Papéis para a auditoria interna governamental na avaliação de controles cibernéticos

Validação de conteúdo da atuação da auditoria interna à luz do Modelo das Três Linhas

Pedro Henrique Portugal de Sousa[1] and Rafael Rabelo Nunes[2]

[1]*Agência Nacional de Saúde Suplementar*
Rio de Janeiro – RJ
[2]*Departamento de Engenharia Elétrica*
Universidade de Brasília
Brasília - DF
portugal.pedroh@gmail.com,rafaelrabelo@unb.br

Abstract

The growing complexity of cyber risks demands an integrated approach between internal audit and other organizational functions, as advocated by the Three Lines Model. This study aimed to validate the content of statements regarding possible roles of internal audit in assessing cyber risks and controls within the public sector. The content validity technique [Lynn 1986; Alexandre and Coluci 2011] was applied to 15 statements derived from the literature [Ferreira et al. 2025]. Eight expert judges evaluated each statement for relevance, clarity, and lack of ambiguity, using a four-point agreement scale. Overall, 10 statements (66.7%) achieved a Content Validity Index (CVI) ≥ 0.75 for relevance, which was adopted as the main criterion and reference for analyzing results and revising the statements. Analysis of the expert assessments revealed differences between evaluators with auditing experience (4 judges) and those from other professional backgrounds (4 judges), particularly regarding the achievement of CVI ≥ 0.75 for relevance: auditors validated 14 statements (93.3%), while non-auditors validated 10 (66.6%). Across all profiles, statements related to compliance received higher ratings than those addressing cybersecurity control assessments, consistent with findings reported in the literature. The study achieved preliminary validation of the evaluated statements, retaining three in their original form and revising twelve, with potential to support future diagnostics and actions for government internal auditing in addressing cyber risks.

Keywords: risk assessment; cybersecurity controls; compliance; public sector; governmental auditing.

Resumo

A crescente complexidade dos riscos cibernéticos exige atuação integrada entre a auditoria interna e demais funções da organização, conforme preconiza o Modelo das Três Linhas. Nesse sentido, o estudo teve como objetivo validar o conteúdo de afirmações sobre possíveis papéis da auditoria interna na apreciação de riscos e controles cibernéticos no setor público. Foi utilizada a técnica de validade de conteúdo [Lynn 1986; Alexandre e Coluci 2011] sobre 15 afirmações derivadas da literatura [Ferreira et al. 2025]. Oito juízes especialistas avaliaram a pertinência, clareza e ausência de ambiguidade das afirmações, em escala de quatro níveis de concordância. No total, 10 afirmações (66,7%) atingiram Índice de Validade de Conteúdo (IVC) $\geq$ 0,75 para pertinência, parâmetro e critério central adotados como referência para análise dos resultados e revisão textual das afirmações avaliadas. Na análise das avaliações pelos especialistas, observou-se divergências entre avaliadores com perfil de experiência em auditoria (4 juízes) e outros perfis (4 juízes), principalmente quanto ao atingimento do IVC $\geq$ 0,75 para pertinência: para auditores, foram 14 afirmações (93,3%); para perfis de não auditores foram 10 afirmações (66,6%). Em todos os perfis, afirmações relacionadas à conformidade receberam avaliações mais altas do que aquelas voltados à avaliação de controles de cibersegurança, o que reflete apontamentos observados na literatura. O estudo obteve validação preliminar das afirmações avaliadas, em que 3 foram mantidas e 12 revisadas, com potencial para apoiar diagnósticos e ações futuras para a auditoria interna governamental no enfrentamento aos riscos cibernéticos.

Palavras-chave: avaliação de riscos; controles de cibersegurança; conformidade; setor público; auditoria governamental.

1. Introdução

No cenário global atual, o risco cibernético é prioridade estratégica para organizações públicas e privadas. Estimativas indicam que cerca de três quartos das instituições planejam ampliar investimentos em segurança da informação, diante de prejuízos médios de US$ 3 milhões por incidente [CrowdStrike 2025; PwC 2024]. No Brasil, o Tribunal de Contas da União (TCU) classifica o país como a quarta maior superfície de ataque desnecessariamente exposta, com aumento de 56% nos incidentes no setor público e risco potencial de até R$ 5,5 trilhões do orçamento de políticas públicas [TCU 2024]. Cenário que exige das organizações estruturas de governança que articulem, com eficácia e coordenação, responsabilidades no tratamento de riscos cibernéticos.

Como proposta de *framework*, o Modelo das Três Linhas do *Institute of Internal Auditors* (IIA) estabelece uma estrutura conceitual para integrar governança, gestão de riscos e controles de segurança cibernética, com funções e responsabilidades definidas de forma clara. A Primeira Linha é responsável pela gestão e operação de ativos, processos e controles; a Segunda Linha, pela supervisão e monitoramento dos processosda Primeira Linha; e a Terceira Linha, pela avaliação independente de riscos e controles organizacionais geridos pelas demais Linhas, um papel atribuído à auditoria interna, foco deste estudo [IIA 2020b; IIA 2020a].

Contudo, apesar da consolidação desse modelo, existem inúmeros desafios na definição de papéis e atribuições entre as Linhas na gestão de riscos e controles cibernéticos [Alves, Queiroz e Nunes 2023; Slapničar et al. 2022]. As dificuldades incluem lacunas de coordenação com as demais linhas de defesa, limitações técnicas, escassez de recursos, baixa influência junto à alta gestão e agendas institucionais divergentes – fatores que limitam a efetividade das auditorias em ambientes de alta complexidade e rápida evolução das ameaças cibernéticas [Bantleon et al. 2021; Steinbart et al. 2018; Vuko et al. 2024].

Assim, de acordo com o contexto apresentado, o presente estudo tem como objetivo validar o conteúdo de afirmações sobre os possíveis papéis da auditoria interna governamental na frente aos riscos e controles cibernéticos, à luz do Modelo das Três Linhas. Para isso, utiliza a metodologia de validação de conteúdo [Lynn 1986; Alexandre e Coluci 2011], com a participação de especialistas do setor público, para avaliar características de pertinência, clareza e ausência de ambiguidade, a partir de possíveis atribuições da auditoria identificadas na literatura especializada [Ferreira et al. 2025]. Como resultado, espera-se oferecer um instrumento preliminarmente validado, com a identificação de possíveis papéis para a avaliação de riscos e controles cibernéticos pela auditoria interna na administração pública.

O trabalho foi organizado em cinco seções: 1 - Introdução; 2 - Referencial Teórico, com a apresentação do cenário de risco cibernético atual, conceitos do Modelo das Três Linhas e da atuação da auditoria interna; 3 Metodologia, que descreve o problema de pesquisa, o objetivo e a abordagem de validade de contúdo adotada; 4 - Resultados e Discussão, com apresentação e análise dos resultados obtidos; e 5 - Conclusão, com considerações, destaques, limitações e sugestões para estudos futuros.

2. Referencial Teórico

A emergência dos riscos cibernéticos apresenta desafios significativos às organizações em todo o mundo, conforme demonstram publicações especialiadas recentes, que registram aumentos contínuos de campanhas de intrusão e em invasões em nuvem; de comercialização de acessos ilegítimos a sistemas (*access brokers*); e de adversários rastreados globalmente [CrowdStrike 2025]. Com um custo médio global de aproximadamente US$ 3 milhões com incidentes de

violação, para o qual 66% dos executivos de tecnologia classificam o risco cibernético como a principal prioridade a ser mitigada e 77% das organizações pretendem ampliar orçamentos de cibersegurança nos próximos anos [PwC 2024].

