' de cada teste.

3.1.2.13 Distribuição na Matriz de Riscos dos Testes de Controle priorizados, conforme perfil de proficiência dos membros da equipe, que orientará as referências '#Atribuído para' no Sisaudit

Registrados no Sisaudit os procedimentos não padrão espelhando os riscos críticos e controles-chave, dentro deles os respectivos testes de controle e complexidade, o Supervisor ou o Auditor responsável devem realizar a distribuição dos testes entre os membros da equipe referenciando o '#Atribuído para' no campo 'Resultado' de cada teste. Essa distribuição deve naturalmente observar o perfil de proficiência dos membros da equipe, para assegurar que possuam os conhecimentos necessários para realizar os testes.

Além disso, deve observar sinergias entre os testes, de modo que a construção do conhecimento pelo auditor auxilie a desenvolver os testes tomados em conjunto.

3.1.2.14 Os membros de equipe atribuídos devem elaborar amostragem aleatória, conforme cabível, de modo a reforçar a abrangência da aplicação dos Testes planejados e submeter ao Supervisor

Sempre que for necessário elaborar amostragem, é recomendável que sejam adotados dois estratos: uma amostra aleatória e uma amostra não probabilística (baseada no julgamento profissional). Como referência, pode ser utilizado o manual do TCU de 'Técnicas de Amostragem para Auditorias' (link). O registro do resultado dessa etapa pode ir desde uma rotina em *software* de planilha, com a ordenação de lista a partir de números aleatórios, utilizando semente não controlada pela equipe (e.g.: nº da auditoria no formato AAAANNN), até a extração de rotina realizada em software estatístico. De todo modo, deve-se buscar assegurar que a amostragem é livre de manipulação e que, com a mesma semente, mesma função e relação de entrada, outro auditor chegue exatamente à mesma amostra. A preocupação quanto à representatividade da amostra é especialmente relevante quando houver a expectativa de realizar inferências estatísticas para avaliar o todo a partir da análise da amostra. Nos demais casos, é suficiente adotar uma abordagem de seleção por Pareto (80/20).

3.1.2.15 Os membros de equipe atribuídos devem, conforme cabível, elaborar amostragem não probabilística, baseadas no Julgamento profissional, de modo a orientar o foco da aplicação dos Testes planejados e submeter ao Supervisor

Pela experiência da equipe com o objeto da auditoria, é possível que tenha desenvolvido avaliação própria quanto a fatores de riscos (de maior materialidade, revisados fora do fluxo, com histórico de problemas, etc). Esses itens devem integrar o estrato de amostra não probabilística, sendo indicado no 'Resultado' as premissas adotadas para seleção e o resultado geral, acompanhado de anexo com o resultado da seleção.

3.1.2.16 Supervisor deve revisar a Matriz de Riscos, inclusive as amostras aleatórias e as não probabilísticas selecionadas, submetendo Matriz e amostras à revisão pelo gerente par

A revisão de qualidade pelo Supervisor deve ocorrer ao longo de todo o processo de planejamento, essa é uma etapa de fechamento, com a revisão final da Matriz de Riscos e dos critérios de amostragem. Concluída essa revisão geral, o Supervisor deve submeter a Matriz de Riscos à revisão pelo gerente par, acompanhada dos critérios de amostragem e outros documentos de suporte.

3.1.2.17 Revisão da Matriz de Riscos pelo gerente par

A revisão pelo gerente par deve ser entendida como revisão expedita, como uma opinião externa à equipe que conduziu diretamente o planejamento. Nesse sentido, a revisão principal continua sendo aquela conduzida pelo Supervisor do trabalho. O gerente par deve buscar avaliar a consistência geral do planejamento e critérios de amostragem, suficiência geral dos testes para sustentar as respostas às questões de auditoria, eventuais aspectos relevantes não contemplados no planejamento, eventuais desvios de foco e alinhamento ao objetivo do trabalho.

3.1.2.18 Atualizar no Redmine a cobertura planejada de Objetivos, Metas, Riscos, Controles e Processos, incluindo e excluindo os relacionamentos adequados na tarefa de Auditoria correspondente, visando manter atualizado o Mapa de Cobertura do PAINT

Encerradas as revisões do Planejamento, considera-se definida a cobertura planejada de Objetivos, Metas, Riscos, Controles e Processos. Nesse ponto, é importante atualizar a cobertura do trabalho na tarefa respectiva no Redmine, incluindo ou excluindo as tarefas relacionadas, visando manter atualizado o Mapa de Cobertura do PAINT.

3.1.2.19 Incluir, no 'Programa de Auditoria' no Sisaudit, procedimento na fase de execução refletindo o OBJETIVO do objeto de auditoria, explicitando os Testes planejados quanto a consistência da apuração das Metas, Resultados e Indicadores associados, considerando os atributos de: Mensurabilidade, Confiabilidade, Estabilidade, Validade, Periodicidade e Auditabilidade. Indicar a distribuição dos Testes na equipe referenciando os '#Atribuído para' e os '#Complexidade'

Na aba 'Programa de Auditoria' no Sisaudit, no procedimento não padrão que reflete o objetivo, deve ser incluído um teste para cada Meta, Resultados e Indicadores associados. Além disso, deve ser incluído um teste geral para avaliação dos seguintes atributos gerais: Mensurabilidade, Confiabilidade, Estabilidade, Validade, Periodicidade e Auditabilidade, conforme conceituado a seguir.

- Mensurabilidade - O indicador é objetivo? Os dados são facilmente localizados?
- Confiabilidade - Os dados do indicador têm fontes confiáveis, com metodologia transparente de coleta, processamento e divulgação?
- Estabilidade - É possível estabelecer séries históricas estáveis e coerentes, que permitam monitoramento e comparações com baixa interferência de variáveis externas?
- Validade - O indicador demonstra, com maior proximidade possível, a realidade que se deseja medir?
- Periodicidade - É possível ter uma menor frequência de mensuração, permitindo uma maior atuação para melhorias de desempenho?
- Auditabilidade - É possível, a qualquer momento, a verificação dos dados relativos à construção e gestão do indicador?

3.1.2.20 Incluir, no 'Programa de Auditoria' no Sisaudit, procedimento na fase de execução refletindo os RISCOS priorizados conforme escopo da auditoria, explicitando os Testes planejados quanto aos seguintes atributos de qualidade do registro de riscos: Adequabilidade, Eficácia e Monitoramento. Indicar a distribuição dos Testes na equipe referenciando os '#Atribuído para' e os '#Complexidade'

Na aba 'Programa de Auditoria' no Sisaudit deve ser incluído um procedimento não padrão para cada Risco priorizado, adotando a nomenclatura padronizada no modelo da Matriz de Riscos. Todo procedimento de risco deve incluir um teste padrão sobre os atributos de qualidade dos registros de riscos, conforme conceituado a seguir.

ATRIBUTOS DE QUALIDADE DOS RISCOS	INEXISTENTE (Nota: 0)	FRACO (Nota: 1)	MEDIANO (Nota: 2)	FORTE (Nota: 3)

Adequabilidade: O risco-chave está definido quanto ao objetivo que atinge, seu impacto, probabilidade, causas, consequências e com definição clara do apetite e dos responsáveis.	0- Inexistente: Não há descrição do risco, ocorrendo de modo informal.	1-Fraco: Há definição formal dos riscos, com definição clara quanto ao objetivo que atinge, seu impacto e probabilidade de ocorrência, mas sem identificar os riscos-chave e riscos de fraude.	2-Mediano: Há definição clara e formal dos riscos-chave e de riscos de fraude. Houve estudo para identificar causas e consequências, com definição clara do apetite e dos responsáveis.	3-Forte: Há visão prospectiva dos riscos emergentes e de riscos positivos (oportunidades), o que reorienta a estratégia e as revisões periódicas da própria gestão de riscos.
Eficácia: A gestão de riscos propicia uma razoável garantia de que os objetivos, metas, resultados e indicadores serão atingidos.	0-Inexistente: Ausência de aplicação da gestão de riscos	1-Fraco: Gestão de riscos sem aplicação consistente. Ocorrem falhas eventuais que impactam resultados ou sua ocorrência é latente.	2-Mediano: A gestão de riscos funciona, reduziu a quantidade e/ou impacto das falhas/deficiências, contudo necessita de aprimoramento	3- Forte: não foram detectadas falhas, sendo realizada análise custo vs. benefícios dos controles para orientar as revisões periódicas da gestão de riscos.
Monitoramento: O nível de risco é revisado numa base frequente, inclusive com a definição de Indicadores (KRI) que demonstrem se realmente há o tratamento esperado em relação ao risco associado, bem como a identificação de riscos emergentes e a comunicação (reporte) de exposições excessivas (fora do apetite).	0-Inexistente: Não é realizado monitoramento dos níveis de riscos.	1- Fraco: O monitoramento dos níveis de riscos é realizado de forma eventual ou sem periodicidade definida.	2-Mediano: O monitoramento dos níveis de riscos é realizado por indicadores (KRI) ou mapeamento de riscos emergentes, sendo comunicadas (reportadas) exposições excessivas a riscos (fora do apetite).	3- Forte: O monitoramento ocorre forma contínua, com gatilhos de alertas quando atingido determinado limite de tolerância dos indicadores-chaves de risco (KRI) ou de riscos emergentes mensurados.

Fonte: MOT-CGU e COSO ICIF.

3.1.2.21 Incluir, no 'Programa de Auditoria' no Sisaudit, procedimento na fase de execução refletindo os CONTROLES priorizados conforme escopo da auditoria, explicitando todos os Testes de Controle detalhados na Matriz de Riscos, referenciando os '#Atribuído para' e os '#Complexidade', e incluindo testes para os seguintes atributos de qualidade dos Controles: Adequabilidade, Eficácia e Monitoramento

Na aba 'Programa de Auditoria' no Sisaudit deve ser incluído um procedimento não padrão para cada Controle priorizado, adotando a nomenclatura padronizada no modelo da Matriz de Riscos. Todo procedimento de Controles deve incluir um teste padrão sobre os atributos de qualidade dos controles, conforme conceituado a seguir.

ATRIBUTOS DE QUALIDADE DOS CONTROLES	INEXISTENTE (Nota: 0)	FRACO (Nota: 1)	MEDIANO (Nota: 2)	FORTE (Nota: 3)
Adequabilidade: O controle está definido em normativo ou instruções escritas, com definição clara de pessoal envolvido, responsabilidades, fluxo do processo e estrutura(sistemas, unidades).	0- Inexistente: Não há descrição do controle, ocorrendo de modo informal.	1-Fraco: Há uma descrição informal do controle-chave, não havendo definição clara e explícita de instruções, responsabilidades, fluxos, sistemas, informações necessárias para validação e tipo do controle.	2-Mediano: Há definição clara e formal do controle-chave, incluindo também categorizações do controle conforme Metodologia corporativa. Houve estudo para identificar e atuar nas causas, nas consequências ou no próprio risco.	3-Forte: A descrição do controle atende aos requisitos da Metodologia corporativa e são proporcionais aos riscos que tratam, o que orienta as revisões periódicas da gestão de riscos.
Eficácia: O controle propicia uma razoável garantia de que os objetivos e metas serão atingidos, evitando falhas de maneira eficaz e eficiente.	0-Inexistente: Ausência de aplicação do controle	1-Fraco: Controle sem aplicação consistente. Ocorrem falhas eventuais ou sua ocorrência é latente.	2-Mediano: Controle funciona, reduziu a quantidade e/ou impacto das falhas/deficiências, contudo necessita de aprimoramento	3- Forte: não foram detectadas falhas, sendo realizada análise custo vs. benefícios dos controles para orientar as revisões periódicas da gestão de riscos.

Monitoramento: O controle é acompanhado numa base frequente, inclusive com a definição de Indicadores que demonstrem se realmente há o tratamento esperado em relação ao risco associado, bem como a identificação e a comunicação (reporte) de materialização do risco e de deficiências de controle.	0-Inexistente: Não é realizado monitoramento e teste dos controles.	1- Fraco: O monitoramento e teste dos controles é realizado de forma eventual ou sem periodicidade definida.	2-Mediano: O monitoramento é realizado por indicadores ou alertas de falhas, sendo acompanhado e reportado via relatório com periodicidade definida.	3- Forte: O monitoramento ocorre forma contínua, com gatilhos de alertas quando atingido determinado limite de tolerância dos indicadores-chaves de risco (KRI) ou de problemas (materialização do risco).

Fonte: MOT-CGU e COSO ICIF.

3.1.2.22 O designado Auditor responsável deve concluir o preenchimento da seção 'Planejamento do Trabalho' da Avaliação Interna de Qualidade, conforme monitoramento contínuo de qualidade previsto no PGMQ

Concluído o registro do planejamento na aba 'Programa de Auditoria' no Sisaudit, o Auditor responsável (ou o Supervisor) deve preencher a seção 'Planejamento do Trabalho na Avaliação Interna de Qualidade (link).

3.1.2.23 Na aba 'Cronograma', informar a 'Data fim realizado' da tarefa da Matriz de Riscos, alterando Situação para 'Concluída'. Concluída a fase de Planejamento no Cronograma, o Status da auditoria deve ser alterado para 'Em execução'

Para fins de acompanhamento da produtividade, deve ser registrado na aba 'Cronograma' a 'Data fim realizado' da macroentrega da Matriz de Riscos da auditoria individual.

3.2 Execução

Na etapa de execução, o programa de trabalho deve ser executado conforme planejamento aprovado no Sisaudit. Se houver revisão ou ajustes no planejamento, o 'Programa de Auditoria' deve ser reaberto no Sisaudit, revisado e novamente submetido a supervisão e aprovação pelo Supervisor do trabalho.

3.2.1 Execução do Programa de Trabalho: Testes, Achados e Recomendações propostas

Nesta fase são realizados os testes previstos, por meio das técnicas de auditoria selecionadas no planejamento. O resultado dos testes deve ser diretamente registrado no Sisaudit. A equipe de auditoria deve comparar a situação encontrada durante a execução do trabalho com os critérios preestabelecidos no programa de trabalho. Os resultados dessa comparação, os achados de auditoria, deverão estar suportados por evidências suficientes, confiáveis, fidedignas, relevantes e úteis que devem ser registradas e armazenadas no Sistema de Auditoria, como papéis de trabalho. Os conceitos constam do MOT e estão transcritos a seguir. A evidência **suficiente** é aquela concreta, adequada e convincente. Uma evidência suficiente permite que qualquer pessoa prudente e informada chegue às mesmas conclusões que o auditor interno governamental. Esse atributo é afetado pelo risco de auditoria e também pelos demais atributos de qualidade. Quanto maior o risco de auditoria, mais provável será a necessidade de uma quantidade maior de evidências. E quanto melhor for a qualidade, menor a quantidade de evidências necessárias. Não obstante, apenas a obtenção de mais evidências não compensará a má qualidade das provas obtidas. Informações **confiáveis** podem ser entendidas como as melhores possíveis de serem obtidas por meio da utilização de técnicas de auditoria apropriadas. Para que sejam confiáveis, as evidências devem ser também

fidedignas, ou seja, válidas e representarem de forma precisa os fatos, sem erros ou tendências. Embora não haja regras rígidas para determinar a confiabilidade das evidências, existem diretrizes gerais que podem ser utilizadas pelos auditores internos governamentais, quais sejam:

a) evidência obtida de terceiros independentes tende a ser mais imparcial do que aquela obtida junto à Unidade Auditada;
b) evidência produzida por um processo ou sistema com controles efetivos é mais confiável do que aquela produzida por um processo ou sistema com controles ineficazes;
c) evidência obtida diretamente pelo auditor interno tende a ser mais confiável do que evidência obtida indiretamente;
d) evidência proporcionada por documentos originais é mais confiável do que a evidência proporcionada por fotocópias;
e) evidência corroborada por informações oriundas de outras fontes tende a ser mais confiável do que aquela que é obtida em uma única fonte.

Ao utilizar as diretrizes acima, no entanto, é necessário que os auditores considerem outros aspectos que podem influenciar as evidências, tais como fonte, natureza e circunstâncias em que são obtidas. Em casos de dúvida a respeito da confiabilidade das informações ou indicações de possível fraude, o auditor deve realizar procedimentos adicionais e determinar quais modificações serão necessárias para solucioná-la. É fundamental também que, nesse processo, avaliem a relação custo-benefício. O atributo da relevância assegura que a evidência esteja diretamente relacionada aos objetivos e ao escopo do trabalho. A avaliação do que seja uma informação relevante é também uma questão de lógica e de julgamento profissional. A utilidade da informação registrada como evidência relaciona-se com a sua capacidade de auxiliar a Unidade Auditada a atingir os seus objetivos. Ou seja, deve agregar valor e permitir a melhoria das operações organizacionais. Para tanto, ela deverá ser útil para a construção dos achados e para a formação da opinião emitida pelo auditor. Mais informações sobre Testes de controle, Testes substantivos, e Técnicas de auditoria podem ser obtidos nos itens 4.3.4.4 a 4.3.4.6 do MOT, respectivamente.

3.3 Encerramento

3.3.1 Elaborar Documento de Apresentação dos Achados

Apresentação ao gestor dos achados de auditoria, com base no resultado dos Testes de Controle confrontados com os critérios de auditoria estabelecidos. Solicitar manifestação ao gestor, acompanhada de Plano de Ação (ações, prazos e responsáveis), e realizar a Reunião de Plano de Ação com foco em pactuar os encaminhamentos (recomendações), aproveitando para validar entendimentos que irão para o Relatório.

3.3.1.1 Na aba 'Cronograma', informar a 'Data início realizado' da tarefa do Documento de Apresentação dos Achados, alterando Situação para 'Em andamento'

Para fins de monitoramento da produtividade, é importante informar a 'Data início realizado' da fase de encerramento do trabalho, ligada à apresentação consolidada dos achados aos gestores.

3.3.1.2 O designado Auditor responsável deve concluir o preenchimento da seção 'Execução dos Exames' da Avaliação Interna de Qualidade, conforme monitoramento contínuo de qualidade previsto no PGMQ, inclusive confirmando a ausência de ameaças, de fato ou veladas, e a manutenção da independência e da objetividade da opinião da equipe.

Logo no início da fase de encerramento, o designado Auditor responsável (ou o Supervisor) deve preencher a seção 'Execução dos Exames' da Avaliação Internas de Qualidade, confirmando que, entre outros requisitos de qualidade, os trabalhos foram executados e que os achados serão desenvolvidos em ambiente de ausência de ameaças, de fato ou veladas, e a manutenção da independência e da objetividade da opinião da equipe.

3.3.1.3 Revisão dos Achados pelo auditor par, avaliando se as evidências reúnem os seguintes atributos de qualidade: são suficientes, confiáveis, fidedignas, relevantes e úteis

Trata de revisão expedita por outro auditor da equipe, buscando assegurar os atributos de qualidade das evidências antes apresentados. O registro do 'Resultado' dessa tarefa no Sisaudit pode ir desde um simples relato da discussão dos achados realizada de modo coletivo na equipe, até o registro do revisor em cada papel de trabalho.

3.3.1.4 Revisão dos Achados pelo auditor par, avaliando se possui causas (raiz) e consequências identificadas, acompanhadas dos critérios de auditoria e das condições (situações encontradas), assim como avaliação de probabilidade e de impacto (nível de risco)

A revisão por pares deve incluir também os referidos atributos de qualidade dos achados, que orientarão a comunicação, a relatoria e o plano de ação.

3.3.1.5 Na aba 'Relatório de Auditoria' no Sisaudit incluir os Achados, detalhando Título, Situação identificada (condição), Corpo do achado (condição detalhada vs. critério), referenciando testes relacionados e respectivos anexos

Concluída a revisão por pares, os achados já podem ser incluídos na aba 'Relatório de Auditoria' no Sisaudit, detalhando no campo 'Situação identificada' a condição e no campo 'Corpo do achado' a condição (situação encontrada) detalhada, comparada ao critério de auditoria esperado. O achado deve referenciar os testes de auditoria que o suportam, assim como os papéis de trabalho respectivos.

3.3.1.6 Para cada Achado, apresentar proposta de Recomendação, prazo e responsável, registrando a Probabilidade e Impacto. Como boa prática de qualidade das Recomendações, verificar se estão claros os requisitos 5W2H: O Quê, Por que, Onde, Quando, Quem, Como, Por quanto. Atendidos os requisitos, submeter à aprovação pelo Supervisor

A equipe deve elaborar uma proposta de Recomendação que auxiliará a conduzir a Reunião de Plano de Ação, compondo com a visão de ações propostas pelos gestores responsáveis. Como boa prática, as recomendações propostas devem definir claramente os requisitos 5W2H, conforme segue.

WHAT	*WHY*	*WHERE*	*WHEN*	*WHO*	*HOW*	*HOW MUCH*
Criação de um novo website	Aumentar a geração de oportunidades comerciais	Online	De 01/11/2015 a 15/11/2015	Pedro Campos	Contratação de agência especializada	R$ 4.500,00
Capacitação da equipe de atendimento	Reduzir o número de reclamações dos clientes	Campinas	10/11/2015	Equipe de atendimento	Treinamento *in-company*	R$ 9.000,00
Implantação de um sistema de gestão orçamentária	Melhorar a previsibilidade de resultados e reduzir riscos futuros	Online	De 05/11/2015 a 10/11/2015	Camila Campos	Contratação de solução *online* especializada	R$ 399,00 / mês

Fonte: Blog Treasy

3.3.1.7 Elaborar Relatório de Riscos e Controles - RRC conforme formulário padronizado pela Auditoria Interna, avaliando os 5 componentes e 17 princípios do COSO ICIF - Estrutura Integrada de Controles Internos, registrando o score obtido no Sisaudit, na aba 'Relatório de Auditoria', campo 'Nota de avaliação do controle interno (NACI)' e o resultado da avaliação no campo 'Conclusão'

O Relatório de Riscos e Controles - RRC, contendo a avaliação da Audin sobre os 5 componentes e 17 princípios do COSO-ICIF deve ser preenchida a partir do modelo disponível na página da Audin (link), registrando o score obtido no Sisaudit, na aba 'Relatório de Auditoria', campo 'Nota de avaliação do controle interno (NACI)' e o resultado da avaliação no campo 'Conclusão'. Futuramente, pretende-se que o detalhamento da informação do RRC seja alimentada em sistema de modo estruturado.

3.3.1.8 Com base no Relatório de Riscos e Controles - RRC elaborado pela auditoria aplicando o COSO-ICIF, levando em conta a autoavaliação pelo gestor na Autoavaliação da Maturidade de Riscos e Controles (RCSA), avaliar a oportunidade e necessidade de propor Recomendação voltada a melhorias significativas de Governança, Gestão de Riscos ou Controles Internos

Considerando que na etapa do planejamento foram incluídos testes voltados a coletar evidências para subsidiar a avaliação com foco no COSO-ICIF e levando em conta a possibilidade de obter melhorias significativas de Governança, Gestão de Riscos ou Controles Internos, a equipe de auditoria deve avaliar a oportunidade e necessidade de propor Recomendação decorrente da avaliação no RRC.

3.3.1.9 Na aba 'Relatório de Auditoria' no Sisaudit gerar o Quadro de Achados (Documento de Apresentação dos Achados), ordenar a comunicação por nível de risco (preferencialmente 1 item de NA por Achado) e encaminhar por meio de Nota de Auditoria (ou aproveitar consolidação de NAs expedidas ao longo do trabalho) para apresentação de Plano de ação (ações, responsáveis e prazos) pelo gestor, acompanhada de eventuais manifestações no prazo de ATÉ 5 (cinco) dias úteis

Preenchidos no Sisaudit os Achados de Auditoria e as propostas de Recomendação, é possível gerar o Quadro de Achados diretamente na aba 'Relatório de Auditoria'. No entanto, essa funcionalidade tem apresentado instabilidade no sistema, havendo chamado aberto para a equipe de desenvolvimento. Nesse sentido, podem ser utilizados os *templates* de 'Quadro de Achados' ou 'Apresentação para Reunião de Plano de Ação', disponibilizados na página da Audin (link) ou outro modelo mais detalhado definido pela equipe

de auditoria. A equipe deve avaliar se o envio ocorrerá em branco (sem texto de recomendações propostas) ou em preto (com texto de recomendações propostas), considerando o equilíbrio entre aspectos como possíveis vieses decorrentes, o histórico de interlocução com a equipe de gestão, a concretude dos encaminhamentos da reunião de plano de ação, entre outros. Esse documento deve ser encaminhado por NA ao gestor como documento orientador da Reunião de Plano de Ação, sendo denominado Documento de Apresentação dos Achados a partir do efetivo envio ao gestor. O envio indicará o prazo de ATÉ 5 (cinco) dias úteis para apresentação de Plano de ação (ações, responsáveis e prazos) pelo gestor, acompanhada de eventuais manifestações adicionais, caso necessário. Vale destacar que o Documento de Apresentação dos Achados pode ser entendido como uma NA consolidadora expedida na fase de encerramento ou o conjunto de NAs encaminhadas ao longo da fase de execução da auditoria, sendo recomendável a adoção desse último modelo para que as equipes de gestão possuam mais tempo para prontamente adotar providências saneadoras. A equipe pode optar com incluir um item de NA, definindo o prazo de resposta e apresentando o detalhamento como documento anexo, ou em apresentar um item de NA para cada achado, de modo que o gestor possa se manifestar expressamente sobre cada um deles e a equipe registrar a aceitação de cada item individualmente.