No contexto do setor público federal brasileiro, relatório recente de órgão de controle destacou um aumento de 56% nos incidentes registrados, a posição do Brasil como a 4ª maior superfície de ataque desnecessariamente exposta no mundo, a ausência de implementação adequada de controles básicos pelas organizações federais auditadas, e o fato de apenas 42% dessas organizações avaliadas terem adotado até 19% das medidas recomendadas. Fragilidades identificadas, segundo o documento, que colocam em risco aproximadamente R$ 5,5 trilhões do orçamento federal destinado a políticas públicas [TCU 2024].

Um cenário que exige das organizações mecanismos adequados para responder a ameaças cibernéticas, através de práticas robustas de gestão de riscos e controles internos. As quais, no contexto estudado, depende da efetividade de abordagens de gestão integradas, com envolvimento ativo entre as áreas tecnologia e segurança da informações com a auditoria interna [Steinbart et al. 2018; Slapničar et al. 2022].

2.1. Modelo das Três Linhas como estrutura de governança de riscos cibernéticos

O Modelo das Três Linhas, amplamente adotado por organizações públicas e privadas em todo o mundo, propõe a articulação de papéis na governança, gerenciamento e controle de riscos para o atingimento de objetivos institucionais, a partir da identificação e definição de Três Linhas de atuação [IIA 2020b; MP/CGU 2016]. Cabe à Primeira Linha a execução das processos e controles operacionais, relacionados aos serviços e produtos fornecidos pela organização. Ao passo que a Segunda Linha é responsável por funções especializadas de suporte, supervisão e monitoramento, por áreas de gestão de riscos, integridade, compliance e segurança da informação, acompanhar a atividade da Primeira Linha em direção aos objetivos organizacionais [IIA 2020b].

A coordenação e a segregação da atuação entre as duas primeiras Linhas organizacionais é assim condição ao adequado funcionamento do gerenciamento de riscos, essenciais para a promoção de uma cultura de riscos e aperfeiçoamento de controles internos cibernéticos [Alves, Queiroz e Nunes 2023]. Em que a efetividade da atuação dessas Linhas depende da clareza da definição de seus papéis, da existência de mecanismos estruturados de comunicação, coordenação e colaboração entre ambas, evitando sobreposições [Bantleon et al. 2021].

No caso das organizações públicas federais brasileiras, os papéis para a gestão de riscos e controles cibernéticos têm sido reforçados, no Modelo das Três Linhas, a partir do Programa de Privacidade e Segurança da Informação (PPSI) [SGD/MGI 2024]. Iniciativa do Governo Fede-

ral que estabelece padrões para a proteção de dados e segurança da informação, para que processos e controles públicos estejam alinhados às melhores práticas internacionais. Onde estão atribuídas funções: de Primeira Linha, aos gestores de tecnologia, de segurança da informação e demais resposáveis por riscos cibernéticos; e de Segunda Linha, aos responsáveis por unidades de controle interno — papel que ainda gera discussões e carece de melhor especificação ou implementação no setor público [Alves, Queiroz e Nunes 2023].

2.2. Papel da Terceira Linha para o aperfeiçoamento de processos de governança, de gerenciamento de riscos e de controles internos cibernéticos

Em continuidade ao Modelo de Três Linhas, o papel de Terceira Linha é atribuído à atividade de auditoria interna, incumbida de avaliar, de forma independente, a adequação e a eficácia da governança, da gestão de riscos e dos controles internos conduzidos pelas demais Linhas [IIA 2020b]. No âmbito governamental, essa função se concretiza por meio de trabalhos voltados a avaliar programas e serviços públicos, aferir o desempenho organizacional, proteger o patrimônio público e examinar sistemas corporativos relevantes, priorizando aspectos gerenciais além da mera conformidade [CGU/SFC 2017].

No contexto específico da cibersegurança, esses trabalhos de auditoria podem incluir: verificar o alinhamento entre a governança de tecnologia e os objetivos estratégicos; colaborar com a avaliação e priorização de respostas a riscos; propor avaliar riscos e controles preventivos e corretivos diante de ameaças e incidentes; e manter comunicação ativa com a alta administração quanto cibersegurança [IIA 2020a]. Embora, para a sua efetiva realização, a auditoria deve preservar a independência e autonomia de sua atuação, evitando assumir responsabilidades típicas da Primeira e da Segunda Linhas [CGU 2025].

Essa postura de preservação da independência não deve implicar isolamento. Relações colaborativas entre auditores e gestores, apoiadas por canais de comunicação eficazes, são capazes de ampliar a eficácia da identificação de fragilidades e da implementação de recomendações de auditoria, fortalecendo a governança de riscos cibernéticos [Steinbart et al. 2012; Steinbart et al. 2018].

De outra forma, uma postura colaborativa depende também do suporte da alta administração na disponibilização de recursos e no estabelecimento de canais adequados de interlocução, propício à cooperação entre auditoria, gestão e áreas estratégicas no enfrentamento das ameaças cibernéticas [Islam, Farah e T. F. Stafford 2018]. Especialmente mais efetivo quando profissionais com conhecimentos em tecnologia e segurança da informação também integram as equipes de auditoria e aos próprias instâncias de governança e da alta gestão [Islam e T. Stafford 2017].

2.3. Desafios ao alinhamento entre as atribuições da auditoria interna e papéis das demais linhas para o tratamento de riscos cibernéticos

A implementação do Modelo das Três Linhas apresenta diferentes desafios. O primeiro desafio está relacionado justamente à necessidade de coordenação eficaz entre as três Linhas, pois frequentemente existem duplicidades ou lacunas de atuação, dificultando a consolidação de uma visão integrada dos riscos cibernéticos na organização [Bantleon et al. 2021]. A indefinição dessas fronteiras entre as funções de tecnologia e segurança da informação, para a Primeira e Segunda Linhas, pode gerar sobreposições de responsabilidades, descaracterizando a independência entre os diferentes processos e enfraquecendo a governança dos riscos cibernéticos [Alves, Queiroz e Nunes 2023].

Tais lacunas ou sobreposições entre Primeira e Segunda Linhas também tendem a impactar diretamente o escopo da atuação da auditoria interna, principalmente diante de eventuais ausências de processos ou atividades da Segunda Linha para com a Primeira [Alves, Queiroz e Nunes 2023]. No caso da administração pública federal, uma preocupação externalizada através da publicação de diversos normativos públicos, com reforço do papel exigido dos auditores, que não devem assumir funções ou atividades típicas das demais Linhas para a preservação da indenpendência e autonomia que possuem. [MP/CGU 2016; CGU 2025].

Barreiras institucionais e culturais também constituem obstáculos ao alinhamento entre as ações da auditoria interna e junto às áreas de tecnologia e segurança da informação [Vuko et al. 2024]. A resistência à colaboração com a auditoria dificulta a identificação de fragilidades e a implementação de melhorias associadas ao tratamento de riscos, o que se relaciona a visões ultrapassadas que gestores podem possuir sobre auditores, como de uma atividade meramente detectiva, corretiva ou punitiva; a existência de rivalidades organizacionais históricas (“turf battles”); ou de isolamento de determinadas áreas de negócio em relação ao trabalho de auditoria [Steinbart et al. 2018].

Ainda no contexto dos riscos cibernéticos, outro desafio ao papel da auditoria está relacionado a limitações técnicas e de conhecimento dos quadros de profissionais que compõem a auditoria da maioria das organizações [Lois et al. 2020; Islam e T. Stafford 2017]. Com frequência, tais unidades apresentam tamanho reduzido diante da escala dos riscos e controles existentes, contam com poucos profissionais formados em tecnologia, dedicam baixo percentual de tempo para ações voltadas à segurança da informação e possuem limitada capacidade de realizar procedimentos mais complexos, como análise de vulnerabilidades ou simulações de ataques [Ferreira et al. 2025].