3.3.1.10 Realizar Reunião de Plano de Ação (busca conjunta de soluções), com base no Documento de Apresentação dos Achados, para discutir e alinhar ações propostas pelos gestores e recomendações propostas pelos auditores, responsáveis e prazos, combinando a devolutiva final por meio de Nota de Auditoria no Sisaudit.

A Reunião de Plano de Ação deve ser realizada com base no Documento de Apresentação dos Achados encaminhado (NA consolidadora ou conjunto de NAs), sempre com foco na discussão do Plano de Ação (recomendações, responsáveis e prazos). No entanto, caso o gestor entenda que existe equívoco na interpretação apresentada pela Audin, deve ser oportunizada manifestação adicional, a ser registrada como resposta ao item de NA correspondente.

3.3.1.11 Para cada Achado, revisar a proposta de Recomendação, prazo e responsável, de acordo com o pactuado na Reunião de Plano de Ação, revisando a Probabilidade e Impacto e submetendo a nova aprovação pelo Supervisor

Encerrado o ciclo de discussão do Plano de Ação com os gestores responsáveis, devem ser revisadas no Sisaudit as propostas de recomendações, responsáveis e prazos no Sisaudit e novamente submetidos os Achados (acompanhados do Plano de Ação) para aprovação pelo Supervisor.

3.3.1.12 No Redmine, preencher os campos complementares de Causas, Consequências, Processo impactado, Risco Archer, Controles, Pendência atual, Risco identificado, Responsável, Corresponsáveis, Email gestor. Riscos que forem considerados inaceitáveis (fora do apetite) ao Serpro devem ser reportados ao Supervisor

O Redmine espelha os Achados e Planos de Ação (recomendações, responsáveis e prazos) aprovados no Sisaudit, estruturando campos complementares que serão aproveitados no processo de Escalada de Recomendações e Reportes de Riscos.

3.3.1.13 No Redmine, se houve alteração, atualizar a cobertura planejada de Objetivos, Metas, Riscos, Controles e Processos, incluindo e excluindo os relacionamentos adequados na tarefa de Auditoria correspondente, visando manter atualizado o Mapa de Cobertura do PAINT

Nessa etapa de encerramento, avaliar se realmente a cobertura planejada foi executada. Caso contrário, atualizar as tarefas relacionadas para manter atualizado o Mapa de Cobertura do PAINT.

3.3.1.14 Validação dos Achados e seus detalhamentos pelo Supervisor, em alinhamento ao mérito discutido e alinhado na Reunião de Plano de Ação. Na validação dos Achados, o Supervisor confirmará se: estão devidamente suportados por evidências e são convincentes, são relevantes para os objetivos dos trabalhos, apresentam condição, critérios, causas e consequências, adotando comunicação clara, completa, concisa, construtiva, positiva, objetiva, precisa e tempestiva

Essa é uma etapa central da revisão de qualidade dos Achados pelo Supervisor, aproveitando o mérito debatidos com os gestores na Reunião de Plano de Ação. Os conceitos estão definidos no MOT e são transcritos a seguir:

a) ser relevante para os objetivos dos trabalhos de auditoria;

- aqueles achados não considerados suficientemente relevantes para compor o relatório final devem ser comunicados à Unidade Auditada por meio de outros instrumentos, como a nota de auditoria, por exemplo. Se esses achados não forem capazes de auxiliar no aprimoramento da gestão ou de evitar casos semelhantes no futuro, poderão ser mantidos apenas como papéis de trabalho;
- quando a equipe identificar, no decorrer do trabalho, situações relevantes que não estejam relacionadas aos objetivos definidos na etapa de planejamento, deverá apresentá-las ao supervisor para que ele defina a abordagem a ser adotada. Entre as possíveis alternativas de tratamento, incluem-se, a depender da criticidade, da materialidade e da relevância da situação encontrada, o registro nos papéis de trabalho ou a programação de uma nova auditoria. Nesse último caso, é necessária a aprovação da inclusão no Plano de Auditoria Interna.

b) estar devidamente fundamentado em evidências, as quais devem ser capazes de demonstrar que a situação registrada realmente existe ou existiu;

c) mostrar-se convincente, ou seja, ser consistente em cada um de seus componentes (enunciados na seção 5.4.2), de forma que mesmo um terceiro (prudente e informado) que não tenha participado da auditoria o compreenda e o aceite.

O desenvolvimento dos achados de auditoria deve contemplar quatro componentes principais, quais sejam: critério, condição, causa e efeito.

- Critério (o que deveria ser): É o padrão utilizado para avaliar se o objeto auditado atende, excede ou está aquém do desempenho esperado. É definido na fase de planejamento do trabalho, conforme especificado na seção 4.3.3 deste Manual.
- Condição ou Situação Encontrada (o que é): Situação existente, identificada e documentada durante a fase de execução da auditoria. Pode ser evidenciada de diversas formas, dependendo das técnicas de auditoria empregadas.
- Causa: É a razão para a existência de diferença entre critério e condição, ou seja, entre a situação esperada e a encontrada. Explica porque a situação encontrada existe, esclarecendo o que permite que ela se configure da forma como está. Sendo assim, é imprescindível que a equipe de auditoria se empenhe em descobrir a causa raiz, ou seja, a causa primeira, mais profunda e mais importante

da condição. Para tanto, é necessário levantar hipóteses sobre quais fontes poderão acarretar as situações encontradas. O Quadro 4, da seção 4.3.2.1.1, pode auxiliar também nesse processo. A determinação da causa raiz pode ser complexa. Em alguns casos, vários fatores, com diferentes graus de influência, podem se combinar para formar a causa raiz de uma situação encontrada, ou a causa raiz pode estar relacionada a uma questão mais ampla, como a cultura organizacional. Sendo assim, é possível que sejam identificadas apenas causas intermediárias para algumas situações. Importante ressaltar que, preferencialmente, a recomendação emitida ao final do trabalho deve estar diretamente relacionada à causa raiz. Quando se atua na causa raiz, é possível eliminar ou reduzir a probabilidade de reincidência da situação negativa encontrada e contribuir mais diretamente para o aprimoramento da gestão.

- Consequências (Efeitos): É a consequência da divergência entre a condição e o critério. Pode ser positivo, correspondendo a benefícios alcançados, ou negativo, correspondendo ao risco ou exposição que sofre o objeto de auditoria ou a Unidade Auditada por não estar conforme o padrão esperado. Trata-se do impacto da diferença entre o referencial utilizado pelo auditor (critério) e a situação real encontrada durante a auditoria (condição). O efeito pode ser existente, quando já se trata de um fato resultante da condição, ou potencial (risco), quando há exposição, sem que tenha sido detectado efeito real. O exemplo mais comum de efeito é o prejuízo ao erário.

Como a comunicação ocorre durante todo o trabalho de auditoria, essas características, descritas a seguir, devem ser observadas em todas as etapas, desde o planejamento, até o monitoramento.

- Claras: comunicações claras são aquelas que facilmente são compreendidas pelo público-alvo. Para isso, devem ser lógicas e fornecer todas as informações significativas e relevantes. Devem usar linguagem consistente com a usada na organização e equilibrada: nem excessivamente simplista, nem excessivamente técnica. A clareza é uma característica da abordagem sistemática e disciplinada de auditoria interna.
- Completas: para garantir a integridade das comunicações, é útil que a equipe considere toda informação essencial para o público-alvo, ou seja, todas as informações significativas e relevantes que apoiem conclusões e recomendações. As comunicações escritas completas geralmente permitem que o leitor chegue à mesma conclusão a que os auditores chegaram.
- Concisas: as comunicações concisas evitam a elaboração desnecessária, detalhes supérfluos, redundância, prolixidade e informações dispensáveis, insignificantes ou não relacionadas ao trabalho.
- Construtivas: as comunicações construtivas são úteis para os destinatários do trabalho de auditoria e para a organização e conduzem a melhorias onde seja necessário. Favorecem um processo colaborativo para elaborar soluções para os problemas encontrados e, consequentemente, para ajudar a organização a atingir seus objetivos. O tom construtivo ao longo das comunicações reflete a seriedade dos achados. Os principais achados podem ser resumidos de forma positiva (foco no aprimoramento) ou de forma negativa (foco em deficiências). A UAIG pode mostrar a tendência (positiva ou negativa) em comparação com auditorias anteriores da mesma atividade.
- Objetivas: as comunicações objetivas são justas, imparciais, neutras, livres de influência indevida. São o resultado de uma avaliação acurada e equilibrada de todos os fatos e circunstâncias relevantes. Para garantir a objetividade nas comunicações, os auditores internos devem usar frases imparciais, sem duplo sentido, e manter o foco nas questões relevantes. A objetividade começa com

a atitude mental imparcial que os auditores internos devem possuir ao realizar os trabalhos. Mais do que um atributo, a objetividade é fundamental para a prática da atividade de Auditoria Interna Governamental.

- Precisas: as comunicações precisas são livres de erros e distorções e são fiéis aos fatos e evidências que lhes dão suporte. Além disso, devem conter todos os fatos relevantes que, se não forem divulgados, podem distorcer a informação. Por esse motivo, se ocorrer um erro nas comunicações, a UAIG deve comunicar imediatamente as informações corrigidas aos destinatários que tiveram acesso à versão anterior.
- Tempestivas: as comunicações tempestivas possibilitam que a organização tome as medidas adequadas no tempo correto. Para alcançar esse requisito, é importante que a UAIG apresente todas as comunicações nos prazos estabelecidos durante a fase de planejamento do trabalho. Como a oportunidade pode ser diferente para cada organização, a fim de determinar o que é oportuno, os auditores internos podem fazer pesquisas relativas ao assunto do trabalho em unidades semelhantes à auditada. Além disso, para estimular o atendimento a esse requisito, o responsável pela UAIG pode estabelecer indicadores de desempenho que meçam a pontualidade na apresentação dos resultados.

3.3.1.15 Validação do Plano de Ação (recomendações, prazos e responsáveis) e seus detalhamentos pelo Supervisor, em alinhamento ao mérito discutido e alinhado na Reunião de Plano de Ação. Na validação das Recomendações, o Supervisor confirmará se: são monitoráveis, viáveis, voltadas a resultados e podem gerar benefícios relevantes de GRC, atuam na causa raiz, nas causas intermediárias ou nas consequências, consideram alternativas, visões prospectivas e possuem boa relação custo-benefício, estão direcionadas aos responsáveis corretos nos prazos acordados. Devem adotar comunicação clara, completa, concisa, construtiva, positiva, objetiva, precisa e tempestiva

Aplicam-se às recomendações do Plano de Ação as diretrizes do item anterior, voltado aos Achados de auditoria, acrescidas dos seguintes atributos de qualidade previstos no MOT aplicáveis às recomendações:

a) monitorável: a recomendação deve ser passível de monitoramento, permitindo verificar se o que se pretendia com a recomendação foi alcançado. Para tanto, é importante que seja prevista a forma por meio da qual será aferido o desempenho das ações a serem implementadas e quais evidências serão apresentadas pela Unidade Auditada ou levantadas pela UAIG para medir a efetiva implementação. É essencial que a recomendação possa ser acompanhada e que sua efetividade possa ser medida posteriormente por meio de seus custos de implementação e benefícios à gestão proporcionados;
b) atuar (preferencialmente) na causa raiz: a recomendação deve se propor a atuar diretamente na causa identificada. Quando se atua na causa raiz, a eficácia da recomendação é maior, posto que terá um efeito preventivo, evitando que a situação se repita no futuro. Quando se atua em causas intermediárias, que são desdobramentos da causa raiz, corre-se o risco de apenas corrigir a situação pontual, não impedindo que ela se repita novamente; As recomendações podem focar na causa, na condição, na consequência e eventualmente até no critério. É fortemente recomendado que haja atenção especial ao tratamento da causa do problema identificado, tendo em vista que a correção da situação encontrada, por si só, não elide a causa do problema. Quando se atua na causa raiz ou na causa mais próxima possível dela, é possível eliminar ou reduzir, consideravelmente, a

probabilidade de reincidência da situação negativa encontrada, contribuindo para o aprimoramento da gestão.

c) viável: é preciso levar em conta restrições de ordem legal, financeira, de pessoal e outras que possam afetar a implementação de medidas propostas pelos auditores. Nesse sentido, a discussão de soluções junto à Unidade Auditada é de suma importância para compreensão do que é e do que não é possível fazer. Além disso, a equipe deve considerar o tempo razoável para a implementação das medidas a serem adotadas pelo gestor, pactuando prazo compatível;
d) apresentar uma boa relação custo-benefício: a equipe de auditoria e o supervisor do trabalho devem avaliar os custos e os benefícios esperados de cada recomendação. Recomendar controle via sistema informatizado, por exemplo, pode representar um custo alto demais para uma determinada operação, mas ser totalmente viável em outra área de negócio. Na medida do possível, deve-se minimizar o gasto de recursos, em atendimento ao princípio da economicidade;
e) considerar alternativas: é importante que a equipe de auditoria e o supervisor do trabalho levantem alternativas e que também analisem aquelas propostas pela Unidade Auditada quando houver a discussão das recomendações. Existem situações em que há várias opções de soluções a serem adotadas, podendo-se optar por aquela que apresente melhor relação custo-benefício, por exemplo;
f) ser direcionada: a recomendação deve ser direcionada para o agente que tem responsabilidade e alçada para colocá-la em prática. A efetividade se perde se a recomendação for direcionada ao agente errado ou se não estiver claro quem deve implementá-la;
g) ser direta: a recomendação deve estar claramente identificada no texto do relatório (ou outra forma de comunicação) como sendo uma recomendação. Não pode haver dúvida sobre seu conteúdo e sobre a necessidade de atendê-la. Por isso, é necessária uma linguagem direta, sem termos vagos que possam dar a impressão de que não se trata de recomendação;
h) especificidade: no âmbito do achado de auditoria ao qual se relaciona, a recomendação deve tratar das medidas a serem tomadas, dos resultados a serem alcançados, não se atendo, via de regra, à forma como será implementada. Também não deve reproduzir exaustivamente a causa identificada, ou repetir a descrição da condição encontrada, por exemplo;
i) significância: essa característica deriva da própria relevância do achado. É importante apontar situações relevantes dentro do escopo da auditoria, assim como recomendar aquilo que pode fazer diferença na gestão, seja melhorando a governança, o gerenciamento de riscos ou a estrutura de controles existente;
j) ser positiva: discorrer sobre as medidas a serem tomadas em tom positivo, com frases afirmativas em vez de negativas, tende a facilitar o convencimento da alta administração e a consequente implementação da recomendação.

3.3.1.16 Como boa prática e suporte à validação do Plano de Ação (recomendações, prazos e responsáveis), o Supervisor verificará se estão claros os requisitos 5W2H: O Quê, Porque, Onde, Quando, Quem, Como, Por quanto. Por fim, registrará a validação dos Achados e do Plano de Ação (recomendações, prazos e responsáveis) por meio da aprovação dos Achados (e Recomendações associadas) no Sisaudit

Como boa prática, o Supervisor avaliará a qualidade do Plano de Ação (recomendações, prazos e responsáveis) considerando a clareza do atendimento dos requisitos do 5W2H, conforme item 3.3.1.1.6. O

resultado dessa avaliação ficará registrado no Sisaudit com a aprovação dos Achados e do Plano de Ação pelo Supervisor do trabalho.

3.3.1.17 Na aba 'Relatório de Auditoria' no Sisaudit gerar novo Quadro de Achados (agora Plano de Ação), que passa a representar o Plano de Ação (recomendações, responsáveis e prazos) aprovado após Reunião de Plano de Ação (busca conjunta de soluções). Os Achados de Auditoria devem estar ordenados por nível de risco no Plano de Ação

Aprovado os Achados e o Plano de Ação pelo Supervisor, deve ser atualizado o artefato antes utilizado para a Reunião de Plano de Ação, que será incorporado como anexo específico do Relatório de Auditoria.

3.3.1.18 Na(s) Nota(s) de Auditoria (Documento de Apresentação dos Achados), reabrir itens considerados não atendidos e sejam possivelmente saneáveis, informando a Data prevista para encerramento do recebimento de informações para o Relatório, o Plano de Ação associado (recomendação, responsável e prazo) destacando que as ações concluídas e com implementação verificada pela Audin nesse Prazo estarão dispensadas do monitoramento por meio de Recomendação (ou receberão monitoramento expedito, dependendo da complexidade da verificação)

Essa etapa visa conceder os gestores o prazo de encerramento do Relatório para a solução de questões pontuais que forem consideradas saneáveis nesse prazo. Caso efetivamente resolvido, será mantido o registro com a aceitação do item de NA em reaberto e feito o registro sumário em Relatório do atendimento durante a execução do trabalho. Caso a verificação do atendimento seja mais complexa e não possa ser realizada na etapa de encerramento sem comprometer o prazo, a equipe pode manter a recomendação, expedir o relatório e realizar verificação expedita quanto ao atendimento logo na sequência, no âmbito do monitoramento do Plano de Ação (recomendação).

3.3.1.19 Equipe de auditoria registrar a aceitação do Plano de Ação em ATÉ 5 (cinco) dias úteis, recebendo as respostas aos itens da Nota de Auditoria e alterando o Status para 'Concluída'

Recebida a resposta dos gestores (proposta de Plano de Ação) para as NAs, a equipe tem o prazo de ATÉ 5 (cinco) dias úteis para aceitar as respostas no Sisaudit, o que altera o Status dos itens de NA para ‘Concluída’.

3.3.1.20 Na aba 'Cronograma', informar a 'Data fim realizado' da tarefa do Documento de Apresentação dos Achados, alterando a Situação para 'Concluída'. Concluída a fase de Planejamento no Cronograma, o Status da auditoria deve ser alterado para 'Em execução'

Para fins de monitoramento da produtividade, deve ser informado na aba ‘Cronograma’ a ‘Data fim realizado’ da tarefa do Documento de Apresentação dos Achados.

3.3.2 Elaborar Relatório de Auditoria

Elaboração do Relatório de Auditoria e respectivos anexos para comunicação do resultado dos exames, acompanhados da revisão de qualidade. *Feedback* para a equipe de resultados e de competências, com foco em desenvolvimento profissional contínuo.

3.3.2.1 Na aba 'Cronograma', informar a 'Data início realizado' da tarefa do Relatório de Auditoria, alterando Situação para 'Em andamento'

Para fins de monitoramento da produtividade, deve ser informado na aba 'Cronograma' a 'Data início realizado' da tarefa do Relatório de Auditoria.

3.3.2.2 Planejar a relatoria com base no Modelo de Relatório, incluindo ao menos as seções Sumário Executivo (Objetivo, Escopo, Achado, Plano de Ação, Nível de Risco, Processo Avaliado, Score RRC/RCSA), Conclusão (incluindo Objetivos, Riscos e Controles avaliados), Resultado dos Exames, Avaliação do Sistema de Controles Internos, Contexto e Metodologia, anexos de Detalhamento dos Achados e de Base de Classificação do Nível de Risco

Essas seções do Relatório já constam do modelo disponibilizado na página da Audin (link), bastando segui-lo.

3.3.2.3 Adaptar a forma de comunicação, destacando os pontos de maior nível de risco e as conclusões (respostas a Questões de Auditoria) no Sumário Executivo (Highlight) em liguagem direta, clara a objetiva, detalhando no corpo do Relatório os elementos de suporte às conclusões. Incluir ou excluir seções ou tópicos, conforme necessário, a exemplo de Boas Práticas Identificadas, Não-Escopo, Delimitação da Opinião, Negativa de Opinião

O modelo de estrutura de Relatório de Auditoria deve ser entendido como base, mas não como imutável, podendo a equipe partir dele e complementar com seções consideradas relevantes para boa compreensão do trabalho realizado, assim como exclusão de seções consideradas desnecessárias naquele trabalho específico, em especial nos relatórios de consultoria. A depender do trabalho realizado, pode ser relevante destacar uma seção de Boas Práticas identificadas, de Não-Escopo para explicitar o que não foi analisado pela equipe, de Delimitação da Opinião para esclarecer o alcance das conclusões apresentadas ou de Negativa de Opinião nos casos em que a equipe não obteve acesso a informações necessárias e suficientes para a formação de opinião.

3.3.2.4 Indicar o campo próprio do Modelo de Relatório a Lista de Distribuição: para Ação, para Informação, para Acompanhamento (2ª linhas e, se couber, Instâncias de Integridade)

A Lista de Distribuição registrada no Relatório orientará os destinatários do Memorando de encaminhamento do trabalho. De regra, os Relatórios devem ser encaminhados para acompanhamento pela SUPCR (ou outras unidades com atribuição de supervisão, a exemplo da SUPSI e SUPPD) e, se couber, instâncias de integridade (em especial quanto às análises envolvendo riscos à integridade).

3.3.2.5 Os Achados de Auditoria devem ser comunicados por ordem do nível de risco (probabilidade e impacto) no anexo próprio (Detalhamento do Achados), explicitando situação encontrada (condição), causas, consequências e critério de auditoria, acompanhados do Plano de Ação (recomendações, prazos e responsáveis)

Os Achados de Auditoria devem ser apresentados, tanto no Sumário Executivo quanto no Anexo de Detalhamento dos Achados, iniciando do maior nível de risco ao menor nível de risco, cabendo registrar a possibilidade de que situações de menor relevância (nível de risco muito baixo) podem ser encaminhadas aos gestores por meio de Nota de Auditoria, sem necessidade de maiores detalhamentos em Relatório.

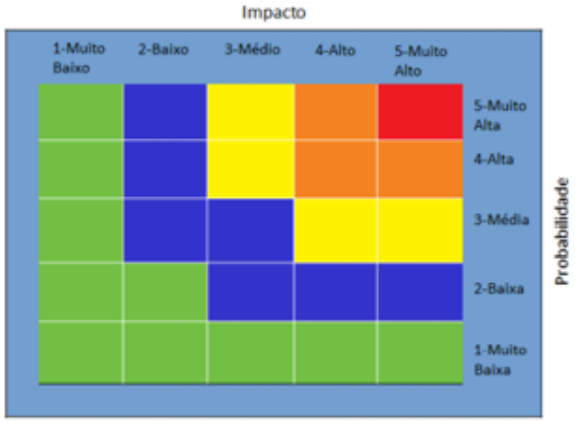
3.3.2.6 A base para classificação do nível de risco dos Achados de Auditoria, seguindo a Metodologia corporativa, deve ser apresentada em anexo próprio, conforme previsto no Modelo de Relatório

A base para classificação do nível de risco (probabilidade x impacto) dos Achados já consta de anexo do modelo disponibilizado na página da Audin (link), adotando a Metodologia de Gestão de Riscos do Serpro.

IMPACTO	DIMENSÃO
MUITO ALTA	**Esforço de Gestão** - Evento com potencial para levar o negócio ou serviço ao colapso. **Regulação** - Determina interrupção das atividades. **Reputação** - Com destaque em mídia nacional e internacional, podendo afetar a missão. **Negócio/Serviços à Sociedade** - Prejudica o alcance da missão do Serpro. **Financeiro** - Pode gerar impacto orçamentário ou financeiro que compromete a continuidade da empresa. **Intervenção Hierárquica** - Presidente/Diretoria Executiva ou Conselhos. **Privacidade e Proteção de Dados** - Os titulares podem encontrar consequências significativas, ou mesmo irreversíveis, que não podem superar.
ALTO	**Esforço de Gestão** - Evento crítico, mas que com a devida gestão pode ser suportado. **Regulação** - Determina ações de caráter pecuniário (multas). **Reputação** - Com algum destaque em mídia nacional, provocando exposição significativa e podendo afetar aos Objetivos Estratégicos. **Negócio/Serviços à Sociedade** - Prejudica o alcance da missão da Unidade e dos Objetivos Estratégicos. **Financeiro** - Pode gerar impacto orçamentário ou financeiro grande. **Intervenção Hierárquica** - Diretoria/superintendente/Gestor de Domínio. **Privacidade e Proteção de Dados** - Os titulares podem encontrar consequências significativas, que convém que sejam capazes de superar.
MÉDIO	**Esforço de Gestão** - Evento significativo que pode ser gerenciado em circunstâncias normais. **Regulação** - Determina ações de caráter corretivo. **Reputação** - Pode ter exposição em mídia. **Negócio/Serviços à Sociedade** - Prejudica o alcance dos Objetivos Estratégicos e/ou das metas de processo/ projeto. **Financeiro** - Pode gerar impacto orçamentário ou financeiro moderado. **Intervenção Hierárquica** - Gestor de Domínio/Gestor do Processo/Projeto. **Privacidade e Proteção de Dados** - Os titulares podem encontrar inconvenientes, que eles serão capazes de superar, apesar de algumas dificuldades.
BAIXO	**Esforço de Gestão** - Evento cujas consequências podem ser absorvidas, mas carecem de esforços da gestão para minimizarem o impacto. **Regulação** - Determina ações de caráter orientativo. **Reputação** - Tende a limitar-se às partes envolvidas. **Negócio/Serviços à Sociedade** - Prejudica o alcance das atividades. **Financeiro** - Pode gerar impacto orçamentário ou financeiro pequeno. **Intervenção Hierárquica** - Gestor do Processo/Projeto/Time. **Privacidade e Proteção de Dados** - Os titulares poderão encontrar alguns inconvenientes, os quais serão superados sem nenhum problema.
MUITO BAIXO	**Esforço de Gestão** - Eventos cujas consequências podem ser absorvidas por meio de atividades do Processo. **Regulação** - Pouco ou nenhum impacto. **Reputação** - Impacto apenas interno, não gera cobertura em mídia. **Negócio/Serviços à Sociedade** - Pouco ou nenhum impacto nas metas. **Financeiro** - Pode gerar impacto orçamentário ou financeiro insignificante. **Intervenção Hierárquica** - Gestor do processo/Projeto/Time. **Privacidade e Proteção de Dados** - Os titulares de DP não serão afetados.

PROBABILIDADE	DESCRIÇÃO
MUITO ALTA	Quase Certa. De forma inequívoca, o evento poderá ocorrer mensalmente, pois as circunstâncias indicam claramente essa possibilidade.
ALTA	Muito Provável. De forma até esperada, o evento poderá ocorrer trimestralmente, pois as circunstâncias indicam fortemente essa possibilidade.
MÉDIA	Provável. De alguma forma, o evento poderá ocorrer semestralmente, pois as circunstâncias indicam moderadamente essa possibilidade.
BAIXA	Pouco Provável. De forma inesperada ou casual, o evento poderá ocorrer uma vez ao ano, pois as circunstâncias pouco indicam essa possibilidade.
MUITO BAIXA	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.

Fonte: Metodologia de Gestão de Riscos do Serpro (RI 158/2021).



MATRIZ DE RISCOS - IMPACTO x PROBABILIDADE

Outra forma de apresentar o mapa de calor, utilizando faixas dos níveis de riscos, está apresentada a seguir:

NÍVEL DE RISCO E APETITE	FAIXA INFERIOR	FAIXA SUPERIOR
MUITO ALTO	25	25
ALTO	16	24
MÉDIO	12	15
BAIXO	6	11
MUITO BAIXO	1	5

3.3.2.7 Conforme Modelo de Relatório, marcar todas as páginas do documento como 'Sigiloso (SG 05/2021)', com base no disposto no Regimento Interno da Auditoria Interna

Em atendimento à Norma SG 05/2021, todas as páginas do modelo de Relatório de Auditoria já estão marcadas como 'SIGILOSO', bastando manter as marcações em todas as páginas no documento final. Nesse ponto, vale destacar o disposto no Regimento Interno da Auditoria Interna quanto à janela temporal de sigilo de documentos na Audin, enquanto pendente o atendimento de recomendações ou a edição de ato ou decisão:

> Art. 15, § 3º Os relatórios, opiniões e demais documentos de registro do resultado de auditorias são considerados documentos preparatórios, nos termos do Art. 20 do Decreto 7.724/2012, enquanto pendente o atendimento de recomendações ou a edição de ato ou decisão, sujeitando-se aos regulares procedimentos de classificação, de proteção e de divulgação de informação sigilosa do Serpro e demais hipóteses legais de restrição de acesso, conforme legislação aplicável.

3.3.2.8 O designado Auditor responsável deve concluir o preenchimento da seção 'Comunicação Final dos Resultados do Trabalho' da Avaliação Interna de Qualidade, conforme monitoramento contínuo de qualidade previsto no PGMQ, inclusive confirmando a ausência de ameaças, de fato ou veladas, e a manutenção da independência e da objetividade da opinião da equipe na Relatoria do trabalho

Deve ser concluído o preenchimento do Formulário de Avaliação Interna de Qualidade e enviada a resposta, gerando o arquivo em formato PDF e subindo no Sisaudit como papel de trabalho da auditoria e do monitoramento contínuo do PGMQ.

3.3.2.9 Validação do Relatório de Auditoria e seus anexos pelo Supervisor, em alinhamento ao mérito discutido e alinhado com a equipe e na Reunião de Plano de Ação. Na validação do Relatório, o Supervisor confirmará se: está devidamente suportado por evidências convincentes, adota comunicação clara, completa, concisa, construtiva, positiva, objetiva, precisa e tempestiva, achados são relevantes para os objetivos dos trabalhos, apresentam condição, critérios, causas e consequências

Essa etapa final de revisão pelo Supervisor reflete o conjunto de verificações de qualidade realizadas ao longo do processo de auditoria, retomando atributos citados da qualidade da comunicação de modo geral. Segundo a Estrutura Global de Competências do The IIA, o Gerente supervisor deve ser um especialista em customizar a informação conforme o público a que se destina: mais objetiva, abrindo mão de detalhes técnicos, mais gerencial, mais volta às operações, mais focada em riscos e controles. O Supervisor deve auxiliar a equipe a estruturar a informação entre as diferentes seções do Relatório para comunicar de modo eficaz com os diferentes públicos a que se destina.

3.3.2.10 Revisão do Relatório de Auditoria e seus anexos pelo gerente par

Diante de todo o acompanhamento realizado pelo gerente par ao longo do trabalho, o Relatório de Auditoria e seus anexos devem receber avaliação expedita, focando a consistência geral, boas práticas e atributos de qualidade citados no presente Manual, em especial quanto à clareza da comunicação para terceiros que não participaram diretamente do trabalho e não possuem maiores detalhamentos sobre os processos operacionais.

3.3.2.11 Na aba 'Cronograma', informar a 'Data fim realizado' da tarefa do Relatório de Auditoria, alterando a Situação para 'Concluída'.

Para fins de monitoramento da produtividade, encerrados os ajustes após a revisão pelo gerente par, a equipe deve informar na aba ‘Cronograma’ a ‘Data fim realizado’ da tarefa do ‘Relatório de Auditoria’.

3.3.2.12 Concluir todos os procedimentos do 'Programa de Auditoria' e todas as ações do 'Cronograma' para alterar o Status da Auditoria para 'Em encerramento'

A partir do momento em que todas as ações do Cronograma têm a ‘Data fim realizado’ informada, o Status da Auditoria é automaticamente alterado para ‘Em encerramento’, refletindo os estágios finais de homologação e assinatura do Relatório do sistema.

3.3.2.13 Na aba 'Relatório de Auditoria' subir a versão final assinada do Relatório de Auditoria (contendo Declaração de Objetividade, Independência e Conformidade com o Código de Ética do IIA e do Serpro), Resumo do Relatório de Auditoria e Quadro de Achados, procedendo com as assinaturas no Sisaudit pelos auditores, auditor responsável, supervisor, chefe de seção e submetendo para validação e assinatura pelo titular da Auditoria Interna

Consta do próprio Modelo de Relatório de Auditoria o parágrafo padrão com a referida Declaração. O Sisaudit possui campos específicos na aba 'Relatório de Auditoria' para ser subido o próprio Relatório, seu Resumo (Sumário Executivo) e o Quadro de Achados.
Subidos os referidos arquivos deve ser realizada a assinatura no Sisaudit por pelo menos um membro da equipe (ou auditor responsável), pelo Supervisor (nos perfis de supervisor e chefe de seção) e pelo titular da Auditoria Interna, que deve validar a versão final dos documentos.

3.3.2.14 Elaborar minuta de Despacho no Memorando de abertura do trabalho, considerando a lista de distribuição registrada no Relatório, juntando Relatório e Respectivos anexos para envio formal aos gestores e demais partes interessadas (incluindo 2ª linhas e, se couber, Instâncias de Integridade).

O modelo de Despacho no Memorando encaminhando o Relatório e anexos aos gestores e demais partes interessadas consta da página da Audin (link).

3.3.2.15 Informar à equipe de assessoramento da Audin a relação de gestores sugeridos para receber a formulário de Feedback para a Auditoria Interna, incluindo da Lista de Distribuição.

A relação de e-mails dos gestores sugeridos para receber o formulário de *Feedback* para a Auditoria Interna deve enfocar interlocutores que estiveram mais diretamente envolvidos no trabalho e ser encaminhada para a equipe de assessoramento da Audin, que encaminhará os convites por e-mail, devendo incluir representantes das unidades de constam da Lista de Distribuição registrada no Relatório.

3.3.2.16 Supervisor realizar avaliação do desempenho da equipe de auditores, registrando no GDES a avaliação de resultados e no formulário 'Guia de Competências - Estrutura Global IIA' a avaliação de competências (conectadas às competências do GDES).

Ao final do trabalho de auditoria, enfocando o desenvolvimento profissional contínuo, o Supervisor dever realizar a avaliação individual do desempenho de cada auditor da equipe, registrando no GDES a avaliação de resultados e no formulário 'Guia de Competências - Estrutura Global IIA' (link) a avaliação de competências (conectadas às competências do GDES).

3.3.2.17 Titular da Auditoria Interna verificar a consistência e validar os documentos finais por meio da assinatura no Sisaudit, alterando o Status da auditoria para 'Concluída' e liberando o Plano de Ação (recomendações, prazos e responsáveis) para os gestores, iniciando a fase de monitoramento (follow-up).

A etapa final para encerramento do trabalho no Sisaudit consiste na assinatura pelo titular da Auditoria Interna, o que registra a validação dos documentos finais e resulta na liberação do Plano de Ação (recomendações, prazos e responsáveis) para os gestores, iniciando a fase de monitoramento (follow-up). Essa tarefa deve ser '#Atribuído para' o Supervisor ou o Auditor responsável, aquele que ficar responsável por interagir com o titular da Auditoria Interna para a assinatura.

3.3.2.18 Titular da Auditoria Interna encaminhar Relatório final e respectivos anexos por meio de Despacho no Memorando de abertura do trabalho, para os destinatários na lista de distribuição, destacando o Plano de Ação (recomendações, responsáveis e prazos), orientando sobre o recebimento da recomendação no sistema, comunicando sobre a lógica de escalada por decurso de prazo e de anuência do superior para prorrogação. Havendo retificação do Relatório, deve ser enviado aos mesmos destinatários do primeiro.

Validada a versão final dos documentos, o titular da Auditoria Interna deve encaminhá-los aos destinatários na lista de distribuição (incluindo o Diretor e o Superintendente responsável) por meio de Despacho no Memorando de abertura do trabalho, destacando o Plano de Ação (recomendações, responsáveis e prazos). Constam do modelo de Despacho as orientações sobre o recebimento da recomendação no Sisaudit, a escalada por decurso de prazo e de anuência do superior para prorrogação. Cumpre registrar que, se houver retificação do texto do Relatório, a nova versão deve ser encaminhada aos mesmos destinatários em novo Despacho retificador.

3.4 Monitoramento

Na fase de monitoramento são verificadas as ações de cumprimento e atendimento às Recomendações e seu Plano de Ação. O Plano Anual da Auditoria Interna prevê para cada trabalho planejado o quantitativo de horas para monitoramento. Porém, esta atividade deve ser realizada de maneira dinâmica e contínua para garantir a efetividade do trabalho realizado. A etapa de monitoramento ocorre no Sisaudit por meio do módulo de acompanhamento. Todas as etapas do processo são registradas no sistema, mantendo o armazenamento dos documentos também no referido sistema. Para avaliar a resposta da unidade auditada às recomendações emitidas, podem ser adotadas as estratégias abaixo ou estratégias que se mostrem convenientes e adequadas para a auditoria:

a) periodicamente, trimestralmente, verificar a situação de todas as recomendações que estejam pendentes de atendimento;
b) realizar trabalhos de avaliação com o objetivo de validar providências implementadas pela administração e avaliar a qualidade das ações corretivas implementadas;
c) proceder ao acompanhamento de recomendações pendentes no decorrer de um outro trabalho de auditoria programado para a mesma área da unidade auditada.

A escolha da estratégia, forma e frequência das ações de monitoramento deve levar em consideração os seguintes critérios:

a) a gravidade dos riscos envolvidos;
b) a complexidade do objeto da recomendação; e
c) o grau de maturidade da gestão de riscos da unidade auditada.

Quanto maior os riscos e a complexidade das medidas a serem implementadas, a auditoria deve aumentar as ações de monitoramento, ou aplicar ações de maior complexidade ou em menor espaço de tempo para verificar o atendimento às recomendações. Para monitorar a implementação de recomendações decorrentes de atividades de consultoria, a equipe de auditoria deve definir durante o planejamento do trabalho, em conjunto com a unidade auditada, se haverá monitoramento e sua forma de realização, devendo ser adequadamente registrado no Documento de Pactuação de Consultoria (DPC) e guardadas as evidências no Sisaudit ou diretório próprio da rede local ou SerproDrive. As recomendações podem ter o status de:

- *Disponível para recepção*: recomendação enviada pela equipe de auditoria e aguardando recepção do auditado;
- *Recepcionada*: recomendação enviada pela equipe de auditoria e recebida pelo auditado;
- *Resposta em elaboração*: recomendação recebida e iniciada a elaboração de resposta;
- *Resposta elaborada*: resposta da recomendação concluída;
- *Em análise pela chefia da unidade*: resposta encaminhada para análise e validação da chefia responsável pela unidade auditada;
- *Em análise pelo componente externo*: área cujo responsável não pertence à base da estrutura hierárquica do Serpro;
- *Em análise pela Auditoria*: recomendação respondida pela unidade auditada e em análise pela equipe de auditoria interna;
- *Comentário elaborado pelo auditor*: o auditor competente após análise da recomendação, redigiu comentários à resposta elaborada pela auditada;
- *Em análise pelo(a) coordenador(a) de Auditoria da Auditoria*: resposta analisada pelo auditor competente e encaminhada para sua chefia imediata para validação e supervisão;
- *Em análise pela chefia da Auditoria*: aguardando validação quanto a análise efetuada pela auditoria interna;
- *Concluída*: recomendação foi implementada e verificado seu completo atendimento;
- *Cancelada*: recomendação cancelada por perda de objeto ou outros motivos especificados.

As alterações no status da recomendação são automaticamente registradas no Sisaudit e devem conter a descrição detalhada do motivo da alteração em campo próprio do Sistema.

3.4.1 Monitoramento de Recomendações reiteradamente não atendidas

Conforme descrito no Regimento Interno da Auditoria Interna: " *Art. 18 O cumprimento das recomendações emitidas pela Auditoria Interna ou pelos órgãos de controle é responsabilidade dos gestores, assegurada a escalada hierárquica quadrimestral, de Superintendentes até Diretor e Diretoria Executiva, dos reportes de riscos decorrentes de recomendações não atendidas, submetendo os de níveis de risco alto ou muito alto para aprovação pelo Conselho de Administração dos encaminhamentos, após ouvido o Comitê de Auditoria".* Desta forma, os auditores e gerentes de departamento devem realizar sistematicamente o acompanhamento das recomendações por meio do Sisaudit, garantindo o efetivo cumprimento de prazos relativos à Auditoria Interna (análise de atendimento, pedidos de prorrogação e demais trâmites previstos no acompanhamento).

O acompanhamento de recomendações pela Auditoria Interna será encerrado mediante o atendimento da recomendação, a perda do objeto, a transferência do monitoramento, a aceitação expressa dos riscos pelo gestor ou a aceitação tácita, quando decorrido 1 (um) ano de expedição da recomendação.

No intuito de viabilizar o envio de Reporte de Riscos aos responsáveis, é importante que todas as recomendações tenham os campos: Risco Archer; Risco identificado; Probabilidade; Impacto; Causas; Consequências e hipóteses de encerramento devidamente preenchidos no Redmine - 2.4. Follow-Up de Recomendações (Monitoramento) - Departamento - recomendações (link).

O efetivo envio de Reporte de Riscos deve ser tratado pelo gerente junto ao titular da Auditoria Interna, tendo em vista suas atribuições de reportar à alta administração exposições a riscos entendidas como

excessivas. Feita a revisão final dos campos, a situação da tarefa deve ser alterada para 'Notificar gestor', visando a efetiva expedição dos Reportes para os e-mails identificados.

3.4.2 Comunicação da situação da implementação das recomendações

Todas as recomendações em acompanhamento pela auditoria interna são relatadas à Diretoria Executiva e Conselhos da empresa, quadrimestralmente. Além disso, é disponibilizado painel gerencial Qlik (link) contendo informações consolidadas e gerenciais sobre recomendações emitidas pela Auditoria Interna.

3.4.3 Quantificação e Registro de Benefícios

A Auditoria Interna deve observar a sistemática de quantificação e registro dos resultados e dos benefícios financeiros e não financeiros decorrentes de suas recomendações proposta pela CGU, permitindo verificar o resultado efetivo de sua atuação. O registro dos benefícios deve ocorrer mediante preenchimento de campos no sistema Redmine (link) na opção: 2.4. *Follow-Up* de Recomendações (Monitoramento) - benefícios. Devem ser informados os benefícios auferidos com a implementação da recomendação após seu encerramento. Após supervisão gerencial, o Gerente encaminha para o Auditor Interno para aprovação. Conforme aprovado pelo Conselho de Administração por meio da ata de 29/01/2019 (link) devem ser atendidas as instâncias de aprovação dos benefícios: *"(...) após validação pelo gestor, as seguintes instâncias de validação para o Serpro: R$ 100 mil a 500 mil (Coordenador de Auditoria), R$ 500 mil a 3 milhões (Auditor-Geral), acima de 3 milhões (Conselho de Administração). O Colegiado aprovou os referidos limites das instâncias de validação".* Desta forma, antes do envio do benefício para aprovação pelo Auditor Interno, avaliar se o benefício já foi aprovado pelo gestor e pelo gerente de departamento, quando for o caso.

4 Gerenciamento da Atividade de Auditoria Interna

4.1 Papéis dos participantes da Auditoria Interna

Na aba "Dados Gerais" de cada trabalho de auditoria no sistema de auditoria – Sisaudit são descritos a relação de participantes e seus respectivos papéis, conforme abaixo:

Participantes

Componente	Nome	Papel
DP/AUDIN/AUDEP	Fernanda de Jesus Mourao	Auditor
DP/AUDIN/AUDEP	Leda Maria Guedes Sotero	Auditor responsável
DP/AUDIN/AUDEP	Nilson Romero Michiles Junior	Supervisor

Auditor: empregado da Auditoria Interna que executa levantamentos, apreciações, análises e procedimentos para o planejamento, execução e relatoria dos trabalhos de auditoria previstos no plano anual de auditoria interna. Suas atividades, em cada trabalho de auditoria, são atribuídas pelo Supervisor diretamente no Sisaudit. O Manual de Orientações Técnicas da CGU (link), no item 3.2, lista as principais atribuições dos Auditores, conforme abaixo:

> a) executar o trabalho de acordo com as normas e práticas de auditoria aplicáveis;
> b) observar as orientações do supervisor e do coordenador de equipe;
> c) em conjunto com o coordenador e o supervisor, elaborar cronograma para o trabalho de auditoria;

d) participar da elaboração do programa de trabalho;
e) executar as atividades de acordo com o planejamento realizado;
f) coletar e analisar informações relevantes e precisas por meio de procedimentos e técnicas de auditoria apropriados;
g) elaborar os documentos de comunicação com a Unidade Auditada e submetê-los à avaliação do coordenador de equipe;
h) assegurar a suficiência e a adequação das evidências de auditoria para apoiar achados, recomendações e conclusões da auditoria;
i) registrar as atividades realizadas em papéis de trabalho, conforme políticas e orientações estabelecidas pela UAIG;
j) manter a confidencialidade e a segurança de informações, dados, documentos e registros;
k) comunicar quaisquer achados críticos ou potencialmente significativos ao coordenador ou ao supervisor do trabalho em tempo hábil;
l) quando houver limitação do trabalho, comunicar o fato, de imediato, ao coordenador ou ao supervisor do trabalho.

Auditor responsável: empregado da Auditoria Interna designado pelo Supervisor diretamente no sistema de auditoria – Sisaudit.

O Manual de Orientações Técnicas da CGU (link), no item 3.2, lista as principais atribuições do Coordenador de Equipe, que aqui assemelha-se ao Auditor responsável, conforme abaixo:

a) auxiliar na elaboração do cronograma de atividades e zelar pelo seu cumprimento;
b) liderar a execução do trabalho, de forma a garantir o cumprimento do planejamento;
c) participar da elaboração do programa de trabalho e, quando necessário, apresentar sugestões de alterações do planejamento ao supervisor;
d) manter interlocução com a Unidade Auditada e atender aos seus servidores/funcionários e dirigentes, sobretudo para esclarecer o conteúdo de documentos emitidos durante o trabalho de auditoria;
e) assegurar-se de que os documentos de comunicação da UAIG com a Unidade Auditada atendam aos parâmetros contidos neste documento e nos demais normativos aplicáveis;
f) acompanhar os integrantes da equipe de auditoria na aplicação de testes que demandem interação com os gestores ou servidores/funcionários da Unidade Auditada, tais como entrevistas ou aplicações de questionários;
g) solicitar a intervenção do supervisor sempre que esta seja necessária para assegurar o cumprimento das normas, das orientações, a segurança da equipe e a solução de eventuais Conflitos.

Supervisor – papel exercido pelos Gerentes de Departamento.

O Manual de Orientações Técnicas da CGU (link), no item 3.2, lista as principais atribuições do Supervisor conforme abaixo:

a) definir a equipe de auditoria, de forma a garantir a proficiência coletiva;
b) indicar o coordenador de equipe;

c) garantir que a auditoria seja realizada de acordo com as normas e práticas de auditoria aplicáveis;
d) interagir com a equipe e instruí-la, durante todo o trabalho de auditoria, inclusive na fase de planejamento, promovendo oportunidades de desenvolvimento dos auditores;
e) em conjunto com a equipe e o coordenador, elaborar cronograma para o trabalho de auditoria e zelar pelo seu cumprimento;
f) conduzir a elaboração do programa de trabalho, promovendo a participação e a interação da equipe de auditoria;
g) aprovar o programa de trabalho e autorizar eventuais alterações;
h) garantir o cumprimento do programa de trabalho e o alcance dos objetivos;
i) confirmar se as evidências suportam os achados, as conclusões e as recomendações elaboradas pela equipe;
j) revisar os papéis de trabalho e certificar-se de que foram devidamente elaborados e de que sustentam os achados e as conclusões alcançadas pela equipe;
k) assegurar a qualidade dos produtos e das comunicações e, se necessário, solicitar aos auditores evidências adicionais ou esclarecimentos;
l) sempre que possível, conduzir as reuniões de abertura e as que tenham como finalidade discutir os achados e as possíveis soluções com os representantes da Unidade Auditada;
m) manter a confidencialidade e a segurança de informações, dados, documentos e registros;
n) garantir que haja evidências da realização do trabalho de supervisão.

Nos procedimentos descritos neste Manual referente ao subprocesso Realizar Auditoria, consta também o detalhamento dos papéis dos participantes dos trabalhos de auditoria.

Conforme descrito no Documento de Atribuições e Competências - DAC/Audin e Regimento Interno da Auditoria Interna:

"São responsabilidades do titular da Auditoria Interna, além das já citadas nesse Regimento Interno e nos elementos obrigatórios da IPPF:

- disponibilizar ao Conselho de Administração, ao Comitê de Auditoria, ao Conselho Fiscal e à Diretoria Executiva os relatórios contendo as informações sobre as ações dos órgãos de controle, da Auditoria Interna e dos órgãos reguladores;

- disponibilizar ao Conselho de Administração, ao Conselho Fiscal e à Diretoria Executiva os relatórios das ações para atendimento das não conformidades, ocorrências, recomendações ou determinações dos órgãos de controle, da Auditoria Interna e dos órgãos reguladores;

- acompanhar o andamento dos processos junto ao Tribunal de Contas da União – TCU;

- coordenar e orientar a elaboração do Plano Anual de Auditoria Interna (PAINT), do Relatório Anual de Atividades da Auditoria Interna (RAINT), do Regimento Interno da Auditoria Interna, da estratégia da atividade de auditoria interna e de pareceres;

- coordenar e apoiar o atendimento às informações relativas a inspeções, auditorias, diligências, solicitações, ocorrências e recomendações dos órgãos de fiscalização e de controle e da Auditoria Interna;

- realizar outras atividades correlatas definidas pelo Conselho de Administração.