Limitações institucionais, técnicas e de escopo, sobretudo diante de referenciais nacionais e internacionais que ressaltam a necessidade de que os auditores possuam proficiência em tecnologia e acesso a ferramentas de cibersegurança para executarem auditorias contínuas, testes de

penetração, análises de configurações e avaliações técnicas específicas [CGU 2024; IIA 2020a]. Desafios que evidenciam dificuldades entre o que se deve, pode ou efetivamente se consegue realizar, a depender do alinhamento existente das atribuições entre as Três Linhas frente aos riscos cibernéticos. Onde a ausência de clareza sobre o papel dos auditores contribui para eventuais sobreposições de tarefas, lacunas de cobertura e, em última instância, para uma falsa sensação de segurança quanto ao tratamento desses riscos [Bantleon et al. 2021].

3. Metodologia

Conforme a classificação metodológica proposta por [Gil 2008], esta pesquisa é de natureza aplicada, com abordagem quanti-qualitativa, voltada à delimitação e validação — por meio de formulário aplicado a especialistas do setor público — dos possíveis papéis atribuídos à auditoria interna frente aos riscos de cibersegurança, à luz do Modelo das Três Linhas. Os objetivos são exploratórios e descritivos, uma vez que se busca analisar, detalhar e compreender as avaliações realizadas pelos especialistas sobre o objeto proposto. Quanto aos procedimentos, a investigação articula levantamento bibliográfico para embasar o referencial teórico, análise de caso para examinar situações concretas no setor público e pesquisa de campo para coleta e validação de dados.

A base empírica fundamenta-se nas unidades de contexto identificadas por [Ferreira et al. 2025], que mapeou situações e desafios enfrentados pela auditoria interna diante dos riscos cibernéticos, utilizando entrevistas semiestruturadas e análise qualitativa de conteúdo, conforme o método de [Bardin 2016]. Das 53 unidades de contexto (proposições ou possibilidades de atuação) ao papel da auditoria interna consolidadas pelo autor, originalmente voltadas ao setor financeiro, realizou-se um refinamento metodológico, selecionando apenas as categorias diretamente relacionadas ao objetivo desta pesquisa. Esse recorte, além de limitar o escopo, foi necessário para que o instrumento final refletisse os aspectos mais relevantes ao contexto das auditorias governamentais, preservando o conteúdo conceitual do trabalho do autor, mas priorizando sua aderência ao foco proposto pelo presente estudo.

3.1. Seleção das afirmações utilizadas a partir das 53 unidades de contexto

As 53 unidades de contexto identificadas por [Ferreira et al. 2025] foram analisadas e agrupadas, no estudo de origem, em oito categorias temáticas: “1 Perfil dos entrevistados”; “2 Atuação das linhas” “3 Relacionamento com as demais áreas da instituição”; “4 Estratégia corporativa”; “5 Avaliação da efetividade dos controles de segurança cibernética”; “6 Ambiente regulatório e conformidade”; “7 Direcionamento de achados e recomendações de auditoria”; e “8 Desafios, tendências e inovações”.

No presente estudo, foram selecionadas 15 possibilidades de atuação (quadros 2 e 3) do referido autor, concentradas nas categorias “5 Avaliação da efetividade dos controles de segurança cibernética”, que aborda como a auditoria interna pode mensurar a efetividade dos controles de segurança implementados nas instituições; e “6 Ambiente regulatório e conformidade”, que trata de como a Terceira Linha pode contribuir para garantir a conformidade com normas e regulamentos relacionados à segurança cibernética. As unidades de contexto foram tratadas como "afirmações"no contexto do presente estudo, tendo em vista pequenas adaptações textuais realizadas para que fossem, de fato, lidas como afirmações – além das formas verbais, principalmente pela inclusão do fragmento "A auditoria interna governamental deve". Essas categorias foram priorizadas por englobarem procedimentos e práticas específicas da auditoria interna, frequentemente associadas a desafios operacionais, discussões técnicas e interpretações divergentes em diversos setores.

As demais categorias não foram utilizadas para preservar a objetividade e a relevância prática desta pesquisa, sem prejuízo de sua utilização em pesquisas futuras. “Perfil dos entrevistados” contém apenas dados pessoais e profissionais dos participantes; “Atuação das linhas”, “Relacionamento com as demais áreas da instituição” e “Estratégia corporativa” abordam funções já consolidadas em normas e manuais; “Direcionamento de achados e recomendações de auditoria” referia-se a etapas padronizadas aplicáveis a qualquer objeto de auditoria; e “Desafios, tendências e inovações” trata de aspectos específicos do setor financeiro.

3.2. Validade de conteúdo das afirmações obtidas a partir das unidades de contexto

As afirmações selecionadas foram submetidas à validade de conteúdo, conforme recomendações clássicas e atuais, que envolvem a avaliação sistemática de itens por um painel de especialistas quanto à relevância (representatividade ou pertinência), clareza e ausência de ambiguidade, combinando análises qualitativas das sugestões recebidas com a mensuração quantitativa por meio do Índice de Validade de Conteúdo (IVC) [Lynn 1986]. No presente estudo, o constructo — conceito central previamente definido pelo pesquisador, não observável diretamente e inferido pelas respostas dos especialistas — refere-se ao papel da auditoria interna, entendido como o conjunto de funções, responsabilidades e atribuições dessa atividade nas organizações [Alexandre e Coluci 2011; Ferreira et al. 2025].

O comitê avaliador selecionado foi formado por oito especialistas (quadro 1), número recomendado para garantir diversidade de perspectivas e viabilidade operacional para pequenos grupos [Alexandre e Coluci 2011; Lynn 1986]. A composição buscou equilíbrio entre formações e experiências, reunindo quatro profissionais da área de auditoria e quatro de tecnologia e segurança da informação, todos com atuação prática em riscos, integridade ou áreas correlatas, assegurando cobertura técnica ampla e alinhada ao objeto do estudo.

3.3. Aplicação e avaliação do formulário de validade de conteúdo juntos aos juízes especialistas

O formulário de validade de conteúdo foi estruturado em meio digital e encaminhado individualmente aos juízes especialistas, conforme recomendações metodológicas para evitar viés de grupo e assegurar a autenticidade das respostas [Alexandre e Coluci 2011; Lynn 1986]. Foram fornecidas instruções detalhadas sobre os objetivos da avaliação e os critérios analisados, garantindo compreensão uniforme e preenchimento padronizado.

Cada item do instrumento foi avaliado segundo uma escala ordinal de quatro pontos para cada critério (discordo totalmente, discordo, concordo e concordo totalmente), permitindo graduações na análise e viabilizando o cálculo do Índice de Validade de Conteúdo (IVC). A avaliação baseou-se em três critérios [Alexandre e Coluci 2011; Lynn 1986]: pertinência, critério central para analisar o alinhamento do item com os objetivos e o constructo do instrumento, garantindo relevância teórica e prática; clareza, para verificar se as sentenças são compreensíveis ao público-alvo, evitando termos ambíguos ou confusos; e ausência de ambiguidade, para assegurar objetividade e prevenir múltiplas interpretações. Além da análise quantitativa, o formulário incluiu campos abertos para comentários e sugestões qualitativas, permitindo identificar oportunidades de melhoria, ajustar redações e eliminar inconsistências remanescentes.

Os dados numéricos consolidados subsidiaram o cálculo do IVC, mensurando o grau de concordância entre especialistas quanto à adequação dos itens. A combinação entre resultados quantitativos e qualitativos, colhidos dos comentários dos avaliadores, possibilitou o refinamento sistemático das afirmações sobre a atuação da auditoria interna governamental, para maior robustez, representatividade e aderência ao contexto investigado.