São responsabilidades dos gerentes da Auditoria Interna:

- supervisionar a realização de auditorias internas, inclusive auditorias contínuas, com acesso irrestrito a áreas e informações, relacionadas entre outros aos temas de natureza contábil, financeira, tributária, orçamentária, administrativa, patrimonial, tecnologia da informação, gestão de aquisições, contratos, logística, pessoas, governança, riscos, controles internos e negócios, bem como na entidade fechada de previdência complementar;

- acompanhar as ações para atendimento pelas áreas auditadas de ocorrências, recomendações e determinações emitidas pelos órgãos de controle, pela Auditoria Interna ou pelos órgãos reguladores;

- debater medidas preventivas, corretivas e planos de ação propostos pelos gestores para atendimento das ocorrências, recomendações e determinações emitidas pelos órgãos de controle, pela Auditoria Interna ou pelos órgãos reguladores;

- avaliar a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança e a confiabilidade do processo de coleta, mensuração, classificação, acumulação, registro e divulgação de eventos e transações, visando ao preparo de demonstrações financeiras;

- coordenar a realização de auditoria sobre denúncia com apuração demandada pelos órgãos de fiscalização e de controle, pelo Conselho de Administração, pelo Conselho Fiscal ou pela Diretoria Executiva.

Compete ao titular, aos gerentes e aos demais profissionais da Auditoria Interna:

- manter atitude de independência em relação ao auditado, de modo a assegurar imparcialidade no seu trabalho, bem como nos demais aspectos relacionados com sua atividade profissional;

- possuir domínio do julgamento profissional, pautando-se no planejamento dos exames de acordo com o estabelecido no escopo da auditoria, na seleção e aplicação de procedimentos técnicos e testes necessários, assim como a obtenção de evidências adequadas e suficientes para suportar as opiniões em relatórios;

- ter habilidade no trato verbal e escrito, com pessoas e instituições, respeitando superiores, subordinados e pares, bem como aqueles com os quais se relaciona profissionalmente;

- manter atualizado seus conhecimentos técnicos, acompanhando a evolução de leis, normas, procedimentos e técnicas aplicáveis ao Sistema de Controle Interno do Poder Executivo Federal e à auditoria interna governamental;

- agir com prudência, habilidade e atenção, de modo a reduzir ao mínimo a ocorrência de erros, zelando pelas normas de ética profissional, pelo equilíbrio de opiniões e atos, pela razoabilidade de recomendações e pelo cumprimento das normas gerais e dos procedimentos de auditoria.

4.2 Participação de Profissionais externos à Auditoria Interna

Conforme previsto no Regimento Interno da Auditoria Interna: Art 17. *"§ 1º Para cumprir os objetivos de auditoria, a Auditoria Interna pode optar por requisitar a assistência de empregados de outras áreas que tenham domínio técnico sobre o objeto auditado, obter assessoria de especialistas externos à empresa ou depositar confiança no trabalho de outros prestadores internos ou externos de serviços de avaliação ou de consultoria.*

§ 2º Caso opte por obter assessoria de especialistas externos ou depositar confiança no trabalho de terceiros, o titular da Auditoria Interna deve estabelecer um processo consistente para obter um entendimento claro do escopo, dos objetivos e dos resultados do trabalho realizado para determinar a extensão da confiança depositada, a suficiência das evidências e eventual necessidade de testes adicionais de confirmação.

§ 3º O referido processo deve confirmar se os especialistas atendem aos requisitos aplicáveis aos auditores internos, especificamente quanto a objetividade, independência, competência, proficiência, zelo profissional devido, ausência de conflito de interesses, ainda que aparente, declaração de ciência e concordância com o Código de Ética do IIA e do Serpro, mantendo adequada estrutura de supervisão suportada por programa de qualidade e melhoria contínua".

No caso de contratação de terceiros, deve ser feita consulta prévia à CGU em consonância com o previsto no Decreto 3.591/2000:

> Art. 16. A contratação de empresas privadas de auditoria pelos órgãos ou pelas entidades da Administração Pública Federal indireta somente será admitida quando comprovada, junto ao Ministro supervisor e ao Órgão Central do Sistema de Controle Interno do Poder Executivo Federal, a impossibilidade de execução dos trabalhos de auditoria diretamente pela Secretaria Federal de Controle Interno ou órgãos setoriais do Sistema de Controle Interno do Poder Executivo Federal. ("Caput" do artigo com redação dada pelo Decreto nº 4.440, de 25/10/2002).

Na decisão de contratação de profissionais externos à auditoria interna, levar em consideração:

- Existência de pessoal na empresa com competência técnica para desempenhar a atividade, considerando a racionalização de recursos públicos;
- Existência de pessoal em outros órgãos/entes públicos com competência técnica para desempenhar a atividade, considerando a racionalização de recursos públicos;
- Obter aprovação do Conselho para contratação;
- A depender do objeto da contratação, avaliar possível conflito com a Empresa que presta serviço de auditoria externa nas demonstrações contábeis do Serpro e do Serpros. No documento "Declaração de Posicionamento do IIA: O papel da Auditoria Interna no Suprimento de Recursos para a Atividade de Auditoria Interna" (link), o IIA se posiciona de forma contrária a contratação da mesma empresa que presta este tipo de serviço.
- As IPPF permitem aos auditores prestarem serviços de avaliação sobre serviços para os quais realizaram consultoria, nesse sentido, os prestados de serviço consultivo no Serpros podem ser contratados para prestação de serviço de avaliação, sendo dada transparência quanto a esse fato no Relatório emitido.
- Do mesmo modo, a auditoria interna contratada pelo Serpros pode ser contratada para prestação de serviço de avaliação para a patrocinadora, desde que o escopo não inclua a supervisão sobre a atuação da própria auditoria interna do Serpros, situação em que sua independência e objetividade estaria prejudicada.
- Observar determinações regulatórias do objeto da contratação;
- Realizar estudo técnico sobre as vantagens e desvantagens da contratação;

Para uso de serviços de prestadores externos, as competências do especialista em relação ao trabalho a ser realizado deve ser avaliada, considerando aspectos importantes, como:

a) certificação/formação/licença profissional e/ou outro reconhecimento de sua competência no tema que será objeto de seus serviços;
b) formação acadêmica e treinamentos recebidos que estejam relacionados com o tema em questão;
c) experiência no tipo de trabalho a ser realizado;
d) filiação em organização profissional apropriada e adesão ao código de ética daquela organização;
e) reputação, que pode ser confirmada mediante contato com terceiros que conheçam seu trabalho.

Outro aspecto fundamental é que haja garantia de objetividade por parte do prestador de serviços externo. Dessa forma, devem ser consideradas as seguintes possibilidades de conflito de interesses, entre outras:

- compensações, incentivos ou punições que possa vir a receber;
- interesses financeiros;
- relação pessoal ou profissional com setores do órgão ou entidade auditada ou com o objeto do trabalho que prejudiquem a objetividade e outros serviços que o especialista possa estar prestando à mesma organização incompatíveis com aquele que desenvolverá no âmbito do trabalho de auditoria.

Os tipos de contratação externa podem ser:

a) *Total*: 100% do trabalho de auditoria realizado por um prestador de serviço externo ao Serpro;
b) *Parcial*: menos de 100% do trabalho de auditoria é realizado por prestador de serviço externo ao Serpro;
c) *Coparticipação* (*Co-sourcing*): recursos externos participam do trabalho de auditoria em conjunto com a equipe da auditoria interna do Serpro. Podendo ser em auditoria contínua ou específicas;

d) *Subcontratação*: um trabalho específico ou parte de um trabalho de auditoria é realizado por um terceiro externo ao Serpro, com escopo definido e específico e tempo limitado. A administração e supervisão do trabalho é realizada pela equipe da auditoria interna do Serpro.

No processo de contratação deve ser estabelecido o nível de confiança no trabalho do prestador de serviço. A confiança no trabalho de terceiros deve seguir um processo seguro, consistente e bem documentado e supervisionado com critérios bem definidos para determinar se a auditoria interna pode confiar no trabalho de outro prestador de serviço. Alguns critérios consistem em:

- Avaliar a objetividade, considerando se o prestador tem, ou parece ter, quaisquer conflitos de interesses e se foram divulgados;
- Considerar a independência, examinando as relações de reporte do prestador de serviços e o impacto dessa hierarquia;
- Confirmar a competência, verificando se a experiência profissional, qualificações, certificações e afiliações do prestador de serviços são apropriadas e vigentes;
- Avaliar o zelo profissional devido, examinando os elementos de prática que o prestador de serviços utiliza para concluir o trabalho (como a metodologia utilizada pelo prestador de serviços e se o trabalho foi devidamente planejado, supervisionado, documentado e revisado);
- A existência de programa de gestão e melhoria da qualidade implantado, compatível com o exigido pelas IPPF.
- O CAE também pode buscar obter um entendimento do escopo, objetivos e resultados do trabalho realizado, para determinar a extensão da confiança dedicada ao trabalho do prestador de serviços.

O CAE normalmente considera se as descobertas do prestador de serviços são razoáveis e baseadas em evidências suficientes, confiáveis e relevantes. O CAE também determina se são necessários trabalhos ou testes adicionais para obter evidências suficientes para apoiar ou aumentar o nível de confiança desejado. Se trabalhos adicionais forem necessários, a auditoria interna deve testar novamente os resultados do outro prestador de serviços. Conforme descrito no Manual de Orientações da CGU - MOT:

> Para que a opinião dos especialistas seja utilizada pelos auditores internos governamentais, quer como subsídio para o desenvolvimento das etapas do trabalho, quer como evidência para os achados de auditoria, é necessário que a UAIG:
>
> a) garanta que o trabalho do colaborador externo seja planejado, documentado e supervisionado;
>
> b) avalie se o trabalho foi realizado de acordo com os critérios predefinidos e com aqueles constantes do PGMQ;
>
> c) verifique se a opinião e as evidências apresentadas são apropriadas e suficientes e se passam pelo crivo da razoabilidade;
>
> d) decida sobre a necessidade de realizar testes adicionais.
>
> Para assegurar que os especialistas contribuam efetivamente para o desenvolvimento dos trabalhos, a UAIG deve emitir termo de confidencialidade e objetividade específico para a atividade a ser desenvolvida. Esse termo deve ser subscrito pelo especialista, o qual deverá se comprometer:
>
> a) com o cumprimento dos preceitos específicos que estejam sendo acordados para o referido trabalho;

b) com o cumprimento dos preceitos da IN SFC nº 3, de 2017, e de outras normas e códigos de ética pertinentes, inclusive quanto à inexistência de conflitos de interesses impeditivos de sua atuação imparcial e objetiva no referido trabalho;

c) a manter em sigilo as informações a que tiver acesso na realização das atividades que lhe serão atribuídas.

Antes de iniciar o trabalho, é importante também que a UAIG obtenha do colaborador externo autorização para utilizar e divulgar a sua opinião.

4.3 Gerenciamento de situações que podem afetar a objetividade

O Estatuto Social do Serpro (link), em seu artigo 42 prevê: "*O Serpro disporá de Auditoria Interna, vinculada ao Conselho de Administração, com atribuições e competências fixadas pelo Conselho de Administração e pela legislação pertinente* ***e se restringirá à execução de suas atividades típicas,*** *preservando sua isenção e imparcialidade*".

Conforme disposto no Regimento Interno da Auditoria Interna, eventuais ameaças, de fato ou veladas, à autonomia técnica e à objetividade devem ser gerenciadas nos níveis da Auditoria Interna, do seu titular, dos trabalhos de auditoria e dos auditores, sendo recusado o trabalho ou reportado à alta administração e ao Conselho de Administração para adequado tratamento e adoção de salvaguardas.

Cabe ao titular da Auditoria Interna, com apoio do Conselho de Administração e supervisão pelo Comitê de Auditoria, garantir que a atividade de auditoria permaneça livre de todas as condições que ameacem a habilidade dos auditores internos de cumprir com suas responsabilidades de forma imparcial, incluindo questões de seleção, escopo, julgamento profissional, procedimentos, frequência, cronograma ou conteúdo dos relatórios de auditoria.

Os profissionais da auditoria interna, no exercício de seu trabalho devem reportar à chefia imediata e ao Auditor Interno ameaças, de fato ou veladas, à independência da sua opinião, à determinação do escopo das auditorias, à execução do trabalho, ao julgamento profissional ou à comunicação dos resultados obtidos. Caberá ao titular da Auditoria Interna o dever de reportar ao Conselho de Administração e ao Comitê de Auditoria tais fatos.

Caso o titular da Auditoria Interna assuma ou espere-se que assuma papéis ou responsabilidades que vão além das atividades típicas de auditoria, devem ser adotadas salvaguardas para limitar o prejuízo à independência ou à objetividade.

A IPPF 1130 que trata de Prejuízo à Independência ou à Objetividade expressa:1130.A1 – *Os auditores internos devem evitar avaliar operações específicas pelas quais tenham sido responsáveis anteriormente*. Presume-se que a objetividade esteja prejudicada se um auditor interno prestar serviços de avaliação de uma atividade pela qual tenha sido responsável durante o ano anterior. Já a IN CGU n.º 3/2017 -Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal aborda: *52. Os auditores internos governamentais devem se abster de auditar operações específicas com as quais estiveram*

envolvidos nos últimos 24 meses, quer na condição de gestores, quer em decorrência de vínculos profissionais, comerciais, pessoais, familiares ou de outra natureza, mesmo que tenham executado atividades em nível operacional.

Desta forma o entendimento é de que não deve ser negada vigência a nenhum dos dois dispositivos, sendo adotada interpretação sistemática deles. Dando exemplos, se o escopo do trabalho alcança sua atuação pretérita, o auditor deve ser abster de auditar um contrato específico no qual atuou como fiscal, gestor técnico ou gestor administrativo nos últimos 24 meses, no entanto não deve ser abster de auditar toda e qualquer contratação que correu na área que atuou. Na auditoria contábil, deve se abster de auditar lançamentos contábeis que fez com o seu usuário no sistema, planilhas de controle que elaborou, mas não deve se abster de auditar as demonstrações contábeis ou notas explicativas fruto do trabalho coletivo das áreas, ainda que tenha atuado operacionalmente no processo como um todo. Não fosse esse o entendimento, teríamos o absurdo de a Auditoria deter o conhecimento técnico atualizado, mas não poder acessá-lo devido a uma atuação operacional pontual, o que vai contra a obrigação de proficiência das equipes.
Aquilo que não se presume comporta prova em contrário e salvaguardas, para essas finalidades considera-se suficiente a própria declaração individual de objetividade, que em última instância externaliza se aquela atuação operacional do passado de algum modo ainda se reflete como um prejuízo à livre formação do convencimento e à objetividade individual, uma escusa de consciência.
Não sendo esse o caso, cabe a adoção de salvaguardas já inseridas no processo de qualidade da auditoria, especificamente quanto à supervisão dos testes e respectivos papéis de trabalho, discussão dos achados de auditoria na equipe, busca conjunta de soluções para apresentação aos gestores, avaliação interna de qualidade.
Esses elementos tomados em conjunto asseguram que não houve e não há prejuízo, ainda que aparente, à objetividade individual do auditor nem da Auditoria Interna. Sendo esse o objetivo primeiro de ambos os dispositivos: assegurar que a opinião da Auditoria Interna foi construída a partir do livre convencimento, não decorrendo de vieses e julgamentos prévios pessoais.

5 Gestão e Melhoria da Qualidade

A Auditoria Interna do Serpro dispõe de um Programa de Gestão e Melhoria da Qualidade (PGMQ), que tem por objetivo promover a melhoria contínua da atividade de auditoria interna e uma cultura que resulta em comportamentos, atitudes e processos de caráter permanente que sustentam entregas de produtos de alto valor agregado, atendendo às expectativas das partes interessadas e ao propósito da Auditoria Interna.

O PGMQ deve ser aplicado tanto no nível de trabalhos individuais de auditoria, quanto no nível mais amplo da atividade de auditoria interna e consistirá na gestão dos riscos da própria Auditoria Interna do Serpro, denominados riscos de auditoria, cujos controles de qualidade integrarão plano de ação, sendo a conformidade evidenciada por meio de avaliações internas e externas de qualidade com base em amostragem, conforme detalhamento adiante descrito.

Conforme definido no Regimento Interno da Auditoria Interna:

Art 22 - "§ 2º O PGMQ adotará o Quality Assessment (Blue Book) do The IIA como referencial para avaliar a conformidade com os elementos obrigatórios da Estrutura Internacional de Práticas Profissionais (IPPF), incluindo as Normas Internacionais, o Código de Ética, os Princípios Fundamentais e a Definição de Auditoria Interna.

§ 3º O PGMQ consistirá de atividades de monitoramento contínuo, avaliação interna periódica e avaliação externa e abrangerá do nível mais amplo da atividade de auditoria interna até o nível de auditorias individuais, incluindo todas as fases da atividade de auditoria, quais sejam, as etapas de planejamento, de execução dos trabalhos, de comunicação dos resultados e de monitoramento de recomendações.

§ 4º Cabe ao titular da Auditoria Interna comunicar ao menos anualmente os resultados do PGMQ ao Conselho de Administração, ao Comitê de Auditoria e à alta administração, com supervisão pelo Comitê de Auditoria do progresso no plano de ações corretivas, se houver, apresentando os resultados das avaliações internas e externas, as oportunidades de melhoria e as fragilidades encontradas que possam comprometer a qualidade da atividade de auditoria interna.

§ 5º Os resultados de avaliações externas e internas periódicas devem ser reportados tão logo sejam concluídas, enquanto os resultados do monitoramento contínuo devem ser comunicados em conjunto com o Relatório Anual de Atividades de Auditoria Interna (RAINT).

Art. 23 Visando sustentar níveis elevados de capacidade da atividade de auditoria interna, as avaliações periódicas incluirão autoavaliação segundo o Modelo de Capacidade de Auditoria Interna (IA-CM), do Instituto dos Auditores Internos (IIA), e conforme normativos vigentes da Controladoria-Geral da União.

Parágrafo único. No exercício da visão estabelecida, visando contribuir com a divulgação do modelo IA-CM, fica a Auditoria Interna autorizada a firmar parcerias, cooperações e a compartilhar materiais de interesse técnico e acadêmico com outras unidades de auditoria interna, assim como divulgar documentos de acesso público, de caráter ostensivo, respeitados os normativos de classificação da informação.

Art. 24 As avaliações externas serão realizadas, no mínimo, a cada 5 (cinco) anos, com o objetivo de obter opinião independente sobre o conjunto geral dos trabalhos de auditoria realizados quanto ao requisito de conformidade com os elementos obrigatórios da IPPF."

5.1 Avaliações

As avaliações no âmbito do PGMQ se dividem em:

5.1.1 Avaliações internas

5.1.1.1 Monitoramento contínuo.

O monitoramento contínuo contempla, entre outras, as seguintes atividades:

a) estabelecimento de indicadores de desempenho;

O item 8.0 Auditoria Contínua possui um detalhamento maior sobre os indicadores.

A Audin utiiza o Qlik sense para acompanhamento dos indicadores (link)

b) supervisão de todas as fases dos trabalhos de auditoria;

O item 4.1 explicita os papéis dos participantes da Auditoria Interna, dentre eles os referentes à supervisão de todas as fases dos trabalhos de auditoria. Tal supervisão fica registrada nos logs do Sistema de Auditoria – Sisaudit. Vale ressaltar também o registro por meio da Avaliação Interna de Qualidade (link), a qual permeia todas as fases dos trabalhos de auditoria.

c) revisão de documentos, de papéis de trabalho e de relatórios de auditoria por pares ou pelo supervisor;

O fluxo de revisão por pares ou pelo Supervisor encontra-se devidamente descrito no item 3 deste manual, a exemplo do transcrito abaixo:

"3.1.1.32 - *Na Audin, a revisão técnica dos trabalhos foi delegada para os Gerentes de Auditoria. Foi criada a figura do Gerente par, inclusive como uma estratégia no âmbito do PGMQ para que temas com interface mantenham um fluxo natural de comunicação e sinergia entre abordagens de auditoria em áreas correlatas, conforme segue:*

Gerência de Auditoria	Gerente par
AUDCF	AUDEP
AUDEP	AUDPC
AUDPC	AUDCF
AUDAC	AUDTN
AUDTN	AUDAC
AUDCN	Conforme escopo

O Gerente par deve revisar os principais artefatos do trabalho, incluindo DAP, Matriz de Riscos e Relatório de Auditoria, para que possa realizar as revisões conhecendo o contexto precedente. Embora exista essa alocação ordinária, a depender do escopo do trabalho, de abordagens precedentes, pode ser mais efetivo definir outro Gerente par para um trabalho específico, que deve ser comunicado pelo gerente da equipe responsável pelo trabalho."

d) listas de verificação (checklists) para averiguar se manuais e procedimentos de auditoria estão sendo adequadamente observados;

Conforme descrito no Regimento Interno da Auditoria Interna: Art. 22 - "*§ 2º O PGMQ adotará o* ***Quality Assessment (Blue Book)*** *do The IIA como referencial para avaliar a conformidade com os elementos obrigatórios da Estrutura Internacional de Práticas Profissionais (IPPF), incluindo as Normas Internacionais, o Código de Ética,*

os Princípios Fundamentais e a Definição de Auditoria Interna". Além disso e, conforme definido no Art 23 do Regimento Interno: "Visando *sustentar níveis elevados de capacidade da atividade de auditoria interna, as avaliações periódicas incluirão* ***autoavaliação*** *segundo o Modelo de Capacidade de Auditoria Interna* ***(IA-CM),*** *do Instituto dos Auditores Internos (IIA), e conforme normativos vigentes da Controladoria-Geral da União."*

O checklist de monitoramento contínuo - formulário Avaliação Interna de Qualidade (link) é aplicado para todos os trabalhos.

O Plano Anual de Auditoria Interna – PAINT, conterá o detalhamento das avaliações de qualidade previstas para cada exercício.

f) feedback de gestores e de partes interessadas:

f1) de forma ampla, para aferir a percepção da alta administração sobre a agregação de valor da atividade de auditoria interna, e

Este feedback ocorre, anualmente, por meio do "Relatório de avaliação de desempenho do Auditor Interno", cuja avaliação é feita pelos membros do Conselho de Administração. A Superintendência de Gestão de Pessoas – SUPGP é a responsável pela condução do processo em conjunto com a Secretaria do Conselho de Administração. Nesta avaliação são avaliadas várias questões que permeiam todo o processo da Auditoria Interna, tais como: 1) Contribuição e Zelo para que os princípios da boa governança corporativa – equidade, transparência, prestação de contas e responsabilidade corporativa sejam aplicados na Empresa; 2) Assessoramento ao Conselho de Administração nos assuntos relacionados à auditoria nos processos de governança, gerenciamento de riscos e controles internos; Apresentação de relatórios periódicos sobre a execução do Plano Anual de Atividades da Auditoria Interna – PAINT e do Relatório Anual de Atividades da Auditoria Interna – RAINT, dentre outros.

Durante a elaboração do documento: "Estratégia da Função de Auditoria Interna" são definidos os alvos de valor para as entregas pelas instâncias de controle. Por meio de formulário, encaminhado aos membros dos Conselhos de Administração e Fiscal, Comitê de Auditoria, Diretoria Executiva é feita votação de itens/assuntos que refletem às expectativas das partes interessadas em relação às entregas que serão realizadas pela Auditoria Interna. Tais itens/assuntos são acompanhados por meio do *balanced scorecard* da Auditoria Interna, o qual é informado tanto no Plano Anual de Auditoria Interna – PAINT, quanto no Relatório Anual de Atividades de Auditoria Interna – RAINT.

f2) de forma pontual, considerando os trabalhos individuais de auditoria realizados;

Ao final de cada trabalho de auditoria, após o envio do relatório à área auditada é enviado o formulário "Feedback para a Auditoria Interna" (link) para os gestores envolvidos em cada trabalho.
O departamento Audie solicita aos gerentes da Audin, indicar pelo menos 3 gestores participantes do trabalho e, por meio do e-mail corporativo da Audin, encaminha mensagem solicitando o feedback, conforme exemplo abaixo:

Assunto: Feedback para Auditoria - Auditoria 'Ano/trabalho - Objetivo do trabalho"

Prezado(a) Senhor(a)

Você está sendo convidado(a) para responder o Feedback para a Auditoria Interna sobre o trabalho xpto.

São apenas seis quesitos avaliados, permitidos comentários complementares, levando cerca de 10 minutos. Pedimos que responda até xx/xx/xxxxx.

As respostas servirão para melhorarmos a abordagem de auditoria interna e serão consolidadas de modo centralizado pela equipe de assessoramento da Audin, sem divulgação individual dos respondentes. A identificação do e-mail visa subsidiar a consolidação por grupos de respondentes e eventuais contatos para melhor compreensão do Feedback, se necessário.

Em caso de dúvidas, entrar em contato com Maria Juliane Leite (maria-juliane.mendonca@serpro.gov.br) #61 8910 ou Alyne Paiva(alyne.paiva@serpro.gov.br) - #61 8099 e Walkirina Pina (walkiria.pina@serpro.gov.br) #81 4510.

Atenciosamente

Caso os gestores não respondam no prazo solicitado, enviar novamente o e-mail concedendo um novo prazo.

O resultado consolidado de todos os feedbacks, é informado no RAINT.

5.1.1.2 Avaliações periódicas

Conforme descrito na Decisão Setorial que regulamenta o PGMQ: *"3.4 No nível de trabalhos individuais de auditoria, as avaliações periódicas serão realizadas de forma sistemática, abrangente e permanente, por meio de amostragem, com base em roteiros de verificação previamente estabelecidos para avaliar a qualidade, a adequação e a suficiência do processo de planejamento, das evidências e dos papéis de trabalho produzidos ou coletados pelos auditores, das conclusões alcançadas, da comunicação dos resultados, do processo de supervisão, e do processo de monitoramento das recomendações emitidas em trabalhos individuais de auditoria, conforme escala de risco definida."* O detalhamento de como serão realizadas tais avaliações constam do item 5.1 - "d" deste Manual.

5.1.2 Avaliações externas

Conforme descrito na Decisão Setorial do PGMQ: *"3.6 As avaliações externas serão realizadas, no mínimo, a cada 5 (cinco) anos, com o objetivo de obter opinião independente sobre o conjunto geral dos trabalhos de auditoria realizados quanto ao requisito de conformidade com os elementos obrigatórios da IPPF citados.*

3.6.1 As avaliações externas serão conduzidas por profissional ou organização certificado e independente, externo à estrutura da Auditoria Interna do Serpro, ou na forma de autoavaliação com posterior validação externa independente".

Os preparativos para nova avaliação externa de qualidade devem começar com antecedência ao mês/ exercício em que se deseja que a avaliação externa seja realizada. Considerando, no mínimo, a cada 5 (cinco) anos e, tomando 2022 como ano base, segue exemplo de prazos a perseguir;

De junho de 2025 até outubro de 2025 = Realizar pesquisas de preços para contratação do serviço de avaliação externa de qualidade; incluir na proposta de PAINT/2026, a contratação dos serviços de avaliação prévia de qualidade e avaliação final e submeter à apreciação do Comitê de Auditoria – Coaud e à aprovação pelo Conselho de Administração).
De outubro de 2025 até abril 2026 = realizar os trâmites de planejamento da contratação (Documento de Oficialização da Demanda – DOD; Elaboração de Estudo Técnico Preliminar – ETP; Projeto Básico).
De maio de 2026 a agosto de 2026 = realizar contratação da empresa responsável pelos serviços de avaliação prévia e avaliação final de qualidade.
De setembro de 2026 a dezembro de 2026 = realizar avaliação prévia de qualidade.
De janeiro de 2027 a maio de 2027 = realizar avaliação final de qualidade.

5.2 Comunicação dos resultados.

Conforme previsto no Regimento Interno- Art 22: *"§ 4º Cabe ao titular da Auditoria Interna comunicar ao menos anualmente os resultados do PGMQ ao Conselho de Administração, ao Comitê de Auditoria e à alta administração, com supervisão pelo Comitê de Auditoria do progresso no plano de ações corretivas, se houver, apresentando os resultados das avaliações internas e externas, as oportunidades de melhoria e as fragilidades encontradas que possam comprometer a qualidade da atividade de auditoria interna.*

§ 5º Os resultados de avaliações externas e internas periódicas devem ser reportados tão logo sejam concluídas, enquanto os resultados do monitoramento contínuo devem ser comunicados em conjunto com o Relatório Anual de Atividades de Auditoria Interna (RAINT)."

Desta forma, o resultado das avaliações internas e externas de qualidade serão informadas por meio de reporte mensal aos Conselhos e Comitê de Auditoria, cujo detalhamento está no item 6.5.1 deste Manual.

No Relatório Anual de Atividades de Auditoria Interna - RAINT há um item específico sobre os resultados do Programa de Gestão e Melhoria da Qualidade – PGMQ. O RAINT é publicado na página do Serpro até o

último dia útil do mês de março do exercício seguinte ao qual se refere, ressalvadas as informações sigilosas previstas em lei.

5.3 Declarações de conformidade

No início de cada trabalho de auditoria deverão ser emitidas declarações quanto a aderência às seguintes Normas Internacionais para a Prática Profissional de Auditoria Interna (IPPF: 1120 - Objetividade individual, 1130 - Prejuízo à Independência ou à Objetividade, 1200 - Proficiência e Zelo Profissional Devido, 2230 - Alocação de recursos para o trabalho da auditoria, Princípios do Código de Ética do IIA), conforme modelo estabelecido no site da Audin. (link). A confirmação positiva e individual de que os auditores não apresentam ameaças a objetividade devem constar de cada trabalho de auditoria.
Anualmente o CAE e auditores emitirão declaração, atestando que leram, compreenderam e agiram conforme as orientações mandatórias de auditoria, que incluem: Princípios Fundamentais para a Prática Profissional de Auditoria Interna; Definição de Auditoria Interna; Normas Internacionais para a Prática Profissional de Auditoria Interna e Código de Ética do IIA e Código de Ética, Conduta e Integridade do Serpro, conforme modelo estabelecido no site da Audin (link). No PAINT e RAINT também deverão constar declarações de independência e objetividade, a exemplo do já praticado a partir do PAINT/2022 e RAINT/2021.

6 Planejamento Anual dos Trabalhos (PAINT)

O planejamento dos trabalhos de auditoria é feito anualmente com base nos normativos expedidos pela Secretaria Federal de Controle Interno (SFC) da Controladoria-Geral da União (CGU) e Estrutura Internacional de Práticas Profissionais (IPPF), que incluem a Definição de Auditoria Interna, os Princípios Fundamentais e as Normas Internacionais para a Prática Profissional de Auditoria Interna, além do Modelo IA-CM.

6.1 Elaboração do Plano Anual de Auditoria Interna (PAINT)

O PAINT apresenta a previsão dos trabalhos de auditoria prioritários a serem executados no ano seguinte e considera:

I. O planejamento estratégico e as expectativas da alta administração do Serpro e demais partes interessadas;
II. Os riscos significativos que a empresa está exposta e os seus processos de governança, de gerenciamento de riscos e de controles internos;
III. O negócio, a estrutura dentre outros fatores relevantes do contexto empresarial;
IV. A estrutura e os recursos humanos, logísticos e financeiros disponíveis na auditoria interna.

O PAINT busca apresentar uma previsão realista dos trabalhos de auditoria a serem realizados, considerando, no mínimo:

I. Relação dos trabalhos de auditoria a serem executados contendo:
    a. o tipo de serviço (avaliação ou consultoria);
    b. o objeto de auditoria;

c. o objetivo da auditoria;
d. datas previstas de início e conclusão;
e. carga horária prevista; e
f. a origem da demanda (obrigação normativa; seleção baseada em riscos; solicitação da alta administração; solicitação de órgãos de controle interno ou externo; e, outras situações, com as devidas justificativas para a sua seleção);

II. Previsão de alocação da força de trabalho, por categorias:
a. serviços de auditoria;
b. capacitação (considerar no mínimo de 40 horas anuais por auditor, incluído o titular da unidade, em treinamentos, cursos de pós-graduação lato e stricto sensu e eventos compatíveis com a atividade de auditoria, com o universo de auditoria e às competências requeridas dos auditores);
c. monitoramento das recomendações;
d. gestão e melhoria da qualidade da atividade de auditoria interna governamental;
e. levantamento de informações para órgãos de controle interno ou externo;
f. gestão interna; e
g. demandas extraordinárias recebidas durante a realização do PAINT.

A elaboração do PAINT ocorre conforme os seguintes passos:

6.1.1 Elaboração do Documento de Análise Preliminar (DAP) do PAINT

A elaboração do DAP do PAINT tem por objetivo realizar uma análise exploratória das fontes de informações disponíveis e vigentes na Empresa, para subsidiar elaboração do planejamento e, assim, promover uma atuação da Auditoria Interna vinculada ao contexto do ambiente de negócio do Serpro, considerando seu modelo de atuação, operações, sistemas, processos-chaves, a maturidade de riscos bem como a legislação federal, normativos internos e boas práticas que regem o planejamento de auditoria interna.
Para isto, busca-se explorar e conhecer a estrutura e organização da empresa, seus principais objetivos, estratégias e metas, suas operações e principais ferramentas e métodos de trabalho vigentes. Além dos assuntos relevantes referentes ao ambiente externo e de negócios no qual a Empresa está inserida.

O entendimento amplo da empresa e seu negócio é essencial para a seleção de objetos de auditoria no planejamento anual em consonância com a Estratégia de Atuação da Auditoria Interna, além de direcionar as entregas que, de fato, auxiliem a tomada de decisões pela Alta Administração e permita a auditoria interna cumpra com sua missão institucional.

6.1.2 Expectativas da Alta Administração

Visando a coleta estruturada das expectativas e da visão de riscos dos colegiados para elaboração do planejamento anual da auditoria interna, a Audin encaminha à Diretoria Executiva, membros do COAUD, Conselheiros de Administração e Conselheiros Fiscais, um formulário (link) no qual devem expressar opinião quanto aos temas nos quais enxergam riscos relevantes e temas, processos, projetos ou serviços específicos para os quais possuem expectativa que sejam realizados trabalhos de auditoria.

6.1.3 Elaboração da Matriz de Riscos do PAINT

Para a elaboração da Matriz de Riscos do PAINT são considerados os riscos associados aos processos da cadeia de valor do Serpro, distribuídos em 3 blocos:

- Avaliação de riscos (GESTOR) - 25%;
- Avaliação de riscos (Auditoria Interna) - 35%;
- Avaliação de riscos (Alta Administração) - 40%.

Após a pontuação dos fatores, é aplicada média ponderada para classificação dos processos em ordem decrescente do nível de risco.

6.1.3.1 Extrair relação de processos vigentes na Cadeia de Valor do Serpro e considerar, também alíneas do Art 1º da CGPAR nº 9 no caso do Serpros

No sistema integra (link) gerar a query: "RELATORIO MACRO - PROCESSO - SUBPROCESSO". O arquivo gerado terá essa formatação:

	E	F	G	H	I	J	K	L	M	N
1	Código do	Nome do subproces	stage_process	stage_sub_proces	CLASSIFICAÇÃO	CRITICIDADE	GESTOR DO PROCESS	ÓRGÃO	Diretoria	Superintendencia
2	01.03.04	Criar produtos	Em Produção	Em Produção	Finalístico, Finalíst	Indefinida, Baixa	Alexandre Seabra Melo F	SUPERINTENDENCIA DE INTELIGENCIA DE NEGOCIO	DIRCL	SUNIN
3	01.05.01	Gerir fomento à inov	Em Produção	Em Produção	Finalístico	Baixa	Marcio de Araujo Benedit	DIVISAO DE GESTAO DO CONHECIMENTO E DA INFC	DIDHM	SUPED
4	01.06.02	Gerir transformação	Em Produção	Em Produção	Finalístico	Média	Maykel Douglas Sousa F	DEPARTAMENTO DE GESTAO COPORATIVA DE PRO	DIJUG	SUPOG
5	02.02.02	Gerir marketing digit	Em Produção	Em Produção			Fábio Renato Silva de M	DIVISAO DE PLANEJAMENTO DE MARKETING	DP	SUPEM
6	02.02.03	Desenvolver planejar	Em Produção	Em Produção	Finalístico, Finalíst	Alta, Indefinida	Fábio Renato Silva de M	DIVISAO DE PLANEJAMENTO DE MARKETING	DP	SUPEM
7	02.02.04	Gerir Publicidade	Em Produção	Em Produção	Finalístico, Finalíst	Alta, Indefinida	Fábio Renato Silva de M	DIVISAO DE PLANEJAMENTO DE MARKETING	DP	SUPEM
8	02.02.05	Gerir promoção e pa	Em Produção	Em Produção	Finalístico	Indefinida	Fábio Renato Silva de M	DIVISAO DE PLANEJAMENTO DE MARKETING	DP	SUPEM
9	02.02.06	Gerir branding do pr	Em Produção	Em Produção	Finalístico, Finalíst	Baixa, Indefinida	Fábio Renato Silva de M	DIVISAO DE PLANEJAMENTO DE MARKETING	DP	SUPEM
10	02.03.01	Direcionar Estrategi	Em Produção	Em Produção	Finalístico	Indefinida	Catharine Rafaele Chaga	COORDENACAO DE SUPORTE ADMINISTRATIVO - DIF	DIRCL	COADM
11	02.04.02	Gerir Relacionament	Em Produção	Em Produção			Catharine Rafaele Chaga	COORDENACAO DE SUPORTE ADMINISTRATIVO - DIF	DIRCL	COADM
12	02.04.03	Gerir Negociacao de	Em Produção	Em Produção			Catharine Rafaele Chaga	COORDENACAO DE SUPORTE ADMINISTRATIVO - DIF	DIRCL	COADM
13	02.05.02	Gerir ciclo de vida d	Em Produção	Em Produção	Finalístico	Indefinida	Catharine Rafaele Chaga	COORDENACAO DE SUPORTE ADMINISTRATIVO - DIF	DIRCL	COADM

Obs: Para inserir *queries* no Integra, deve-se utilizar o seguinte caminho: Integra - home - meus favoritos - adicionar item - item do SA - em categorias escolher system manager - em tipos escolher query - selecionar pasta do lado direito e escolher a query desejada. Neste caso é o: ELATORIO MACRO - PROCESSO - SUBPROCESSO - OK - salvar.

No caso do Serpros, considerar como processos, as alíneas do Art 1º da CGPAR nº 09: a) política de investimentos e sua gestão; b) processos de concessão de benefícios; c) metodologia utilizada no cálculo atuarial, custeio, consistência do cadastro e aderência das hipóteses; d) procedimentos e controles vinculados à gestão administrativa e financeira da entidade; e) despesas administrativas; f) estrutura de

governança e de controles internos da entidade; e g) recolhimento das contribuições dos patrocinadores e participantes em relação ao previsto no plano de custeio.

6.1.3.2.1 Avaliação de riscos (Gestor)

O bloco relativo à avaliação de riscos pelo gestor contempla a avaliação de riscos dos processos da cadeia de valor com base nos critérios de probabilidade e impacto dos riscos mais críticos associados a cada processo. Abrir planilha com aba: "I. Avaliação de riscos (GESTOR)". A planilha terá inicialmente as seguintes colunas:

- Unidade de Auditoria: Informar, de acordo com o processo, o departamento de auditoria responsável pelo tema.
- Tema: Preencher conforme tabela de temas vigente (link).
- Unidade Responsável: Gestor responsável pelo processo conforme extração do sistema integra.
- Classificação Processo: Finalístico ou Viabilizador, conforme extração do sistema integra.
- Macroprocesso: Conforme classificação cadeia de valor no sistema integra.
- Nº Processo: conforme extração do sistema integra.
- Processo: conforme extração do sistema integra.

No Archer (link) deve-se gerar uma extração dos riscos operacionais, estratégicos e de projetos que contenha os processos da cadeia de valor devidamente associados. Com base nesta extração, considerar a maior classificação de probabilidade e impacto para cada processo. Preencher as seguintes colunas:

Impacto Atual

Classificação: Inserir a classificação que consta no impacto do processo conforme extração Archer (muito baixo (1), baixo (2), médio (3), alto (4) e muito alto (5)). Pontuação: considerar a pontuação da metodologia de gestão de riscos e controles (link)

Probabilidade Atual

Classificação: Inserir a classificação que consta na probabilidade do processo conforme extração Archer (muito baixa (1), baixa (2), média (3), alta (4) e muito alta (5)). Pontuação: considerar a pontuação da metodologia de gestão de riscos e controles (link)

Probabilidade Agravada: =SE(K15>=Q15;K15;K15+1)

Corresponde à incidência do score RCSA (autoavaliação de riscos e controles pelos gestores) normalizado como agravante de probabilidade. Se o score RCSA normalizado (Q15) for maior que a probabilidade registrada no Archer (K15), a pontuação deve ser agravada somando 1 à probabilidade considerada.

Nível de Risco Atual

O Nível de Risco (NR) é gerado pelo produto resultante entre a probabilidade e o impacto. Classificação: Inserir a classificação que consta no nível de risco atual conforme extração archer. Pontuação: considerar a pontuação proposta na tabela abaixo:

NÍVEL DE RISCO E APETITE	FAIXA INFERIOR	FAIXA SUPERIOR
MUITO ALTO	25	25
ALTO	16	24
MÉDIO	12	15
BAIXO	6	11
MUITO BAIXO	1	5

Fatores de Risco

Score RCSA pelo Gestor (Agravante de Probabilidade)

Score RCSA

Por meio de formulário (link) o próprio gestor realiza uma Autoavaliação da Maturidade de Riscos e Controles (RCSA). Em 17 questões objetivas, os 5 componentes do COSO ICIF - Framework Integrado de Controles Internos são detalhados de forma a apoiar o gestor na análise de gaps e possíveis ações para melhoria. Inserir nesta coluna o resultado da autoavaliação realizada pelos gestores em cada processo da cadeia de valor do Serpro.

Score RCSA Normalizado =ARRED(1+(P15/MÁXIMO($P$15:$P$201))*4;0)

Com o objetivo de trazer o resultado para uma escala comum de probabilidade, de 1 a 5, sem distorcer as diferenças nos intervalos de valores, efetuar a normalização da pontuação do score por meio da fórmula indicada. O "p" nesta fórmula representa o score do RCSA.

Explicando: a função máximo procura o maior valor de score do RCSA e compara com o score do processo atual. Processos não avaliados (score 0) receberão 1 e os maiores scores receberão probabilidade 5.

Apetite a risco (Agravante do Nível de Risco)

Conforme consta na metodologia de riscos, o apetite a risco nada mais é que o nível máximo de risco em que é possível aceitar o risco. No Archer, cada processo da cadeia de valor possui um Apetite a Riscos definido, também nas 5 faixas.

Esse campo é considerado como um agravante do nível de riscos atual, com o seguinte comportamento: se o nível de risco atual agravado (considerando probabilidade agravada) for maior que o apetite, a pontuação é agravada em 1 (uma) unidade. Se não, a pontuação é mantida.

Classificação: Inserir a classificação que consta no apetite conforme extração Archer.

Pontuação: considerar a pontuação da faixa superior proposta na tabela a seguir:

NÍVEL DE RISCO E APETITE	FAIXA INFERIOR	FAIXA SUPERIOR
MUITO ALTO	25	25
ALTO	16	24
MÉDIO	12	15
BAIXO	6	11
MUITO BAIXO	1	5

Nível de Risco Atual Agravado =SE(E(O15>S15,O15<>25),O15+1,O15)
Conforme antes explicado, se o nível de risco (O15) está fora do apetite (S15), agravar somando 1 (exceto se nível de risco já for 25). Caso contrário, manter a pontuação.

6.1.3.2.2 Avaliação de riscos (Auditoria Interna)

O bloco relativo à avaliação de riscos pela Auditoria Interna contempla a avaliação de riscos dos processos da cadeia de valor com base nos critérios de probabilidade e impacto dos riscos mais críticos associados a cada processo, sob a ótica da Audin.
Para pontuação deste fator devem ser observados os riscos das recomendações emitidas pela Auditoria Interna nos últimos 5 anos, assim como a avaliação (RRC) do sistema de controle interno dos processos avaliados pela Auditoria Interna, com base nos 17 princípios do COSO - ICIF.
Os riscos relativos à fraude e corrupção são considerados com base nos riscos de integridade associados a cada processo, além da existência de denúncias e processos de sindicância e administrativo disciplinar (PAD), considerados em escala de gravidade.
Este bloco também leva em consideração a rotação de ênfase. São verificados os trabalhos realizados nos últimos 5 anos e pontuados conforme a seguinte escala: 5 - Processo não auditado nos últimos 5 anos; 3 - Processo auditado há mais de 3 anos e 1 - Processo auditado nos últimos 3 anos. Ao final , chega-se ao Nível de Risco Audin Agravado.

Avaliação pela Auditoria Interna quanto ao nível de risco do processo

Impacto e Probabilidade
Os gerentes de departamento da auditoria interna, em conjunto com as equipes, devem fazer uma avaliação de probabilidade e impacto relativa a cada processo. Nesta avaliação, devem considerar o nível de risco da recomendação mais grave daquele processo nos últimos 3 anos. Após essa classificação, deve verificar a necessidade de revisão da probabilidade x impacto e processos associados no redimne (follow-up de recomendações).

Racional (inclusive Fraude)
Nesta coluna deve ser registrado o racional utilizado para fazer a classificação de probabilidade e impacto pela Auditoria Interna. É preciso que o racional descrito permita o correto entendimento da classificação atribuída pela Audin nas colunas de impacto e probabilidade.

Probabilidade Agravada =SE(OU(I18>=MÁXIMO(N18,P18,R18),I18=5),I18,I18+1)
Se a probabilidade (I8) já for 5 ou for maior ou igual aos agravantes 'Score RRC Normalizado' (N18), score de 'Rotação de ênfase' (P18) e pontuação de 'PAD/Sindicância/Denúncia' (R18), manter a pontuação. Caso contrário (se for menor que os agravantes), agravar somando 1.

Score RCSA pela Auditoria Interna

Avaliação Audin por meio do RCSA

Nesta coluna deve ser informado o histórico de avaliação do processo pela Audin. Se tiver havido avaliação por meio do RCSA, informar o trabalho a que se refere tal avaliação.

Score RCSA

Informar a nota da avaliação mais recente realizada no processo.

Score RCSA Normalizado =ARRED(1+(M18/MÁXIMO($M$17:$M$200))*4,0)

Com o objetivo de trazer o resultado para uma escala comum de probabilidade, de 1 a 5, sem distorcer as diferenças nos intervalos de valores, efetuar a normalização da pontuação do score por meio da fórmula indicada. O "M" nesta fórmula representa o score do RRC.
Explicando: a função máximo procura o maior valor de score do RRC e compara com o score do processo atual. Processos não avaliados (score 0) receberão 1 e os maiores scores receberão probabilidade 5.

Rotação de Ênfase (Até 5 exercícios)

Exercícios auditados

Com base nos dados do sistema de auditoria - Sisaudit, informar os exercícios nos quais houve serviço de avaliação em cada processo. Considerar os últimos 5 exercícios para relacionar os trabalhos em que houve avaliação. É possível extrair essa informação também por meio do sistema Info.Audin (link). Na opção arquivo - novo - Saiku/Analytics - cubo - dimensão 01. Auditoria Interna - 0.01 PAINT - Auditoria, seleciona a dimensão 1.3 Auditoria - seleciona os itens: ano e auditoria e arrasta para o campo linha; Em seguida, seleciona a dimensão Processo SISAUDIT - item processo para o campo coluna. Isto gera uma planilha com as quantidades de auditorias realizadas nos processos. No Saiku, consta somente a partir de 2019. Informações anteriores são extraídas da análise de rotação de ênfase realizada para os PAINT anteriores.

Pontuação

Inserir pontuação conforme tabela abaixo:

ROTAÇÃO DE ÊNFASE	ESCALA
5	Processo não auditado nos últimos 5 anos
3	Processo auditado há mais de 3 anos
1	Processo auditado nos últimos 3 anos

Conforme previsto no Regimento Interno da Auditoria Interna: *"Art. 7º - (...) § 2º A rotação de ênfase consistirá em ciclos de 1 (um) a 5 (cinco) anos de intervalo máximo para nova auditoria no mesmo objeto, correspondendo respectivamente aos níveis de risco de muito alto a muito baixo.*
§ 3º Excepcionalmente e mediante justificativa, a depender do nível de risco e da relação custo-benefício, o titular da Auditoria Interna poderá propor que determinados objetos sejam avaliados em intervalos ainda maiores, por avaliação combinada das demais linhas ou por supervisão de autoavaliação pelos gestores".

Existência de PAD/Sindicância

Quantidade por tipo (denúncia /pad e sindicância)

No início da elaboração do PAINT, por meio do sistema de correspondência, enviar solicitação para Ouvidoria e Corregedoria, em correspondências distintas nos seguintes termos:

> No intuito de elaborarmos a Matriz de Riscos, a qual subsidiará o Plano Anual de Auditoria Interna - PAINT/20xx, peço a gentileza de encaminhar a esta Audin, a relação de Denúncias, Processo Administrativo Disciplinar - PAD e Sindicâncias, registrados nos exercícios X e Y (até o momento), contendo informações relativas ao órgão, assunto, objetivo e providência adotada.
>
> Conforme arquivos enviados em exercícios anteriores, ressaltamos a necessidade de a relação conter a descrição dos fatos (sem informações relativas ao denunciante/denunciado e empregados envolvidos em PAD ou sindicâncias). Tais informações são necessárias para que possamos classificar os procedimentos de acordo com os processos da Cadeia de Valor do Serpro.
>
> Expectativa de recebimento: xx/xx/20xx

Com base na informação recebida e descrição dos fatos, efetuar classificação dos PAD's, Sindicâncias e denúncias e os respectivos processos da cadeia de valor envolvidos.