3.4. Cálculo do Índice de Validade de Conteúdo (IVC)

O Índice de Validade de Conteúdo (IVC) foi adotado como parâmetro objetivo para mensurar o grau de consenso entre os especialistas. Seu cálculo foi realizado individualmente para cada afirmação e critério, atribuindo-se valor 1 às avaliações positivas (concordo ou concordo totalmente) e valor 0 às negativas (discordo ou discordo totalmente). O IVC de cada item corresponde à razão entre a soma de avaliações positivas e o total de juízes participantes [Alexandre e Coluci 2011; Lynn 1986].

$$\text{IVC Critério} = \frac{\text{Soma de Avaliações Positivas}}{\text{Total de Juízes}}$$

Em um painel composto por 8 especialistas, a literatura recomenda um IVC mínimo de 0,78, o que exige pelo menos sete avaliações positivas ($7 \div 8 = 0,88$) para que uma afirmação

seja considerada válida – enquanto em painéis menores que seis participantes, recomenda-se a concordância total (IVC = 1,00). Valores inferiores não possuem o mesmo rigor estatístico, como no caso de seis avaliações positivas, que resultariam em IVC apenas 0,75, embora possam ter valor para contextos exploratórios específicos [Lynn 1986; Alexandre e Coluci 2011]. Esse cálculo permite identificar, de forma objetiva, as sentenças com maior consenso, contribuindo para selecionar aquelas mais representativas e alinhadas ao constructo proposto.

4. Resultados e Discussão

O painel de oito juízes especialistas (quadro 1) reuniu três profissionais com formação em gestão e cinco em tecnologia ou segurança da informação, sendo cinco com especialização e três com titulação stricto sensu (dois mestrados e um doutorado). Metade dos juízes possui experiência em auditoria interna ou independente, a maioria acumula mais de dez anos de atuação em riscos, integridade ou áreas correlatas, e seis têm experiência significativa em tecnologia ou segurança da informação. Essa composição assegura diversidade de perspectivas e equilíbrio entre conhecimentos em auditoria, gestão de riscos e aspectos técnicos, contemplando diferentes papéis no Modelo das Três Linhas.

Perfil	Formação	Grau de Instrução	Experiência Profissional		
			Auditoria Interna ou Independente	Riscos, Integridade ou Correlatas	Tecnologia ou Segurança da Informação
1	Gestão	Especialização	Mais de 10 anos	Mais de 10 anos	Não possui
2	Gestão	Mestrado	Mais de 10 anos	Mais de 10 anos	Não possui
3	Tecnologia	Mestrado	Não possui	Mais de 10 anos	Mais de 10 anos
4	Tecnologia	Especialização	Mais de 10 anos	Mais de 10 anos	6 a 10 anos
5	Tecnologia	Especialização	Não possui	Mais de 10 anos	Mais de 10 anos
6	Tecnologia	Especialização	Não possui	6 a 10 anos	6 a 10 anos
7	Tecnologia	Doutorado	Não possui	Até 2 anos	Mais de 10 anos
8	Gestão	Especialização	6 a 10 anos	Não possui	Não possui

Quadro 1: Perfil dos Juízes

O formulário eletrônico aplicado junto aos juízes, entitulado “Questionário de validação de instrumento sobre o papel da auditoria interna frente aos riscos cibernéticos”, apresentava as seguintes 15 afirmações (quadros 2 e 3), extraídas e adaptadas de Ferreira et al. (2025), agrupadas nas categorias “Avaliação da efetividade dos controles de segurança cibernética” e “Ambiente regulatório e conformidade”. As quais foram avaliadas segundo os critérios de pertinência, clareza e ausência de ambiguidade, conforme metodologia reconhecida de validade de conteúdo.

Itens	Afirmações
1	A auditoria interna deve verificar aspectos de gestão e governança dos processos, realizando avaliações de alto nível e estratégicas.
2	A auditoria interna deve realizar ou contratar empresas especializadas para efetuar testes de Invasão ou de Penetração (PenTest).
3	A auditoria interna deve avaliar o processo de gestão de vulnerabilidade, as ferramentas utilizadas, as etapas estabelecidas, a documentação gerada e as regras definidas e aplicadas.
4	A auditoria interna deve realizar avaliações e testes de segurança em conjunto equipes de TI e de Segurança Cibernética.
5	A auditoria interna deve utilizar auditoria contínua baseada em dados e informações para monitorar e avaliar continuamente os controles e processos de segurança.
6	A auditoria interna deve avaliar como as áreas de TI e de segurança cibernética implementam ferramentas de monitoramento contínuo que detectam atividades anormais ou suspeitas em tempo real.
7	A auditoria interna deve compilar e analisar dados sobre violações e incidentes de segurança anteriores, além de tendências atuais em segurança cibernética para identificar áreas de risco emergente.
8	A auditoria interna deve desenvolver relatórios de segurança e painéis de controle que apresentam uma visão do status da segurança cibernética da organização.
9	A auditoria interna deve estabelecer métricas e indicadores que forneçam uma visão clara e objetiva do estado atual da segurança cibernética na organização.
10	A auditoria interna deve adotar frameworks que ofereçam estruturas padronizadas para a gestão de processos, avaliação de riscos e controles de segurança.

Quadro 2: Categoria - Avaliação da efetividade dos controles de segurança cibernética

Itens	Afirmações
11	A auditoria interna deve ir além da mera conformidade nas avaliações para verificar se os ativos mais críticos da organização estão adequadamente protegidos.
12	A auditoria interna deve realizar monitoramento contínuo para identificar quando novas regulamentações foram introduzidas ou atualizações serem realizadas em normas existentes.
13	A auditoria interna deve trabalhar em colaboração com a Segunda Linha para obter uma visão unificada e suficientemente abrangente da conformidade em toda instituição.
14	A auditoria interna deve realizar auditorias regulares de conformidade para identificar áreas com risco de não conformidade.
15	A auditoria interna deve realizar a interface com Reguladores, Auditores e Consultores para auditorias regulatórias externas.

Quadro 3: Categoria - Ambiente regulatório e conformidade

4.1. Análise dos resultados obtidos com a aplicação do formulário de validade de conteúdo

Após o colhimento e compilação das respostas dos juízes, as afirmações foram então consolidadas e agrupadas para análise do índice de validade de conteúdo (IVC), por critério, para identificar de forma quantitativa os níveis de pertinência, clareza e ausência de ambiguidade atribuídos pelos juízes a cada item. O gráfico 1 apresenta a distribuição geral dos índices, considerando a avaliação de todos 8 profissionais participantes.