Pontuação

Inserir pontuação conforme tabela abaixo:

PAD / SINDICÂNCIA / DENÚNCIA	ESCALA
5	Existência de PAD
3	Existência de denúncia
1	Existência de denúncia (sem PAD ou sindicância associados)

Relação de Sistemas

Sistemas internos que suportam o processo

Os gerentes de departamento da Audin deverão informar a relação dos principais sistemas que suportam o processo. Ex: processo de folha de pagamento: sistema SGP; sistema FCT.

Sistemas de clientes relacionados a atividade fim

O (a) Gerente do Departamento de Auditoria em Tecnologia da Informação e Negócios deverá informar a relação dos sistemas de clientes mais críticos relacionados ao processo. Ex: Dívida Ativa - SIDA; Pucomex - Balança Comercial; eSocial.

Pontuação

Preencher conforme a escala:

SISTEMA	ESCALA
5	Não auditado
3	Auditado e com fragilidades apontadas
1	Auditado e sem fragilidades apontadas

Essa pontuação de sistemas internos ou sistemas de clientes envolvidos será utilizada a partir do PAINT 2023 como agravante de impacto, visando o cálculo do nível de riscos final.

Nível de Risco Audin Agravado =H18*K18
H é o impacto avaliado pela Audin e K é a probabilidade agravada

6.1.3.2.3 Avaliação riscos (Alta Administração)

O bloco relativo à avaliação de riscos pela Alta Administração contempla a Expectativa da Alta Administração como fator de probabilidade.

Fatores de Risco - Probabilidade
Expectativa da Alta Administração - Riscos Estratégicos

Para preenchimento desta coluna, são consideradas as respostas dadas pelos Conselheiros de Administração e Fiscal, membros do Coaud e Diretores no formulário encaminhado pela Audin com o objetivo obter expectativas e visão da Alta Administração do Serpro quanto aos riscos estratégicos, processos, projetos e serviços específicos da empresa que julgam ser relevantes e críticos para atuação da auditoria interna no exercício seguinte.

Probabilidade/Pontuação
Para efetuar a pontuação, utilizar a seguinte escala:

NÚMERO DE CITAÇÕES	VALOR*
> 2	4
2	3
1	2
0	1

* Não atribuído o valor 5 para evitar viéses, visto que nos blocos anteriores (gestor e Audin) é exceção atribuir probabilidade máxima de ocorrência do risco (quase certo). De todo modo, agravantes aplicados posteriormente podem aumentar a pontuação

Fatores de Risco - Impacto Estratégico

Objetivos Cobit 2019

Indicar na célula código e título dos objetivos COBIT 2019 associados ao processo.

Pontuação

1 - Associado aos 12 Objetivos priorizados 2021

0 - Não associado

Fatores e Riscos GTAG 11

O GTAG 11 deve ser utilizado para desenvolver o Plano de Auditoria de TI. (link) Na elaboração do plano de auditoria de TI, podem ser consultados também outros "PRACTICE GUIDES - GTAG (Global Technology Auditor Guide)" - (Guias Práticos de Auditoria de Tecnologia, tais como: Business Continuity Management (Previously GTAG 10) (link); Riscos e Controles de Tecnologia da Informação (link). A lista encontra-se publicada no site do IIA (link) Para preenchimento desta coluna, indicar na célula descrição do Risco GTAG 11 associado ao processo.

Pontuação

1 - Associado aos Riscos do GTAG 11

0 - Não associado

	GLOBAL TECHNOLOGY AUDIT GUIDE - GTAG 11	PONTUAÇÃO
Fatores do Ambiente de TI que apoiam os riscos GTAG 11	(i) O grau dos sistemas e a centralização geográfica (distribuição dos recursos de TI) (ii) As tecnologias implantadas. (iii) O grau de customização. (iv) O grau de formalização de políticas e padrões da empresa. (v) O grau de regulamentação e de conformidade. (vi) O grau e o método de terceirização. (vii) O grau de padronização operacional. (viii) O grau de confiança na tecnologia.	1 - Sim 0 - Não
Riscos GTAG	(a) Disponibilidade, (b) Confidencialidade (c) Impacto Financeiro (d) Integridade (e) Mudanças na Unidade de Auditoria Interna (planejamento, universo auditável) (f) Qualidade dos Controles Internos	Processo auditado há mais de 3 anos

Relação c/ Ativ. Fim

Relação com Projeto Estratégico

Projeto Estratégico - Pontuação

Relação com PEE

Relação c/ PETI / PDTI

Relevância Estratégica

Interação com Cliente

Impacto na Imagem

Obrigação Legal

Preencher itens conforme escala abaixo:

CRITICIDADE DE PROCESSOS - INFORMAÇÕES DA SUPOG		PONTUAÇÃO
Relação com Atividade Fim	Processos Finalísticos	1 - Sim 0 - Não
Relação com Planejamento Estratégico Empresarial (PEE)	Processos vinculados diretamente a objetivos ou direcionadores do PEE	1 - Sim 0 - Não
Relação com Plano Estratégico de Tecnologia da Informação (PETI) e Plano Diretor de Tecnologia da Informação (PDTI)	Processos vinculados à estratégia de TI da empresa	1 - Sim 0 - Não
Relevância Estratégica	Processos com relevância estratégica, de acordo com a visão dos avaliadores (avaliação da DIRETORIA por intermédio da COADM)	1 - Sim 0 - Não
Interação com Cliente	Processos com interação entre empresa e cliente (Ouvidoria, Atendimento ao cliente, CSS, etc.)	1 - Sim 0 - Não
Impacto na Imagem	Processos que afetam diretamente a imagem da empresa	1 - Sim 0 - Não
Obrigação Legal	Obrigação legal registrada	1 - Sim 0 - Não

Impacto Estratégico =M25+O25+R25+SOMA(T25:Z25)

O score de Impacto Estratégico é o simples somatório da pontuação relacionada a Objetivos Cobit 2019 (M), Fatores e Riscos GTAG 11 (O), Relação c/ Ativ. Fim (R); e o somatório dos valores obtidos referentes a: Projeto Estratégico - Pontuação; Relação com PEE; Relação c/ PETI / PDTI; Relevância Estratégica; Interação com Cliente , Impacto na Imagem e Obrigação Legal (T até Z)

Impacto Estratégico Normalizado ARRED(1+4*AA25/MÁXIMO(AA25:AA202);0)

Com o objetivo de trazer o resultado para uma escala comum de probabilidade, de 1 a 5, sem distorcer as diferenças nos intervalos de valores, efetuar a normalização da pontuação do score por meio da fórmula indicada. O "AA" nesta fórmula representa o score do Impacto Estratégico.

Explicando: a função máximo procura o maior valor do Impacto Estratégico e leva proporcionalmente a uma escala de 1 a 5. Processos pouco relacionados aos fatores citados receberão score de impacto estratégico 1 e os mais relacionados receberão score 5.

Risco Emergente

Nível de Risco Risco Regulatório

Nível de Risco Mudança no Processo

Os riscos emergentes e regulatórios decorreram da sistematização no DAP da pesquisa pela Audin em fontes externas, considerando o julgamento profissional do titular da Auditoria Interna. Antes de iniciar a pontuação de tais colunas, é necessário realizar uma revisão dos riscos considerados e da escala utilizada. Para elaboração do PAINT 2022, foi considerado o seguinte:

RISCOS REGULATÓRIOS, RISCOS EMERGENTES, MUDANÇAS NO PROCESSO	CATEGORIA	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO
Cybersecurity (aumento de ataques, ambiente de TI híbrido on site/nuvem e domiciliar, ramsonware as a service, cyberextortion pessoal ou de propriedade intelectual)	Riscos Emergentes - Externos	3	5	15
Pós-pandemia *(retenção de talentos, disparidade no tratamento de empregados por regime remoto/presencial/híbrido ou por vacinação, uso indevido de dados médicos dos empregados, alterações culturais irreversíveis, inadaptabilidade do modelo de negócios legado, concorrentes nato-digitais com modelos de negócios hiperescaláveis com baixo custo, sustentar NPS de clientes, Parcerias/aquisições/Joint Ventures, desemprego interno pela digitalização de serviços, ciclo contínuo de novas ondas e lockdowns, pressão do triângulo para fraude: oportunidade com o remoto, pressão por resultados com menos recursos, racionalização pelas disparidades)*	Riscos Emergentes - Externos	3	3	9
Descontinuidade de fornecedores *(Interrupção, concentração e re-shoring devido aos motivos anteriores ou Eventos climáticos extremos)*	Riscos Emergentes - Externos	2	2	4
Implantação do 5G	Riscos Emergentes - Externos	2	3	6
ESG como *Hype (Overselling, Underestimating, Greenwashing)*	Riscos Emergentes - Externos	3	2	6
Redução da arrecadação *(Teto de gastos e contingenciamento)*	Riscos Emergentes - Externos	3	3	9
Desestatização do Serpro *(tratamento inadequado de dados sigilosos ou sensíveis; instabilidade, interrupção, sabotagem ou perda de conhecimentos críticos dos sistemas estruturantes do Estado, lock in à empresa adquirente)*	Riscos Emergentes - Serpro	2	4	8
Indisponibilidade Elétrica	Riscos Emergentes - Serpro	2	4	8
Privacidade e Proteção de Dados (ANPD)	Regulatório	3	4	12
Limitações do período eleitoral (eventos e patrocínios)	Regulatório	3	3	9
Normas de Saúde Suplementar (ANS)	Regulatório	2	3	6
Auditoria-Fiscal do Trabalho (ME)	Regulatório	2	3	6
Responsabilização de Gestores e Administradores (TCU)	Regulatório	2	3	6
Normas de Previdência Complementar (PREVIC)	Regulatório	2	2	4
Diretrizes de Governança para Estatais (SEST)	Regulatório	2	2	4
Alterações de fluxos, áreas, competências, normas	Mudança no processo	2	2	4

O Nível de riscos é sempre o produto entre probabilidade e impacto.

Fatores de Riscos (Score) =AD25+AF25+AH25

Corresponde à visão de Risco Emergente (AD), Risco Regulatório (AF) e Mudança no Processo (AH) como fatores agravantes do nível de risco estratégico. O score é calculado como o simples somatório desses três fatores.

Nível de Risco Ajustado =SE(AI25>MED($AI$25:$AI$202);I25+1;I25)

Se o score de Fatores de Riscos (AI) é maior que a média (MED), agravar o Nível de Risco Normalizado (I) somando 1.

6.1.3.2.4 Priorização processos cadeia de valor do Serpro

Após o cálculo dos três blocos acima citados, inserir as pontuações conforme colunas abaixo a fim de ao final aplicar a média ponderada, fazer a classificação em ordem decrescente do nível de risco e plotá-los no mapa de calor.

Probabilidade (GESTOR)
Informa a probabilidade original avaliada pelo gestor no Archer, correspondendo ao resultado da coluna "Pontuação - Probabilidade Atual" - aba I. Avaliação de riscos (GESTOR)

Impacto (GESTOR)
Informa o impacto original avaliado pelo gestor no Archer, correspondendo ao resultado da coluna "Pontuação - Impacto Atual" - aba I. Avaliação de riscos (GESTOR)

Avaliação de Riscos (GESTOR)
Informa o resultado final agravado do nível de riscos avaliado pelo gestor, correspondendo ao resultado da coluna "Nível de Risco Atual Agravado" - aba I. Avaliação de riscos (GESTOR)

Coeficiente Agravante (GESTOR) =K12/(H12*I12)
Corresponde ao cálculo do coeficiente agravante, obtido pela razão entre o resultado final agravado do nível de riscos avaliado pelo gestor (K) e o produto da avaliação inicial pelo gestor de probabilidade (H) e impacto (I).

Probabilidade (AUDIN)
Informa a probabilidade original avaliada pela equipe de auditoria, correspondendo ao resultado da coluna "Pontuação - Probabilidade Atual" da aba: II. Avaliação de riscos (AUDIN)

Impacto (AUDIN)
Informa ao impacto original avaliada pela equipe de auditoria, correspondendo ao resultado da coluna "Pontuação - Impacto Atual" - aba II. Avaliação de riscos (AUDIN)

Avaliação de Riscos (AUDIN)
Informa o resultado final agravado do nível de riscos avaliado pela equipe de auditoria, correspondendo ao resultado da coluna "Nível de Risco Audin Agravado" - aba II. Avaliação de riscos (AUDIN)

Coeficiente Agravante (AUDIN) = O12/(L12*M12)
Corresponde ao cálculo do coeficiente agravante, obtido pela razão entre o resultado final agravado do nível de riscos avaliado pela equipe de auditoria (O) e o produto da avaliação inicial pela Audin da probabilidade (L) e do impacto (M).

Probabilidade (Alta Admin.)
Informa a probabilidade original atribuída com base no número de citações pela Alta Administração, correspondendo ao resultado da coluna "Probabilidade" da aba: III. Avaliação riscos (Alta Adm)

Impacto (Alta Admin.)

Informa o Impacto Estratégico Normalizado calculado com base nos fatores de risco antes detalhados, correspondendo ao resultado da coluna "Impacto Estratégico Normalizado" da aba: III. Avaliação riscos (Alta Adm)

Avaliação de Riscos (Alta Admin.)

Informa o resultado final agravado do nível de riscos considerando a visão da Alta Administração e os fatores de riscos citados, correspondendo ao resultado da coluna "Nível de Risco Ajustado" - aba: III. Avaliação riscos (Alta Adm)

Coeficiente Agravante (Alta Admin.) =S12/(P12*Q12)

Corresponde ao cálculo do coeficiente agravante, obtido pela razão entre o resultado final agravado (S12) considerando a visão da Alta Administração e os fatores de riscos citados, dividido pelo produto da avaliação inicial de probabilidade (P) com base nas citações pela Alta Administrações e do impacto com base nos fatores de impacto estratégico (Q).

Resultado

Probabilidade Ponderada

Resultado obtido por meio da fórmula: =(H12*0,25)+(L12*0,35)+(P12*0,4), onde "H" = Probabilidade (GESTOR) multiplicada pelo peso gestor = 25% + "L" = Probabilidade (AUDIN) multiplicada pelo peso Audin = 35% + "L" = Probabilidade (Alta Admin.) multiplicada pelo peso Alta Admin. = 40%.

Impacto Ponderado

Resultado obtido por meio da fórmula: = (I12*0,25)+(M12*0,35)+(Q12*0,4), onde "I" = Impacto (GESTOR) multiplicado pelo peso gestor = 25% + "M" = Impacto (AUDIN) multiplicado pelo peso Audin = 35% + "Q" = Impacto (Alta Admin.) multiplicado pelo peso Alta Admin. = 40%.

Média Ponderada

Resultado obtido por meio da fórmula: =(K12*0,25)+(O12*0,35)+(S12*0,4), onde "K" = resultado da Avaliação de riscos (GESTOR) multiplicado pelo peso gestor = 25% + "O" = resultado da coluna "Avaliação de riscos Audin" multiplicado pelo peso Audin = 35% + "S" = Resultado da Avaliação de riscos (Alta Admin.) multiplicado pelo peso Alta Admin. = 40%.

Coeficiente Agravante

Resultado obtido por meio da fórmula: =Y12/(T12*U12), onde "Y" = resultado da média ponderada dos resultados Avaliação de riscos - Gestor, Audin e Alta Administração; "T" = probabilidade ponderada e "U" = Impacto ponderado.

Probabilidade Agravada

Resultado obtido por meio da fórmula: =T12*RAIZ(V12), onde "T" = probabilidade ponderada e "V" = coeficiente agravante.

Impacto Agravado
Resultado obtido por meio da fórmula: =U12*RAIZ(V12), onde "U" = impacto ponderado e "V" = coeficiente agravante.

Mapa de Calor (AUX)
Esses são campos auxiliares para plotar os mapas de calor separando o que foi priorizado para o PAINT, do que ficou de fora. Assim, os níveis de riscos são agrupados entre duas séries: Escopo e Não escopo.

Priorizado PAINT
Probabilidade Agravada
Informa o resultado da coluna Probabilidade Agravada.

Não Escopo (Impacto) =SE(AC12="Não";X12;)
Se não priorizado para o PAINT (AC=NÃO), preenche com o impacto agravado (X). Caso contrário (se priorizado), deixa zerado.

Escopo (Impacto) =SE(AC12="Sim";X12;)
Se não priorizado para o PAINT (AC=Sim), preenche com o impacto agravado (X). Caso contrário (se não priorizado), deixa zerado.

Priorização PAINT 2022 Motivação

Após a classificação dos processos em ordem decrescente (resultado da coluna Y), os gerentes devem efetuar uma análise considerando a capacidade operacional disponível e preencher as colunas: Priorização PAINT 2022 e Motivação. A motivação deve ser suficiente para explicar o escopo e não escopo do PAINT.

Desta forma, considerando a capacidade instalada disponível, a Audin apresenta a proposta de trabalhos selecionados para o exercício 2022, bem como, ressalta que há um rol de outros trabalhos, denominado *backlog*, o qual será considerado no processo de revisão do PAINT/2022 ou de preparação do PAINT/2023.

6.1.4 Dimensionamento da Capacidade Operacional

No início da elaboração do planejamento anual deve ser aberta uma planilha denominada: PAINT xxxx - Proposta Capacidade Operacional. A primeira aba desta planilha, denominada: Capacidade Operacional, deve conter: relação de empregados da Audin por departamento; tabela com a quantidade de horas úteis disponíveis tanto para jornada de 8 horas, quanto para jornada de 6 horas, se houver na data de elaboração do PAINT, empregados que possuam essa jornada. O conceito de horas úteis abrange o total de dias no ano menos a quantidade de sábados, domingos e feriados nacionais, menos 22 dias úteis de férias e 06

dias de Abono Social (APPD). Este último é estabelecido no ACT, sendo necessária a confirmação no acordo vigente. A quantidade de horas úteis disponível para cada departamento é o somatório da quantidade de analistas multiplicada pelas horas úteis + as horas úteis do gerente de departamento.

a) Horas disponíveis para monitoramento de recomendações: a Audin encaminha a cada quadrimestre, uma posição relativa as recomendações da Auditoria Interna, CGU e TCU, para Diretoria Executiva, Conselhos de Administração e Fiscal e COAUD. Desta forma, em que pese o monitoramento ocorrer ao longo dos trabalhos de auditoria e, considerando a periodicidade de informações acima descrita, devem ser destinadas a atividade de monitoramento: 8 horas, durante 5 dias, 3 vezes ao ano por auditor, o que totaliza 120 horas de monitoramento por auditor por ano.

b) Horas disponíveis para treinamento: a CGU recomenda, por meio da IN SFC nº 3/2017 e Manual de Orientações Técnicas - MOT, a previsão de, no mínimo, 40 horas de capacitação para cada auditor interno governamental, incluindo o responsável pela Unidade de Auditoria Interna.

c) Horas disponíveis para serviços de avaliação e consultoria, Gestão Interna, Melhoria da Qualidade, outros: para facilitar a correta alocação dos recursos, deve ser aberta uma aba para cada departamento e nesta, especificada a relação dos recursos com a distribuição das horas entre: treinamento, monitoramento de recomendações e demais serviços.

6.1.5 Seleção dos objetos auditáveis e elaboração da proposta de PAINT

Com base na matriz de riscos do PAINT e considerando a capacidade operacional disponível, deve ser feita a seleção dos objetos auditáveis e elaborada a proposta de PAINT, a qual será apresentada a Diretoria Executiva por meio de reunião e Comitê de Auditoria (COAUD).

Após a apresentação da proposta de PAINT ao COAUD e realizado os ajustes por ventura solicitados pelo Comitê, o PAINT é enviado para CGU. Conforme previsto na instrução técnica da CGU que define o conteúdo mínimo do PAINT, a proposta de PAINT deve ser encaminhada à respectiva unidade de supervisão técnica até o último dia útil do mês de novembro do exercício anterior ao de sua execução.

A CGU tem o prazo máximo de 15 (quinze) dias, a contar do recebimento da proposta de PAINT para enviar sua manifestação. A ausência de manifestação formal no prazo estipulado não impede a adoção das providências necessárias à aprovação interna do PAINT pelo Conselho de Administração.

A impossibilidade de atendimento às recomendações emitidas pela CGU sobre o PAINT deve ser justificada por ocasião de seu encaminhamento definitivo àquela Controladoria.

6.2 Comunicação e aprovação do Plano de Auditoria Interna

O PAINT deve ser aprovado pelo conselho de administração antes do início do exercício a que se refere. Desta forma, no início do processo de elaboração do plano, já verificar o calendário de reuniões do Conselho de Administração a fim de verificar a data em que a proposta de PAINT com a manifestação da

CGU deve ser enviada para aprovação pelo Colegiado. O envio da proposta do PAINT, deve acompanhar a minuta de voto e apresentação contendo os principais pontos da proposta de PAINT. O PAINT aprovado pelo Conselho de Administração deve ser encaminhado à CGU até o último dia útil do mês de fevereiro do ano a que se refere. Deve ser solicitada publicação do PAINT na página do Serpro, à área responsável pelo portal de transparência, no prazo de 30 dias após a aprovação, ressalvadas as informações sigilosas previstas em lei.
O PAINT aprovado deve ser compartilhado, também, com a Superintendência de Controladoria – SUPCO, para reserva e liberação dos recursos aprovados; Superintendência de Educação - SUPED em função dos treinamentos aprovados; Superintendência de Controles, Riscos e Conformidade – SUPCR e Superintendência de Organização, Processos e Projetos – SUPOG, em função da estruturação dos planos de riscos e agenda de melhoria de processos, as quais tem como insumo o Plano Anual da Auditoria Interna. Vale ressaltar que o PAINT publicado na página do Serpro pode ser acessado por todas as áreas internas e externas à organização.

6.3 Cadastramento do Plano Anual de Auditoria Interna - PAINT no Sisaudit

A fim de viabilizar o início dos trabalhos no ano subsequente ao da aprovação do PAINT, este precisa ser cadastrado no Sisaudit. Para efetuar o referido cadastro, segue o passo a passo a ser realizado pelo Departamento de Assessoramento a Auditoria Interna e Externa (AUDIE), provavelmente no início do mês de dezembro. Inserir os processos da Cadeia de Valor - Arquitetura de Processos vigente no sistema de auditoria (link) Planejamento -> Processos auditáveis do Sisaudit. Excluir os processos que não estiverem mais vigentes. Atualizar os processos vigentes, alterando nome, objetivo, número do processo, unidade de auditoria responsável, gestor do processo, se necessário. Inserir os novos processos, se houver. Caso o processo esteja obsoleto, deve ser excluído ou colocado como inativo no Sistema de Auditoria.

Neste cadastramento:
Incluir/preencher o campo Nome conforme nome e código do processo constante do Sistema Corporativo de Processos; informar no campo Descrição, o número do processo e objetivo do processo conforme Sistema Corporativo de Processos.

O campo auditoria obrigatória deve ser preenchido com “SIM” somente se for auditoria naquele processo por força de lei/normativa.

O campo unidade de auditoria deve ser preenchido com o Departamento de Auditoria que será responsável pela auditoria no processo.

O campo Gestor do Processo deve conter a informação da lotação do gestor do processo, preferencialmente, até o nível de Superintendência. Esta informação é obtida no Sistema Corporativo de Processos.

O campo executor deve ser preenchido com a informação igual à preenchida no campo Gestora do Processo.

O campo Gestor Tático, recebe a lotação até a Superintendência do Gestor do Processo.

O campo Gestor Estratégico é preenchido com a Diretoria do Gestor do Processo. Clicar em Adicionar.

No campo Componente Selecionado deve existir somente uma linha com a informação dos executores, atuais.

Clica em salvar e preencher o campo comentário com a informação do que foi realizado, nome do gestor do processo e seu departamento (informações obtidas no Sistema Corporativo de Processos). Em seguida, Salvar.

No link, Planejamento-> Fatores de Risco, verificar se os fatores de riscos permanecem os mesmo que estão cadastrados. Se sim, Inclui. Se não, efetua a alteração e prossegue com a inclusão. Selecionar os fatores de risco conforme aparecem na Matriz de Riscos do PAINT, depois incluir o critério de classificação.

No link, Planejamento - > cria o planejamento do ano seguinte. Clica em Editar, na aba Quadro de Horas: Em força de trabalho, seleciona o tipo, a praça, a quantidade respectiva de cada e horas úteis por ano. Conforme Capacidade Operacional calculada e registrada no PAINT.

Estes valores acima que serão cadastrados já devem ser o líquido (já abatidos de férias/appd/feriados), ou seja, não descontar estes itens dentro do sisaudit.

Em “Outras Atividades”, descontar as horas de capacitação (40horas por empregado), tanto para Hora de Auditoria quanto Hora de Supervisão. Descontar, também, HH do Auditor Interno (CAE).

Descontar, também, as horas de Monitoramento de Recomendações por empregado.

O total final deve bater com o PAINT aprovado.

Consultar sempre o planejamento do ano anterior para verificar como foi o cadastramento, para fins de orientação.

Na aba Elaboração do planejamento, inserir os fatores de riscos e preencher cada fator com os valores da Matriz de Riscos do PAINT. Ao final, clica em definir matriz de planejamento. Posteriormente, agendar questionário.