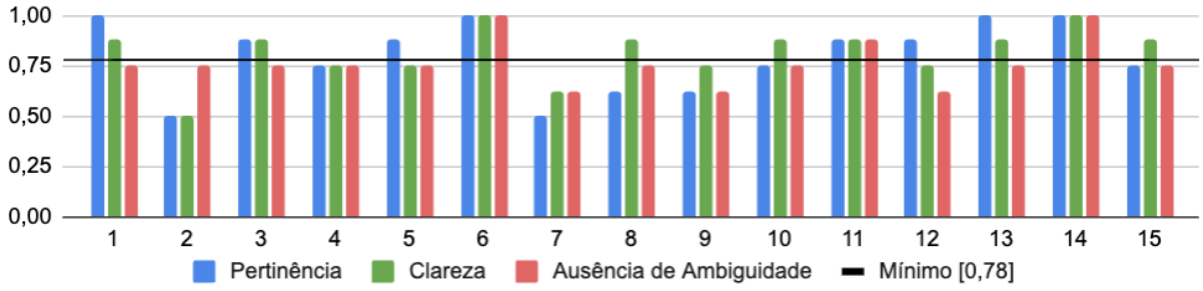

Gráfico 1: IVC - Todos os Perfis

Dos 15 itens avaliados, na análise geral para todos os perfis (gráfico 1), apenas 3 (20%) foram plenamente validados, alcançando IVC geral acima do mínimo recomendado para pequenos grupos (IVC $\geq$ 0,78) em todos os critérios — itens 6, 11 e 14. Considerando uma análise na faixa de IVC = 0,75, por critério, 11 itens (73,3%) atenderam ao requisito de pertinência, 13 (86,7%) à clareza e 12 (80%) à ausência de ambiguidade. Ainda assim, o rigor da metodologia de validade de conteúdo exige que todos os critérios de um item superem o valor mínimo estabelecido, de IVC = 0,78, para que seja considerado validado.

4.1.1. Pertinência – a afirmação é pertinente com relação à categoria, está alinhada ao objetivo do instrumento e é relevante para o contexto de auditoria interna e riscos cibernéticos

A avaliação da pertinência de cada item foi adotada como fator central no processo de validade (grafico 2), pois pretende garantir que as afirmações representem os domínios essenciais do construto que se deseja mensurar [Lynn 1986]. A literatura ressalta que a heterogeneidade do painel de juízes pode gerar divergências, conforme observado entre perfis de auditores e não auditores. Porém isso deve também ampliar o espectro de análise para evidenciar possíveis pontos de fragilidade ou de incompletude, oportunidades para aprimoramento que podem sinalizar diferenças de entendimento entre as áreas de formação e atuação dos especialistas avaliadores [Alexandre e Coluci 2011; Vazzoler-Mendonça, Rondini e Costa-Lobo 2023] – base para o refinamento das afirmações e proposição de novas rodadas de avaliação.

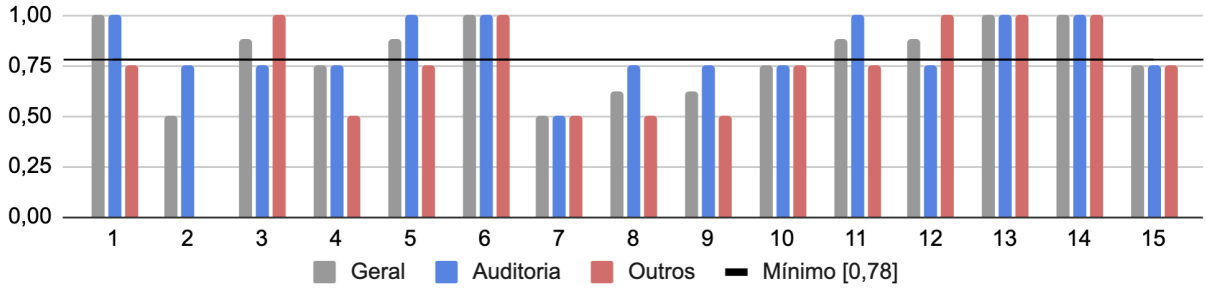

Gráfico 2: IVC - Pertinência

Na avaliação do critério pertinência, por tipos de perfil, para os juízes com experiência em auditoria, 14 itens (93,3%) atingiram um índice de ao menos 0,75, indicando alto nível de convergência inicial, dos quais 6 itens (40%) ficaram acima do mínimo de 0,78 para serem validados sem revisão. Enquanto para o perfil de profissionais de tecnologia, segurança, riscos ou correlatas, a avaliação foi pior: 10 itens (67,7%) atingiram o parâmetro de 0,75 e 33,3% o de 0,5 ou menos – a afirmação nº 2 ficou com zero. Houve uma relevante avaliação negativa dos profissionais de tecnologia quanto a pertinência do papel da auditoria, principalmente para afirmações da categoria de avaliação de controles. Ao passo que as afirmações a respeito da categoria de conformidade, de forma geral, obtiveram avaliações melhores, o que indica maior consenso a respeito do papel estratégico e de conformidade da auditoria, porém menor para o trabalho sobre riscos e controles cibernéticos operacionais, mais afetos à atividade da Primeira Linha.

Essas divergências entre os perfis refletem aspectos já debatidos na literatura, em que profissionais de auditoria reconhecem seu papel na avaliação de processos e controles operacionais, enquanto especialistas em tecnologia frequentemente questionam a efetividade das avaliações conduzidas pela auditoria sobre controles técnicos [Slapničar et al. 2022; Steinbart et al. 2018]. Também são observadas ressalvas quanto à profundidade desejada da atuação da auditoria em segurança cibernética por profissionais de diversos perfis, com divergências quanto avaliações estratégicas ou operacionais, além de reconhecidas limitações culturais, institucionais, técnicas e de recursos para a adequada auditoria de cibersegurança em todos os casos [Ferreira et al. 2025; Islam e T. Stafford 2017; Lois et al. 2020].

Por fim, destaca-se um ponto central da contribuição qualitativa por meio da caixa de considerações do formulário, comum a todos os perfis, que diz respeito a possíveis sobreposições entre as Linhas e prejuízos à independência da auditoria. Especialmente no contexto das atividades técnicas e operacionais de segurança cibernética, itens nº 1 a 10, em que o comprometimento da independência e a extrapolação do papel da auditoria foram destacados de forma preponderante para os itens 2 (PenTest), 8 (Relatórios e Painéis), 9 (Métricas e Indicadores). Preocupações consistentes com a própria literatura, que evidencia a necessidade de colaboração, mas também

reconhece que sobreposições entre papéis são desafios para a efetividade e a independência previstas no modelo das Três Linhas para os riscos cibernéticos [Alves, Queiroz e Nunes 2023; Steinbart et al. 2012].

4.1.2. Clareza – a redação da afirmação é compreensível e adequada ao público-alvo; e Ausência de Ambiguidade – a afirmação é objetiva e não permite múltiplas interpretações

A metodologia de validade de conteúdo preconiza que critérios como clareza e ausência de ambiguidade devem ser avaliados quanto à redação dos itens, para assegurar que cada afirmação seja compreendida de forma inequívoca pelo público-alvo, evitando múltiplas interpretações [Lynn 1986]. Nesse sentido, a análise cuidadosa da linguagem empregada é fundamental, cabendo ao comitê de especialistas indicar ajustes sempre que identificados termos, expressões ou estruturas que possam gerar dúvidas ou interpretações ambíguas [Alexandre e Coluci 2011].

A análise dos critérios de clareza e ausência de ambiguidade (gráficos 3 e 4) mostrou maior consenso entre avaliadores com experiência em auditoria, 13 itens (86,7%) apresentaram IVC maior ou igual a 0,75 em ao menos um dos critérios, e 3 (20%) atingiram IVC de 0,5 em ao menos um. O desempenho foi menor para profissionais sem experiência em auditoria, embora 12 (80%) itens tenham atingido a faixa de 0,75 em ao menos um dos critérios, 4 itens (26,7%) atingiram 0,5 em ao menos um critérios. O que indica um menor concsenso positivo e um maior consenso negativo para os aspectos textuais, de forma geral, entre perfis de não auditores. Novamente como uma pior avaliação geral para afirmações do grupo de avaliação de controles, itens nº 1 a 10.