Enviar o questionário. Na tela inicial do Sistema de Auditoria (após clicar na logo do Sistema), clicar em Batch envio questionário. Na Matriz de Risco, encerrar o prazo de resposta do questionário.

Em seguida, ir em Elaboração do planejamento e excluir os processos que não foram selecionados para serem auditados no ano seguinte. Depois, incluir o HH de auditoria* e supervisão* de cada processo conforme capacidade operacional preenchida pelos Gerentes de Departamento para cada processo.

Sempre verificar se está conforme o PAINT do ano em questão. Quando os Gerentes finalizarem a capacidade operacional, verificar se o saldo final de auditoria e supervisão é igual ao valor calculado pela área responsável pela elaboração do PAINT.

Clicar em cada processo e incluir o Objetivo/Escopo/Conhecimentos Específicos/ Riscos.

Gerar o planejamento.

Carregar o PAINT versão definitiva para dentro do Sistema de Auditoria como anexo.

Ao tentar imprimir este PAINT carregado, o sistema abre um arquivo .rtf, este deve ser salvo com a extensão para .pdf, assim o arquivo abre normalmente.

Em seguida, aguardar a aprovação do PAINT pelo Auditor Interno (CAE).

(*) ponto crítico que demanda atenção durante o cadastramento!!

No item do Sisaudit "Programa de Auditoria Padrão" (link) adicionar o arquivo: "Matriz de Riscos - PAINT 20XX" e clicar em salvar. Este arquivo só deve ser carregado no sisaudit depois que o PAINT do exercício seguinte for aprovado pelo titular da Auditoria Interna para que não conste dos trabalhos em andamento.

6.4 Revisão do Plano de Auditoria Interna

O plano anual de atividades de auditoria interna é elaborado considerando a priorização de trabalhos com base na maior classificação dos riscos associados aos processos constantes da cadeia de valor, levando em conta a capacidade operacional da Auditoria Interna.
Trabalhos não incluídos são registrados em backlog para subsidiar eventual repriorização futura. Em função de eventuais alterações na estratégia da organização, mudanças no ambiente regulatório, riscos emergentes ou outra alteração relevante, o plano anual poderá ser revisto de ofício e submetido à apreciação do Comitê de Auditoria e aprovação pelo Conselho de Administração.
A avaliação quanto a eventual necessidade de revisão do PAINT deve ocorrer preferencialmente, após o primeiro semestre de execução do PAINT. Neste sentido, deve-se verificar a disponibilidade de recursos disponíveis, backlog de trabalhos previstos durante a elaboração do PAINT e contexto organizacional ou casos de força maior que venham a impactar na execução do PAINT no último semestre.

6.5 Acompanhamento do Plano Anual de Auditoria

A execução do PAINT é acompanhada de forma contínua por meio do Sistema de Auditoria – Sisaudit (link), módulos: "execução" e "acompanhamento" e também por meio de painel no Qlik sense (link) - "PAINT - trabalhos" e "Recomendações, Solicitações e Notas de Auditoria".
Mensalmente é reportado ao Comitê de Auditoria – Coaud e ao Conselho Fiscal a execução do PAINT. Quando da conclusão dos relatórios de auditoria, estes são enviados para o Coaud e Conselho Fiscal na íntegra, à CGU, também na íntegra por meio do sistema e-Aud e após apresentação ao Conselho de Administração. Por solicitação deste, é informado um resumo com os principais pontos de cada trabalho.

6.5.1 Reporte mensal aos Conselhos e Comitê de Auditoria

Objetivo: Informar aos Conselhos de Administração e Fiscal e Comitê de Auditoria sobre o andamento dos processos do Serpro junto aos Órgãos de Fiscalização e Controle, documentos expedidos e recebidos bem como, posicioná-los sobre a execução do plano de auditoria interna e resultados dos trabalhos.

Meio: Material disponibilizado aos Conselhos e COAUD por meio do SerproDrive;

Frequência: Mensalmente, conforme calendário de reunião dos colegiados. Os documentos e informações devem ser disponibilizados às secretarias dos Colegiados com antecedência de 7 dias úteis da data da primeira reunião agendada, a qual normalmente é a do Conselho de Administração.

Atores internos: Comitê de Auditoria (COAUD); Conselho de Administração e Conselho Fiscal.

Responsável: AUDIE - Departamento de Assessoramento a Auditoria Interna e Externa.

Entregas:
1- Paper Executivo – Conselho de Administração;
2 - Planilha: 01-Acompanhamentos_AUDIN_mês_ano – Conselho de Administração;
3 - Sumário Executivo – CF_ mês_ano – Conselho Fiscal;
4 - Anexo detalhado - Informações do Controle Interno e Externo mês_ano – Conselho Fiscal;
5 - Acompanhamento da execução do PAINT e recomendações da Auditoria Interna e Órgãos de Controle_reunião dia_mês_ano - Coaud;
6 – Minuta da Ata CF – Conselho Fiscal;
7 – Informação lista participantes das reuniões

Atividades pós-reuniões:

1 – Enviar relatórios de auditoria para CGU por meio do e-Aud
2 – Acompanhar publicação das atas de reuniões para ver se há demandas para Audin;
3 – Acompanhar retorno do feedback dos auditados

Detalhamento por entregas:

1- Paper Executivo – Conselho de Administração

O paper executivo é um documento Word que a Secretaria do Conselho de Administração compartilha com a Auditoria Interna para que sejam preenchidos os principais pontos de atenção que serão informados ao Conselho de Administração durante a reunião.

Não há um prazo específico para que a secretaria do CA compartilhe o documento com a Audin. Normalmente isso é feito na semana que antecede o envio do material e há em torno de 1 ou 2 dias úteis para que o preenchimento seja feito.

Este documento é utilizado para fechamento da pauta com o Presidente do Conselho.

Características do documento:

- Deve conter os pontos mais importantes do material que será apresentado pela Audin naquele mês;
- O resumo de cada item deve ser claro e objetivo;
- Os pontos informados não devem ultrapassar duas páginas do paper;
- Deve ser validado pelo Auditor-Geral antes do envio a secretaria do CA.

2 - Planilha: 01-Acompanhamentos_AUDIN_mês_ano – Conselho de Administração;

Todos as informações que serão prestadas aos Conselhos de Administração e Fiscal precisam ser cadastradas no Info.Audin (link).

Após realizar todas as atualizações necessárias no referido sistema, ir na opção "Demanda Extração" – Mês: escolher o mês da reunião – Planilha CA. Os dados que serão gerados numa planilha em excel, devem ser colados na aba "Dados" da planilha "CA – Demandas" que se encontra disponível na pasta do OneDrive: AUDIE/Material Conselhos. Após a colagem, deve-se alterar o mês constante na célula: E5.

Verificar se todas as linhas estão aparecendo sem informações cortadas. Se necessário, ajustar a largura das linhas. Para realizar a impressão da planilha que será enviada em formato PDF, selecionar todas as colunas a partir da coluna B, até a G – Linha 1, até a linha final. Arquivo imprimir. Na opção configurar página, escolher Imprimir: Seleção atual – orientação retrato e salvar com o nome: 01-Acompanhamentos_AUDIN_mês_ano.

3 - Sumário Executivo – CF_ mês_ano – Conselho Fiscal;

Todos as informações que serão prestadas aos Conselhos de Administração e Fiscal devem ser informadas no arquivo Sumário Executivo - CF mês_ano. Tal arquivo é sempre salvo na pasta do OneDrive: AUDIE/Material Conselhos/Mês.

Características do documento:

- Deve conter os pontos mais importantes do material que será apresentado pela Audin naquele mês;
- O resumo de cada item deve ser claro e objetivo;
- Deve ser validado pelo Auditor-Geral antes do envio a secretaria do CA.
- O arquivo normalmente é composto de uma sessão destinada aos expedientes da CGU e do TCU e outra destinada à Auditoria Interna, na qual deve sempre ser informado sobre a execução do PAINT.

O gráfico que compõe o Sumário encontra-se disponível no documento: "Acompanhamento PAINT ano".

4 - Anexo detalhado - Informações do Controle Interno e Externo mês_ano – Conselho Fiscal;

O objetivo deste documento é fornecer detalhamento aos itens constantes do Sumário. Caso os Conselheiros desejem conhecer na íntegra os documentos citados no Sumário, poderão avaliá-los com base neste documento.

Os documentos que baseiam cada item do Sumário Executivo do CF, devem ser salvos na pasta OneDrive: AUDIE/Material Conselhos/Mês, para que sejam consolidados em um único arquivo denominado: Anexo detalhado - Informações do Controle Interno e Externo mês_ano.

Para consolidar os documentos, em ordem cronológica e agrupá-los por itens, deve-se abrir uma pasta específica para cada expediente e numerar os documentos à medida em que estes forem sendo produzidos.

Nem todos os documentos precisam constar do anexo. Avaliar os mais representativos e essenciais para o entendimento do item.

5 - Acompanhamento da execução do PAINT e recomendações da Auditoria Interna e Órgãos de Controle_reunião dia_mês_ano - Coaud;

Mensalmente deve ser elaborada apresentação para o Coaud com o seguinte conteúdo mínimo:

Recomendações da auditoria interna em acompanhamento no exercício atual;
Estoque das recomendações da auditoria interna considerando todos os exercícios;
Recomendações - Estoque/com prazo expirado (fora do prazo)
Eficiência (tempo de vida < 12 meses)
Posição sobre as recomendações da CGU e TCU;

O posicionamento deve ser obtido por meio de painéis na ferramenta Qlik (link).

6 – Minuta da Ata Coaud e CF – Conselho Fiscal;

Por solicitação da Secretaria do Coaud e Conselho Fiscal fazer um resumo dos principais pontos abordados pela Auditoria Interna. Em função da publicação das atas, avaliar o conteúdo a ser exposto e fazer uma redação clara e objetiva.

Na minuta da ata do CF sempre inserir um item específico sobre a execução do PAINT.

7 – Informação lista participantes das reuniões

Com base nos itens descritos na pauta das reuniões e, por solicitação da secretaria dos colegiados, informar os gerentes de departamento que deverão participar das reuniões em cada item descrito na pauta. Validar lista com o Auditor Interno antes do envio às secretarias dos colegiados.

7 Relatório Anual de Atividades de Auditoria Interna (RAINT)

O RAINT tem a finalidade de demonstrar a execução dos trabalhos planejados no PAINT, contemplando seus principais resultados com o objetivo de fomentar a melhoria dos processos de governança, de gerenciamento de riscos e dos controles internos da gestão empresarial.

É elaborado anualmente com base na legislação específica da SFC/CGU - PR, a qual define seu conteúdo mínimo. Antes de iniciar a elaboração do RAINT, importante consultar no site da CGU a legislação mais atual sobre o tema (link). Geralmente a CGU solicita:

> I - quadro demonstrativo da alocação efetiva da força de trabalho durante a vigência do PAINT;
> II - posição sobre a execução dos serviços de auditoria previstos no PAINT, relacionando aqueles finalizados, não concluídos, não realizados e realizados sem previsão no PAINT;
> III - descrição dos fatos relevantes que impactaram a execução dos serviços de auditoria;
> IV - quadro demonstrativo do valor dos benefícios financeiros e do quantitativo dos benefícios não financeiros auferidos em decorrência da atuação da UAIG ao longo do exercício, conforme as disposições da Instrução Normativa nº 10, de 28 de abril de 2020, da CGU;
> V - informe sobre os resultados do Programa de Gestão e Melhoria da Qualidade - PGMQ.

A CGU solicita que o RAINT seja comunicado ao Conselho de Administração, porém em virtude do disposto no Estatuto Social do Serpro (link): Art. 16. - XXVI - O Relatório Anual de Atividades de Auditoria Interna (RAINT), deve ser aprovado pelo Conselho de Administração, sem a presença do Diretor-Presidente do Serpro.

O RAINT deve ser enviado à CGU, por meio do sistema e-Aud **(link)** e publicado na página do Serpro (link) até o último dia útil do mês de março do exercício seguinte ao qual se refere, ressalvadas as informações sigilosas previstas em lei.

Observação: Não esquecer de adicionar a declaração de independência e objetividade no RAINT, a exemplo do modelo adotado no RAINT/2021. (link)

8 Auditoria Contínua

A Auditoria Interna do Serpro dispõe de um Departamento de Auditoria Contínua - AUDCN cujas atribuições são:

a) coordenar e executar auditorias contínuas baseadas em dados;
b) implementar metodologia de análise de dados com foco em controle preventivo e auditoria, buscando cooperação com demais instâncias de controle interno ou externo;
c) criar e gerir modelos descritivos, preditivos e prescritivos de dados;
d) gerir e implantar arquitetura para sustentar o uso intensivo de dados com enfoque em gestão preventiva e auditoria;
e) executar ações referentes ao uso de dados na auditoria interna:
    e1) configurar e gerir métricas,
    e2) análise automatizada,
    e3) mineração de dados de interesse da Auditoria Interna; e
f) subsidiar e participar da elaboração dos documentos abaixo, com as informações pertinentes ao seu âmbito de atuação e competência:
    f1) Plano Anual de Auditoria Interna - PAINT,
    f2) Relatório Anual de Atividades da Auditoria Interna - RAINT; e
    f3) Parecer da Auditoria Interna sobre a Prestação de Contas Anual e Controles Internos.

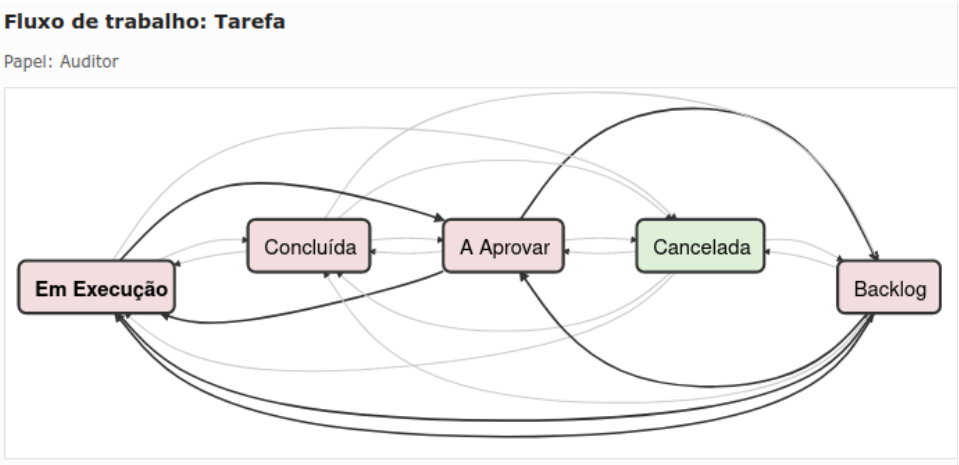
Neste contexto, a AUDCN desempenha um papel fundamental no Programa de Gestão e Melhoria da Qualidade dos trabalhos da Auditoria Interna (PGMQ), suportando todo o processo de monitoramento contínuo dos indicadores da Audin.

8.1 Critérios para a priorização do desenvolvimento de novos indicadores, bem como da pertinência dos que estão em funcionamento.

A demanda inicial para criação de um novo indicador é feita através da criação de uma Subt*arefa* no Redmine AUDIN, no Projeto 2.7. Produtividade -> AUDCN (link), cada departamento da Auditoria Interna possui uma *Tarefa* específica para novos indicadores/trilhas de auditoria, a *Subtarefa* deverá ter como *Pai* esta tarefa:

- AUDAC (link) - https://gestao.audin.serpro/issues/3646
- AUDEP (link) - https://gestao.audin.serpro/issues/3683
- AUDTN (link) - https://gestao.audin.serpro/issues/3106
- AUDPC (link) - https://gestao.audin.serpro/issues/18957
- AUDPC (link) - https://gestao.audin.serpro/issues/18955
- AUDIE (link) - https://gestao.audin.serpro/issues/18956
- AUDCN (link) - https://gestao.audin.serpro/issues/18958

Uma vez registrada no Redmine AUDIN, a *Subtarefa* é submetida ao fluxo abaixo:



No geral, os indicadores possuem 2 categorias:

- Assessoramento - Indicadores utilizados para apoio das equipes e gestores da Auditoria Interna e/ou apoio e publicidade junto aos conselhos e gestores. Normalmente este tipo de indicador é oriundo da AUDIE ou AUDCN, equipes que estão alocadas totalmente ou parcialmente ao subprocesso "12.04.02 - Assessorar Auditoria Interna e auditorias externas"
- Trilhas de Auditoria - Normalmente iniciador é criado no decorrer da execução de um trabalho de auditoria, demandado das áreas realizam Auditoria, alocadas ao subprocesso "12.04.01 - Realizar auditorias".

Uma vez criado a demanda, a AUDCN realiza uma avaliação, visando complementar alguma informação e avaliar as seguintes características:

- Disponibilidade de Informações - Viabilidade de coleta dos dados em bases estruturas e/ou o custo para obter os dados por técnicas de coleta de dados não estruturados.
- Complexidade - Grau de conhecimento das regras de negócio necessário para geração daquele indicador, assim como a demanda computacional de processamento.
- Apresentação - Viabilidade de uma apresentação objetiva que possa ser aferida a eficiência do acompanhamento e agregue valor ao processo.
- Histórico de Dados - Levantamento do histórico e caso não exista avaliação do impacto para validação das regras e coerência do indicador.

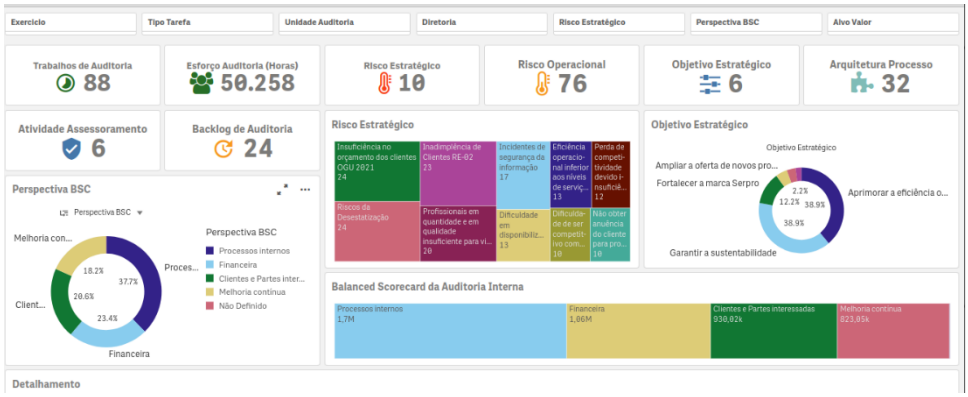
Feito esta avaliação, o indicador é submetido para priorização na reunião gerencial, exceto indicadores simplificados que a AUDCN já possua expertise para criar sem impactar o seu planejamento, neste caso o indicador já é criado durante a fase de avaliação.

No item 8.2 será detalhado o processo de validação e acompanhamento dos indicadores, mas a pertinência da continuidade de um indicador é avaliada na reunião gerencial periodicamente, baseado na análise subjetiva do demandante e usuários no caso de indicadores de assessoramento, no caso do indicador de trilhas de auditoria são utilizados critério objetivos dos resultados aferidos para colocar em pauta a sua pertinência.

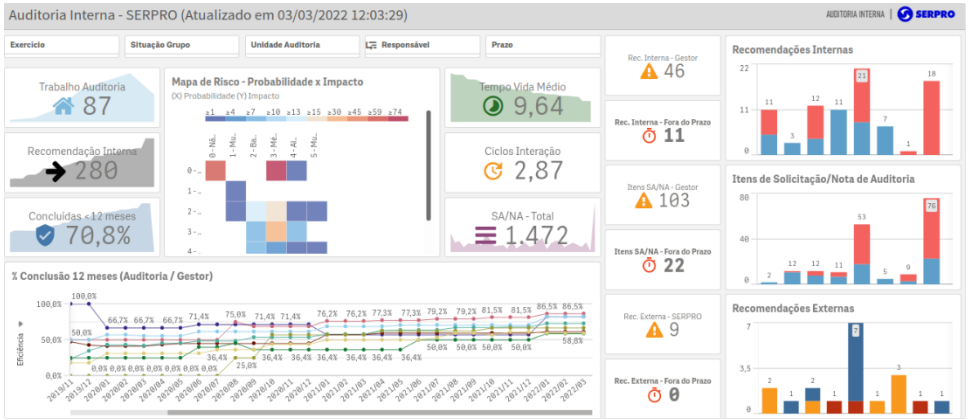
8.2 Validação contínua das regras de negócio, além da periodicidade de avaliação e reporte dos resultados

Indicadores de Assessoramento, normalmente são baseados no SISAUDIT (Sistema Interno de Auditoria Interna) ou Sistemas de Controle Externo (CGU/TCU), sendo uma visão simplificada para os gestores e conselhos, são ajustados constantemente com novas métricas e novas visualizações por todos os envolvidos, são ferramentas fundamentais tanto para acompanhamento de pendências como geração de material para conselhos.

Exemplo de indicadores utilizados para Conselho

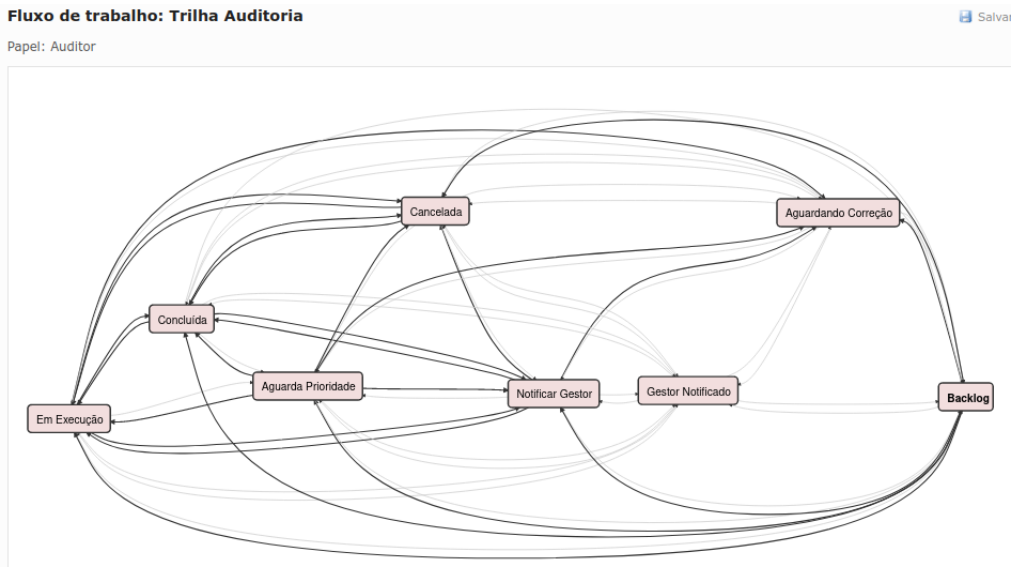


Exemplo de indicador utilizado para acompanhamento da Gestão



Como mencionamos no item 8.1, indicadores de Trilhas de Auditoria normalmente são baseados em testes e/ou recomendações geradas no decorrer da execução dos trabalhos de auditoria, e possuem diversas fontes de dados e regras de negócio especifica.

Apesar desta variabilidade, cada incidência gerada pela trilha do indicador é replicada como uma *issue* no Redmine AUDIN, no Projeto 2.6. Trilha de Auditoria Contínua (link) obedecendo um fluxo próprio dentro do sistema:



Sempre que possível, o responsável pelo indicador pode delegar para sua equipe uma validação subjetiva da incidência podendo ou não interagir com o gestor, e informar um resultado genérico desta análise:

- Não Avaliado - Incidência registrada pela ferramenta de automação, mas não avaliada por nenhum auditor.
- Inconsistência Confirmada - Auditor realizou uma avaliação e confirmou a inconsistência identificada pelo indicador, o gestor será notificado.
- Falso Positivo - Inconsistência na trilha de auditoria, será reportado para AUDCN ajustar o processo de automação.
- Incidência Justificada - Auditor realizou uma análise da incidência e considerou como justificável pode ou não ter interação com o gestor, mas a AUDCN não é envolvida com demandas evolutivas no processo de automação.
- Periodicidade - Qual a periodicidade possível e eficiente o indicador poderá ser gerado.