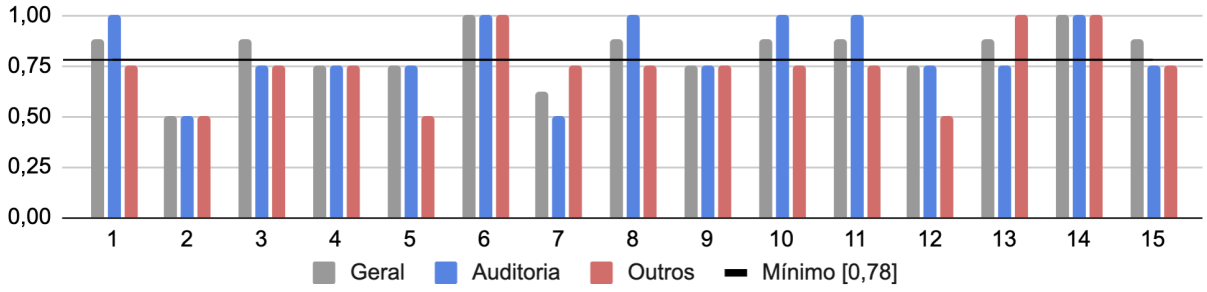

Gráfico 3: IVC - Clareza

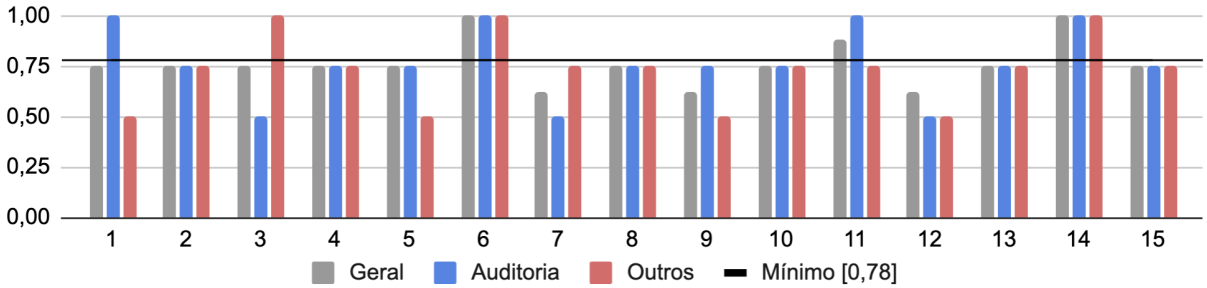

Gráfico 4: IVC - Ausência de Ambiguidade

Os resultados indicam que, embora haja itens bem compreendidos em ambos os grupos, é necessário aprimorar a redação de parte das afirmações para garantir clareza e reduzir ambiguidades para todos os perfis de avaliadores. Embora, apesar dos aspectos textuais, algumas divergências de compreensão das afirmações também possam estar relacionadas a fatores subjetivos diversos, como relacionados à comprensão do especialistas sobre a pertinência, ou associados a aspectos de experiência e atuação diante dos riscos cibernéticos.

Uuma maior uniformidade observada entre os profissionais de auditoria na avaliação das afirmações (gráficos 3 e 4) pode estar associada ao domínio, desses avaliadores, sobre padrões e práticas profissionais reconhecidas de auditoria, aspecto não compartilhados pelos demais juízes com formação em tecnologia [Vuko et al. 2024]. Em contrapartida, profissionais de TI, por terem formação e experiência mais aprofundadas para trabalhar com controles cibernéticos, podem ser mais críticos com relação às terminologias utilizadas e ao possível raio de atuação da auditoria diante dos riscos e controles operacionais [Lois et al. 2020]. Nesse contexto, a integração multidisciplinar entre perfis para um consenso textutal pode também oportunizar maior alinhamento sobre as responsabilidades em cibersegurança, servindo à mitigação de possíveis divergências de compreensão sobre papéis de cada ator diante dos riscos cibernéticos, evidenciados na literatura [Alves, Queiroz e Nunes 2023; Islam, Farah e T. F. Stafford 2018].

4.2. Revisão das afirmações de acordo com os resultados observados

As afirmações que atingiram IVC igual ou superior a 0,78 em todos os critérios (quadro 4) foram mantidas em sua redação original, por apresentarem consenso entre os avaliadores quanto à pertinência, clareza e ausência de ambiguidade. Posteriormente, para a etapa de revisão, as afirmações foram organizadas em dois quadros, conforme o Índice de Validade de Conteúdo (IVC) do critério de pertinência: o quadro 5 reúne aquelas com IVC igual ou superior a 0,75, enquanto o quadro 6 apresenta as que ficaram abaixo desse valor.

Item	Afirmação	P	C	A	G
6	A auditoria interna deve avaliar como as áreas de tecnologia e segurança da informação implementam ferramentas de monitoramento contínuo que detectam atividades anormais ou suspeitas em tempo real.	1,00	1,00	1,00	1,00
11	A auditoria interna deve ir além da mera conformidade nas avaliações para verificar se os ativos cibernéticos mais críticos da organização estão adequadamente protegidos.	0,88	0,88	0,88	0,88
14	A auditoria interna deve realizar auditorias regulares de conformidade para identificar áreas com risco cibernético de não conformidade.	1,00	1,00	1,00	1,00

Quadro 4: Afirmações mantidas com IVC $\geq$ 0,78 em todos os critérios

Item	Afirmação	P	C	A	G
1	**Original:** A auditoria interna deve verificar aspectos de gestão e governança dos processos, realizando avaliações de alto nível e estratégicas.	1,00	0,88	0,75	0,88
	Revisada: A auditoria interna deve realizar avaliações para verificar aspectos de gestão e governança dos processos, sob uma perspectiva estratégica dos riscos cibernéticos.				
3	**Original:** A auditoria interna deve avaliar o processo de gestão de vulnerabilidade, as ferramentas utilizadas, as etapas estabelecidas, a documentação gerada e as regras definidas e aplicadas.	0,88	0,88	0,75	0,84
	Revisada: A auditoria interna deve avaliar o processo de gestão de vulnerabilidades, o seu alinhamento às boas práticas recomendadas e a efetividade das ações corretivas para o tratamento de riscos cibernéticos.				
4	**Original:** A auditoria interna deve realizar avaliações e testes de segurança em conjunto com equipes de TI e de Segurança Cibernética.	0,75	0,75	0,75	0,75
	Revisada: A auditoria interna deve realizar avaliações e testes cibernéticos, sem prejuízo de sua independência, de forma colaborativa com as equipes de tecnologia e segurança da informação.				
5	**Original:** A auditoria interna deve utilizar auditoria contínua baseada em dados e informações para monitorar e avaliar continuamente os controles e processos de segurança.	0,88	0,75	0,75	0,79
	Revisada: A auditoria interna deve utilizar técnicas de auditoria contínua, baseadas no uso sistemático de dados e informações, para monitorar e avaliar os controles e processos de segurança cibernética.				
10	**Original:** A auditoria interna deve adotar frameworks que ofereçam estruturas padronizadas para a gestão de processos, avaliação de riscos e controles de segurança.	0,75	0,88	0,75	0,79
	Revisada: A auditoria interna deve utilizar frameworks reconhecidos para avaliar se a organização adota estruturas padronizadas de gestão de riscos e controles de segurança cibernética.				
12	**Original:** A auditoria interna deve realizar monitoramento contínuo para identificar quando novas regulamentações foram introduzidas ou atualizações foram realizadas em normas existentes.	0,88	0,75	0,62	0,75
	Revisada: A auditoria interna deve monitorar de forma contínua o surgimento ou a atualização de regulamentações e normas aplicáveis sobre riscos cibernéticos.				
13	**Original:** A auditoria interna deve trabalhar em colaboração com a Segunda Linha para obter uma visão unificada e suficientemente abrangente da conformidade em toda instituição.	1,00	0,88	0,75	0,88
	Revisada: A auditoria interna deve adotar postura colaborativa com a Segunda Linha para obter uma visão unificada e abrangente da conformidade em segurança cibernética da instituição.				
15	**Original:** A auditoria interna deve realizar a interface com Reguladores, Auditores e Consultores para auditorias regulatórias externas.	0,75	0,88	0,75	0,79
	Revisada: A auditoria interna deve realizar a interface junto a reguladores, auditores e consultores externos, para o alinhamento institucional de informações a respeito de avaliações externas sobre riscos e controles cibernéticos.				