Todas as incidências são centralizadas no Projeto 2.6. Trilha de Auditoria Contínua (link), sendo que para cada indicador é criado um subprojeto, com a padronização da sua nomenclatura:

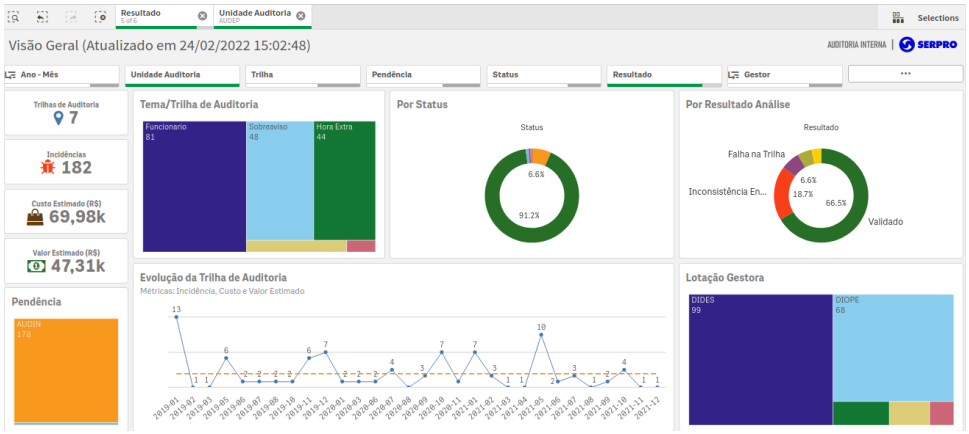
- Departamento Responsável

- Tema do Indicador

- Título da Trilha de Auditoria

Para facilitar a avaliação dos resultados e a pertinência da continuidade dos indicadores durante a reunião gerencial, foi criado um painel com uma visão padronizada de todas as trilhas implementadas e sua avaliação, assim possibilitando análises objetivas para pautar a pertinência da sua continuidade na reunião gerencial como aumentar a transparência internamente na AUDIN dos resultados dos trabalhos baseado em dados.

Painel de Acompanhamento de Trilhas de Auditoria (link)



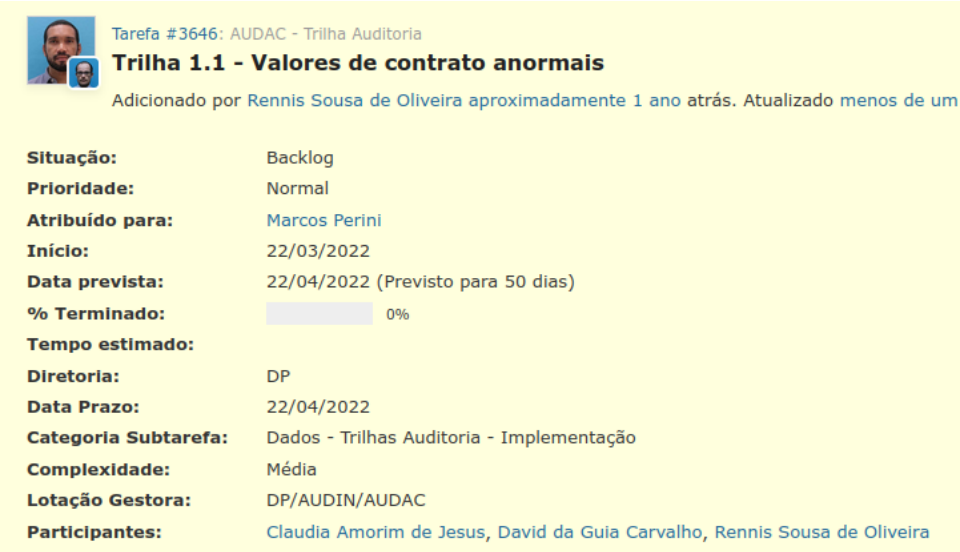
Durante a reunião de avaliação, poderá ser avaliado e/ou ajustado a periodicidade definida na fase inicial de avaliação da trilha. É realizado uma análise geral de todas as trilhas a cada semestre na reunião gerencial ou diretamente com o demandante com a participação da AUDN e do Auditor-Geral.

8.3 Responsáveis pelo acompanhamento dos indicadores e validação contínua das regras de negócio, além da periodicidade de avaliação e reporte dos resultados.

O responsável por acompanhar ou delegar algum membro da equipe é o demandante do indicador, que registrou a Subtarefa no Redmine AUDIN, conforme mencionado no item 8.1. Reforçando, as características do indicador, como regra de negócio, periodicidade continuidade ou não são registradas no Projeto 2.7. Produtividade -> AUDCN (link),

GANTT com as demandas para AUDCN

Exemplo de demanda de trilha/indicador



Tarefa #3646: AUDAC - Trilha Auditoria

Trilha 1.1 - Valores de contrato anormais

Adicionado por Rennis Sousa de Oliveira aproximadamente 1 ano atrás. Atualizado menos de um

Situação:	Backlog
Prioridade:	Normal
Atribuído para:	Marcos Perini
Início:	22/03/2022
Data prevista:	22/04/2022 (Previsto para 50 dias)
% Terminado:	0%
Tempo estimado:	
Diretoria:	DP
Data Prazo:	22/04/2022
Categoria Subtarefa:	Dados - Trilhas Auditoria - Implementação
Complexidade:	Média
Lotação Gestora:	DP/AUDIN/AUDAC
Participantes:	Claudia Amorim de Jesus, David da Guia Carvalho, Rennis Sousa de Oliveira

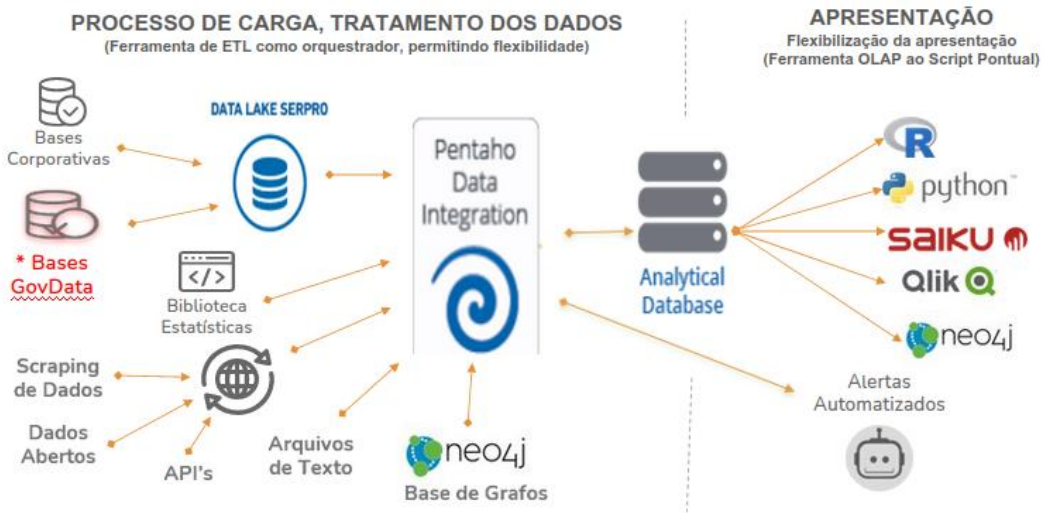
Já a avaliação dos resultados no Projeto 2.6. Trilha de Auditoria Contínua (link) e no Painel de Acompanhamento de Trilhas de Auditoria (link)

Apesar de não necessariamente uma ação prevista no PAINT, caso a consolidação dos resultados das trilhas tenha materialidade suficiente até o último trimestre do ano, é gerado um trabalho de Auditoria Extraordinário, conduzido pela AUDCN com participação dos demandantes dos indicadores de trilhas de auditoria.

8.4 Documentação mínima necessária dos programas/scripts desenvolvidos

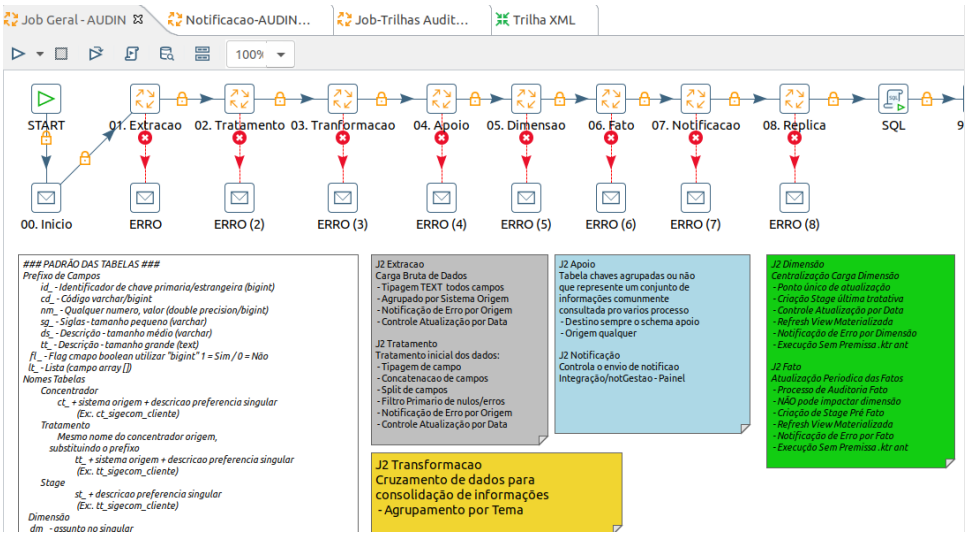
Atualmente a Auditoria Interna do Serpro conta uma robusta arquitetura de dados, com um espaço dedicado dentro do DataLake Corporativo, integrado a diversas ferramentas de apresentação e manipulação de dados.

Arquitetura de Dados Simplificada

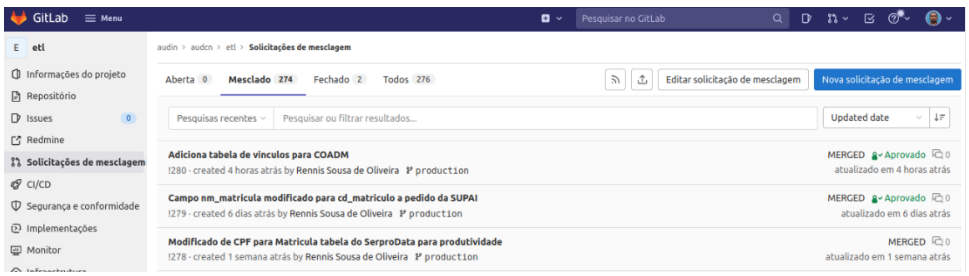


O ponto central para o trabalho de Auditoria Continua seria o fluxo de dados (pipeline) que em nosso caso é feito pela ferramenta de ETL (Pentaho Data Integration) que tem como resultado a base de dados analítica, referência para todo o nosso trabalho, podendo ser apresentado de diversas maneiras. Nesta

ferramenta, cada passo do fluxo de dados é estruturado em Jobs e Transformações que possuem registrados na própria ferramenta as regras de negócio utilizadas.



Utilizamos a ferramenta corporativa GIT (link) para documentar e versionar todas as modificações/inserções de códigos em produção controlando tudo que possa afetar o nosso pipeline de dados, **nenhum código é publicado em produção sem o devido versionamento e comentário**, existe um fluxo do nosso CI/CD (Continuous Integration/ Continuous Delivery) que obriga todos os desenvolvedores, não existe outro caminho para publicação em produção que não seja o GIT. Com isso, complementamos as informações do PDI/ETL com as informações do GIT.



Quando necessário, a AUDCN cria um manual de operação para os Indicadores em conjunto com o demandante, mas uma das metas ao criar o painel é que ele seja autoexplicativo, que o usuário que conheça o negócio consiga naturalmente navegar e utilizar as informações.

9 Sistemas utilizados pela auditoria interna e gerenciamento de acessos.

No desempenho de sua missão, a Audin utiliza o rol de sistemas internos disponibilizados pelo Serpro, conforme relação constante na intranet (link).

O sistema de auditoria utilizado é o Sisaudit (link). Como ferramentas de apoio são utilizados: Redmine (link); Qlik sense (link); Office 365 (link), dentre outros.

O Serpro dispõe de uma norma específica para Gestão de Identidade e Controle de Acesso Lógico aplicada às informações, sistemas e serviços corporativos do SERPRO, visando a
proteção dos ativos de informação contra o acesso não-autorizado - Norma SG 037. (link)
O item "4.2.4 Gerenciamento de Permissões de Acesso" da referida Norma, regulamenta como deve ocorrer o gerenciamento de permissões e acessos a todos os sistemas do Serpro.

> 4.2.4.1 Os usuários devem receber acesso somente aos serviços para os quais tenham sido especificamente autorizados de acordo com os princípios "necessidade de conhecer" e "privilégio mínimo".
> 4.2.4.1.1 O credenciamento de acesso aos sistemas habilitados por padrão (acesso a Rede Local, Ferramentas Colaborativas em Nuvem, Correio Eletrônico, dentre outros) é realizado de forma automática por meio do sistema de gestão de identidade, no momento da inclusão de usuário em sua fonte autoritativa.
> 4.2.4.1.2 A revogação de acesso aos sistemas habilitados por padrão é realizada automaticamente no momento de exclusão de usuários do sistema SGP.
> 4.2.4.2 A concessão e uso de permissões de acesso devem atender, pelo menos, os seguintes requisitos de controle: uso de privilégio mínimo, rastreabilidade e auditabilidade sob responsabilidade do gestor do sistema.
> **4.2.4.3 Cabe a chefia do órgão de lotação do empregado solicitar acesso aos sistemas, aplicações e ferramentas, de acordo com as necessidades estabelecidas pelo exercício da função, conforme as atribuições de competência do empregado.**
> 4.2.4.4 Cabe ao gestor do serviço ou aprovador analisar a justificativa da solicitação realizada de acordo com o item 4.2.4.3, devendo rejeitar, revogar ou aprovar o acesso providenciando a execução da configuração necessária.
> **4.2.4.5 A mudança de lotação de um empregado deverá provocar a revogação dos acessos e das permissões vinculadas.**
> **4.2.4.5.1 Para os casos onde o acesso e suas permissões estão integrados ao sistema de gestão de identidade e acesso corporativo do SERPRO, a revogação será realizada automaticamente no momento da mudança de lotação do empregado.**
> **4.2.4.5.2 Para os demais casos é de responsabilidade da chefia do órgão de lotação de origem do empregado solicitar a revogação do acesso e de suas permissões, respondendo inclusive solidariamente pelo mau uso que o ex-empregado venha a fazer com a permissão remanescente.**

Desta forma, todos os sistemas e ferramentas utilizados pela Audin devem seguir os procedimentos de gerenciamento de acessos previstos na Norma acima citada. Os gerentes de departamento devem, quando da saída de empregados da Audin para outras áreas da Empresa, verificar a relação de sistemas e acessos que o empregado dispunha e solicitar a remoção destes acessos. Adiante seguem exemplos de tratativas para remoção dos acessos. É importante checar, antes do envio, se o gestor responsável pelo sistema permanece o citado ou houve alterações:

SUPGS Bruno Silva <bruno.silva@serpro.gov.br>

Solicito a gentileza de remover o acesso consultivo pleno para os sistemas **ADPAT**, **SIPES** e **SVPC**, haja vista a movimentação do empregado <nome>, matrícula <número>, CPF <número>, para a área <área>.

SUPGP	Leonardo Silveira <leonardo.silveira@serpro.gov.br>

Solicito a gentileza de proceder o cancelamento de acesso com perfil de "Auditor" para o sistema SGP do empregado <nome>, matrícula <número>, CPF <número>, considerando sua movimentação para a área <área>, sendo concedido o perfil padrão de acesso.

DIOPE/COADM	Cleber Teixeira <cleber-alves.teixeira@serpro.gov.br>

Solicito a gentileza de proceder ao cancelamento do acesso ao DMDIOPE - Data Mart Diretoria de Operações, para todas as bases existentes no sistema, haja vista a movimentação do empregado <nome>, matrícula <número>, CPF <número>, para a área <área>.

DIOPE/SUPOP	André Centenaro <andre.centenaro@serpro.gov.br> Bernhard Zanker <bernhard.zanker@serpro.gov.br>

Em observância à norma RE 008, solicito a revogação de impressão corporativa colorida para o empregado <nome>, matrícula <número>, CPF <número>, considerando recente movimentação para a área <área>.

SUPOP	GOVI Controle

1. Centro de Autoatendimento > Solicitar um novo serviço > Administração de Rede Local > Administração de Servidor > **Criação/Alteração de Pastas, Volumes e Permissões**

Considerando a movimentação do empregado <nome> (CPF <número>) para área a área <área>, solicito a gentileza de remover o mapeamento à pasta e subpastas da AUDIN na RLSL, em todos os contextos em que esteja ativo (BSA, SPO, RJO e SEDE).

AUDIN	Sistemas e serviços - e-mail às áreas abaixo

1. Compartilhamento das pastas no **SerproDrive** e na **Lista-Auditores e/ou Lista/Audin**→ AUDIN/AUDIE

Considerando a movimentação do empregado <nome> (CPF <número>) para área a área <área>, solicito a remoção do compartilhamento das pastas no SerproDrive e DiscoRL (Audin) e da lista de auditores do SerproMail.

2. **KANBAN** / **SISAUD** / **SISAUDIT** / Serviço de Acesso Remoto (**SAR**) → AUDIN/AUDAC

Considerando a movimentação do empregado <nome> (CPF <número>) para área a área <área>, solicito a remoção dos acessos aos seguintes sistemas: Kanban, Sisaud, Sisaudit e Serviço de Acesso Remoto (SAR). Solicito, adicionalmente, atualizar o conteúdo do parâmetro "listaResponsaveisTarefaPadrao" da tabela do Sisaudit.

SUPGS	Atair Costa <atair.costa@serpro.gov.br>

Para efeito de gestão de patrimônio, informo que, em virtude da movimentação do empregado <nome> (CPF <número>) para área a área <área>, houve alteração na titularidade da coordenação. Favor direcionar os bens da coordenação para o <nome> (CPF <número>) para área a área <área>.

Caso seja necessária a realização de mais algum procedimento, peço informar.

SUPOG	Processo Decisório <processo.decisorio@serpro.gov.br>

Gostaria de solicitar a gentileza de conceder acesso ao sistema Processo Decisório ao empregado <nome> (CPF <número>, matrícula <número> e e-mail <e-mail>), com o perfil "ConsultaAuditor", para fins de visualização dos documentos, em virtude dos trabalhos de auditoria.

Adicionalmente, a cada 6 meses é feito um levantamento no sistema de auditoria - Sisaudit para avaliação dos habilitados/perfis de acesso com o objetivo de verificação da base e limpeza de usuários indevidos.

Importante ressaltar que além dos empregados da Audin, possuem acesso ao Sisaudit os empregados da Supdg, por responderem pelo desenvolvimento/manutenção do sistema.

Tal procedimento é efetuado conforme roteiro:

1. Acessar sistema Autentikus (https://autentikus.estaleiro.serpro.gov.br/) e acionar a opção RELATÓRIO DE USUÁRIOS no menu, informando como filtro a opção Sisaudit.
2. Na tabela de pesquisa, incluir a informação SAUD na coluna PAPEL e pressionar o botão EXPORTAR. Os dados serão direcionados em planilha, com nome listaUsuarios_SISAUDIT.csv.
3. Abrir a planilha e confrontar os nomes existentes com aqueles afetos ao escopo da Auditoria Interna, registrando os CPFs daqueles indevidos.
4. No Autentikus, acessar a opção PAPEL no menu, preencher com o CPF indicado e selecionar as opções SERPRO como CLIENTE e depois SISAUDIT como SISTEMA para verificar.
5. Todas as caixas apresentadas devem ser desmarcadas, exceto o papel FUNCI (Funcionario), se empregado do Serpro.

Os acessos aos painéis da Audin no Qlik são administrados pela Audcn. Desta forma, solicitações de inclusão/exclusão de usuários devem ser enviados diretamente pelas chefias imediatas ao titular do departamento de auditoria contínua. Demais acessos/remoções a outros painéis, devem seguir os procedimentos definidos pela equipe do Serprodata (link).

Esse procedimento poderá ser simplificado quando a nossa ferramenta de ETL passar a executar rotinas diárias para validar se todos os usuários ativos em perfis específicos para Auditoria Interna pertencem ao quadro Audin.

10 Desenvolvimento Profissional dos empregados da Auditoria Interna

Conforme descrito no item 4.1.5.4 do MOT da CGU: *"A previsão de carga horária mínima de 40 horas de capacitação anual dos auditores internos governamentais visa a permitir o aperfeiçoamento dos seus conhecimentos, de suas habilidades e de outras competências, por meio do desenvolvimento profissional contínuo. Essa capacitação deve se dar preferencialmente com base em um programa de formação e desenvolvimento de recursos humanos e pode incluir cursos formais, seminários, workshops, encontros, visitas técnicas, cursos de pós-graduação, cursos à distância, curso de progressão funcional, treinamento no trabalho, entre outros. Importa destacar ser competência do responsável pela UAIG: identificar as deficiências e as lacunas na formação e no desempenho dos auditores e buscar supri-las por meio de ações como as citadas no parágrafo anterior. Caberá, portanto, também a ele identificar a necessidade de fornecer oportunidades que excedam a carga horária mínima obrigatória, o que é bastante recomendável, sobretudo em decorrência das constantes modificações pelas quais a área de auditoria vem passando, além do surgimento de novas tecnologias, da maior exigência da sociedade em relação à prestação de contas, à transparência, entre outros".*

As orientações para implantação das IPPF trazem parâmetro equivalente para aderência à Norma 1230 – Desenvolvimento Profissional Contínuo, por ser compatível com a educação continuada necessária para manutenção da maior parte das certificações.

10.1 Trilha de Conhecimento da Auditoria Interna

O processo de desenvolvimento da trilha de conhecimento da Auditoria Interna foi iniciado em junho de 2018 com o apoio da Superintendência de Educação. Ela foi estruturada por meio do *software Xmind* e está organizada em eixos temáticos (categorias de assuntos), considerando os processos de trabalho da AUDIN, bem como possíveis agrupamentos do público-alvo das soluções educacionais, conforme exemplo abaixo.

Ao menos anualmente será avaliada a necessidade de atualizar o documento "Trilhas de conhecimento da Auditoria Interna, disponível na página da Audin (link).

10.2 Gerenciamento de desempenho dos empregados

O Serpro dispõe de norma específica para o Gerenciamento de Desempenho dos Empregados - GDES (link). O GDES se aplica a todos os empregados que cumpram os requisitos estabelecidos nos editais que regulamentam o processo. O processo é composto por dois instrumentos: a Avaliação de Competências e a Avaliação de Resultados. O processo ocorre anualmente. O GDES prevê, ainda, a elaboração do Plano de Desenvolvimento Individual – PDI contendo a indicação de ações necessárias para o desenvolvimento profissional do empregado. O PDI é regulamentado e gerido pela área responsável pela Educação Corporativa. Anualmente essa Superintendência divulga edital específico. Para efeito do PDI, considera-se lacuna de desempenho as competências e as metas nas quais o empregado obteve pontuação igual ou inferior a 80,00 (oitenta) pontos.

10.3 Mapeamento das lacunas de Conhecimento

O mapeamento das lacunas de conhecimento busca identificar os gaps de conhecimentos e habilidades a fim de subsidiar o planejamento de capacitações, desenvolvimento individual e até processos de recrutamento interno.

As trilhas de conhecimento da Auditoria Interna (link), as avaliações de desempenho da equipe de auditores - avaliação de resultados – GDES (link) e o formulário 'Guia de Competências - Estrutura Global IIA' a avaliação de competências (conectadas às competências do GDES) (link) são os instrumentos norteadores para o mapeamento das lacunas.

Ao menos anualmente deve ser avaliada a necessidade de atualização, por meio de formulário, do nível de conhecimento de cada empregado por eixo de formação com base nos processos da Auditoria Interna.

11 Comunicação Auditoria Interna

Internamente, a comunicação na Audin é suportada pelas ferramentas corporativas que a Empresa disponibiliza: e-mail; *teams;* Sistema de Correspondência - Siscor*;* Site da Auditoria Interna (link); dentre outros.

Destaca-se o e-mail Fique por Dentro - informe periódico para divulgar ações de interesse da auditoria interna, informações importantes e urgentes de caráter processual, capacitação, eventos, resultado de trabalhos, dentre outros.

O site da Audin contém informações sobre a auditoria interna como estrutura, processo da auditoria, modelo de documentos, PAINT, RAINT, links úteis dentre outros. O departamento Audie é o responsável pela sua atualização contínua.

11.1 Mapa de Entregas - Audin

No intuito de mapear as principais entregas realizadas pela Audin, o objetivo de cada uma, meio, frequência, atores internos e externos envolvidos e responsáveis na Audin, foi estabelecido um mapa de entregas - comunicação (link).

Este arquivo deve ser periodicamente revisado. No mínimo, anualmente.

11.2 Mapa de Avaliação / Asseguração

O mapa de avaliação/ asseguração (link) está estruturado por meio das categorias de riscos e de suas fontes de informação e evidencia como as linhas de defesa da empresa (e fora dela) cobrem estes riscos.

A escala utilizada reflete o nível de independência da opinião de cada avaliador que atua sobre o risco. Em relação às tipologias de riscos, foram usadas as tipologias corporativas previstas na Metodologia de Gestão de Riscos e Controles Internos. O mapa de avaliação se relaciona à IPPF 2050 -Coordenação e Confiança.
Este arquivo deve ser periodicamente revisado. No mínimo, anualmente.