Quadro 5: Afirmações revisadas com IVC $\geq$ 0,75 para o critério de pertinência

A pertinência foi adotada como critério central por refletir a recomendação metodológica de que

apenas itens essenciais ao construto sejam mantidos [Lynn 1986; Alexandre e Coluci 2011]. Índices satisfatórios nesse critério podem indicar que eventuais discordâncias estejam ligadas a aspectos textuais, passíveis de correção. Considerando o caráter exploratório deste estudo, as afirmações com pertinência igual ou superior a 0,75 foram priorizadas para ajustes pontuais voltados aos demais critérios, por apresentarem maior potencial de atingir o patamar recomendado em etapas futuras de validação. As revisões realizadas no quadro 5 concentraram-se, assim, na eliminação de ambiguidades e no aprimoramento da precisão dos termos, com atenção especial às observações qualitativas que apontaram riscos de sobreposição de funções ou comprometimento da independência.

Foram adotados ajustes como: contexto de termos “alto nível” (item 1), “em conjunto” (item 4), “frameworks” (item 10) e “interface” (item 15); papel avaliativo da auditoria (item 3); conceito de auditoria contínua no contexto cibernético (item 5); caráter avaliativo no acompanhamento de normas (item 12); aspectos da colaboração e independência entre Linhas (item 13).

O quadro 6 reúne afirmações com pertinência inferior a 0,75, com prioridade de reformulação mais profunda dos enunciados, ou até mesmo para a reconsideração futura da manutenção desses itens no instrumento, visto que as discordâncias sobre pertinência podem não ser sanadas apenas com ajustes textuais. Nesses casos, a metodologia recomenda avaliar se o conteúdo do item é de fato essencial ao construto, considerando que sua exclusão ou reestruturação pode ser necessária para garantir a validade e a aderência ao escopo proposto [Lynn 1986; Alexandre e Coluci 2011].

Item	Afirmação	P	C	A	G
2	**Original:** A auditoria interna deve realizar ou contratar empresas especializadas para efetuar testes de Invasão ou de Penetração (PenTest).	0,50	0,50	0,75	0,58
	Revisada: A auditoria interna deve avaliar os resultados dos testes de invasão (PenTest) realizados pela área de segurança da informação, podendo acompanhar a sua contratação e execução, para avaliar a efetividade dos controles.				
7	**Original:** A auditoria interna deve compilar e analisar dados sobre violações e incidentes de segurança anteriores, além de tendências atuais em segurança cibernética para identificar áreas de risco emergente.	0,50	0,62	0,62	0,58
	Revisada: A auditoria interna deve compilar e analisar os dados sobre violações e incidentes de segurança, produzidos pelas áreas de técnicas organizacionais, visando identificar tendências atuais em segurança cibernética e áreas de risco emergentes.				
8	**Original:** A auditoria interna deve desenvolver relatórios de segurança e painéis de controle que apresentam uma visão do status da segurança cibernética da organização.	0,62	0,88	0,75	0,75
	Revisada: A auditoria interna deve analisar informações de relatórios e painéis de controle desenvolvidos pelas áreas de tecnologia e segurança da informação, com o objetivo de obter uma visão do status da segurança cibernética da organização.				
9	**Original:** A auditoria interna deve estabelecer métricas e indicadores que forneçam uma visão clara e objetiva do estado atual da segurança cibernética na organização.	0,62	0,75	0,62	0,66
	Revisada: A auditoria interna deve conhecer e avaliar as métricas e indicadores estabelecidos pelas áreas responsáveis, utilizando-os para obter uma visão clara e objetiva do estado atual da segurança cibernética na organização.				

Quadro 6: Afirmações revisadas com IVC $< 0{,}75$ para o critério de pertinência

As avaliações dos especialistas, de modo geral, refletiram discordâncias mais substanciais quanto

ao alinhamento das afirmações ao papel institucional da auditoria interna. Entre as considerações qualitativas recorrentes, em todos os perfis de juízes, destaca-se o entendimento de que determinadas afirmações extrapolam as funções típicas da auditoria e se aproximam de responsabilidades próprias da Primeira e Segunda Linhas, tais como testes de invasão (item 2) e acompanhamento de dados operacionais (itens 7, 8 e 9). De forma semelhantes à análise realizada nas situações de conflitos entre linhas, sobreposições e lacunas existentes nos tópicos anteriores.

5. Conclusão

O presente estudo teve como objetivo delimitar, utilizando validade de conteúdo como método central de análise, os possíveis papéis assumidos pela auditoria interna no contexto da cibersegurança em instituições públicas, à luz do Modelo das Três Linhas.

Apenas 3 das 15 afirmações (itens nº 6, 11 e 14) atingiram o (IVC $\geq$ 0,78) em todos os critérios, mantidas sem ajustes (quadro 4). Foram observadas divergências significativas na avaliação do critério de pertinência entre os perfis de juízes respondentes, em que auditores avaliaram 14 itens (93,3%) com IVC $\geq$ 0,75, enquanto profissionais de tecnologia avaliaram apenas 10 itens (66,6%) nesse parâmetro. Os especialistas registraram restrições sobre a atuação da auditoria na avaliação de controles cibernéticos e possíveis sobreposições de papéis junto às demais Linhas, conforme também apontado pela literatura [Steinbart et al. 2018; Slapničar et al. 2022]

Considerando o caráter exploratório do estudo, o IVC de 0,75 foi adotado como referência para identificar itens com potencial de aprimoramento textual. As afirmações com IVC $\geq$ 0,75 (quadro 5) passaram por ajustes pontuais de clareza e precisão (itens nº 1, 3, 4, 5, 10, 12, 13 e 15); enquanto as com IVC inferior (quadro 6) receberam revisões mais profundas (itens nº 2, 7, 8 e 9). Em uma abordagem que buscou preservar conteúdos essenciais ao construto.

De forma geral, a validade de conteúdo trabalhou a qualidade do conjundo de proposições, porém pode envolver limitações associadas à subjetividade dos avaliadores, ao tamanho da amostra e a possíveis distorções de representatividade dos grupos de juízes selecionados [Lynn 1986]. Restrições com potencial de impactar o grau de consenso obtido e a generalização dos resultados, tornando recomendável que esse processo seja complementado por etapas ou metodologias suplementares [Alexandre e Coluci 2011].

Futuras pesquisas podem explorar outros aspectos, como: repensar o número ou diversidade de especialistas participantes; realizar novas rodadas de validade de conteúdo a partir das mesmas ou novas unidades de contexto extraídas [Ferreira et al. 2025]; promover aplicações-piloto do instrumento com grupos específicos, testando a capacidade de julgamento e execução das atividades propostas; ou confrontar as afirmações validadas frente a frameworks de referência,

como COBIT, ISO/IEC 27001 ou NIST, de modo a expandir sua aplicabilidade e robustez no diagnóstico dos papéis da auditoria interna em cibersegurança no setor público.

Referências

Lynn, Mary R. [1986]. "Determination and quantification of content validity". Em: *Nursing Research* 35.6, pp. 382–385. DOI: 10.1097/00006199-198611000-00017. [Acesso em 05/06/2025].

Gil, Antonio Carlos [2008]. *Como elaborar projetos de pesquisa*. 4ª ed. São Paulo: Atlas.

Alexandre, Neusa Maria Costa e Marina Zambon Orpinelli Coluci [2011]. "Validade de conteúdo nos processos de construção e adaptação de instrumentos de medidas". Em: *Ciência Saúde Coletiva* 16.7, pp. 3061–3068. URL: https://www.scielo.br/j/csc/a/8SwTdhcvF8vYv9dFSZcCk3P/abstract/?lang=pt [acesso em 10/05/2025].

Steinbart, Paul John et al. [2012]. "The relationship between internal audit and information security: An exploratory investigation". Em: *International Journal of Accounting Information Systems* 13.3, pp. 228–243. DOI: 10.1016/j.accinf.2012.06.007. URL: https://doi.org/10.1016/j.accinf.2012.06.007 [acesso em 10/06/2025].

Bardin, Laurence [2016]. *Análise de Conteúdo*. São Paulo, Brazil: Edições 70—Almedina Brasil.

Ministério do Planejamento, Orçamento e Gestão (MP) and Controladoria-Geral da União (CGU) [mai. de 2016]. *Instrução Normativa Conjunta MP/CGU Nº 01, de 10 de maio de 2016*. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. URL: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/22234568/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-22234515 [acesso em 15/06/2025].

Islam, Md. Shariful e Thomas Stafford [2017]. "Information Technology (IT) Integration and Cybersecurity/Security: The Security Savviness of Board of Directors". Em: *Twenty-third Americas Conference on Information Systems (AMCIS 2017)*. Emergent Research Forum Paper. Boston, USA, pp. 1–5. URL: https://aisel.aisnet.org/amcis2017/ISSecurity/Presentations/23/ [acesso em 20/06/2025].

Ministério da Transparência e Controladoria-Geral da União (CGU). Secretaria Federal de Controle Interno (SFC) [dez de 2017]. *Manual de orientações técnicas da atividade de auditoria interna governamental do poder executivo federal*. Este manual orienta tecnicamente órgãos e unidades do Sistema de Controle Interno do Poder Executivo Federal (SCI) e as auditorias internas singulares sobre como operacionalizar o Referencial Técnico. Distrito Federal. URL: https://repositorio.cgu.gov.br/handle/1/64815 [acesso em 28/05/2025].

Islam, Md. Shariful, Nusrat Farah e Thomas F. Stafford [2018]. “Factors associated with security/cybersecurity audit by internal audit function: An international study”. Em: *Managerial Auditing Journal* 33.4, pp. 377–409. DOI: 10.1108/MAJ-07-2017-1595. URL: https://doi.org/10.1108/MAJ-07-2017-1595 [acesso em 02/04/2025].

Steinbart, Paul John et al. [2018]. “The influence of a good relationship between the internal audit and information security functions on information security outcomes”. Em: *Accounting, Organizations and Society* 72, pp. 1–15. DOI: 10.1016/j.aos.2018.04.005. URL: https://doi.org/10.1016/j.aos.2018.04.005 [acesso em 25/06/2025].

Lois, Petros et al. [2020]. “Internal audits in the digital era: opportunities, risks and challenges”. Em: *EuroMed Journal of Business* 15.2, pp. 205–217. DOI: 10.1108/EMJB-07-2019-0097. URL: https://doi.org/10.1108/EMJB-07-2019-0097 [acesso em 21/06/2025].

The Institute of Internal Auditors (IIA) [set. de 2020a]. *Assessing Cybersecurity Risk: The Three Lines Model*. Rel. técn. Bradley C. Ames et al. Lake Mary, FL, USA: The Institute of Internal Auditors. URL: https://www.theiia.org/globalassets/documents/standards-guidance/practice-guides/gtag-assessing-cybersecurity-risk.pdf [acesso em 14/04/2025].

— [jul. de 2020b]. *O Modelo das Três Linhas do IIA*. Rel. técn. The Institute of Internal Auditors. URL: https://www.theiia.org/globalassets/documents/translations/portuguese-brazil/o-modelo-das-tres-linhas-do-iia.pdf [acesso em 10/05/2025].

Bantleon, Ulrich et al. [2021]. “Coordination challenges in implementing the three lines of defense model”. Em: *International Journal of Auditing* 25.1, pp. 59–74. DOI: 10.1111/ijau.12201. URL: https://onlinelibrary.wiley.com/doi/10.1111/ijau.12201 [acesso em 12/06/2025].

Slapničar, Sergeja et al. [2022]. “Effectiveness of cybersecurity audit”. Em: *International Journal of Accounting Information Systems* 44, p. 100548. DOI: 10.1016/j.accinf.2021.100548. URL: https://doi.org/10.1016/j.accinf.2021.100548 [acesso em 28/04/2025].

Alves, Renato Solimar, Carlos Eduardo Mancini Queiroz e Rafael Rabelo Nunes [jul. de 2023]. “Os tribunais têm estrutura para gerenciar riscos de segurança da informação? Um estudo à luz das Três Linhas”. Em: *Revista CEJ* XXVII.86, pp. 145–160. URL: https://revistadecej.cjf.jus.br/cej/article/view/2838 [acesso em 16/06/2025].

Vazzoler-Mendonça, Adriana, Carina Alexandra Rondini e Cristina Costa-Lobo [2023]. “Procedimento de avaliação de instrumentos por comitê de juízes especialistas para aprimoramento de coleta de dados”. Em: *Revista GESTO-DEBATE* 23.3, pp. 47–86. URL: https://www.gestodebate.org.br/ [acesso em 10/06/2025].

Controladoria-Geral da União (CGU) [ago. de 2024]. *Portaria nº 2.821, de 29 de agosto de 2024*. Dispõe sobre competências na atividade de auditoria interna governamental do Poder Executivo Federal. URL: https://www.in.gov.br/en/web/dou/-/portaria-n-2.821-de-29-de-agosto-de-2024-581189836 [acesso em 08/06/2025].

PwC [2024]. *2025 Global Digital Trust Insights: Bridging the gaps to cyber resilience. The C-suite playbook*. Relatório global sobre confiança digital e resiliência cibernética. PwC. URL: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html [acesso em 16/06/2025].

Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos [dez de 2024]. *Guia do Framework de Privacidade e Segurança da Informação*. Versão 1.1.4. Equipe Técnica de Elaboração: Adriano de Andrade Moura et al. Brasília. URL: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos [acesso em 08/04/2025].

Tribunal de Contas da União (TCU) [2024]. *Lista de Alto Risco da Administração Pública Federal: 2ª edição*. Relatório elaborado pelo TCU apresentando 29 áreas críticas com riscos significativos para a Administração Pública Federal. Brasília: Tribunal de Contas da União. URL: https://sites.tcu.gov.br/listadealtorisco [acesso em 20/06/2025].

Vuko, Tina et al. [2024]. "Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective". Em: *International Journal of Auditing*, pp. 1–19. DOI: 10.1111/ijau.12365. URL: https://onlinelibrary.wiley.com/doi/10.1111/ijau.12365 [acesso em 22/05/2025].

Controladoria-Geral da União (CGU) [mai. de 2025]. *Portaria nº 1.436, de 9 de maio de 2025*. Dispõe sobre responsabilidades no processo de Gestão de Riscos e Controles Internos no âmbito do Poder Executivo federal. URL: https://www.in.gov.br/en/web/dou/-/portaria-n-1.436-de-9-de-maio-de-2025-628919820 [acesso em 15/06/2025].

CrowdStrike, Inc. [2025]. *CrowdStrike 2025 Global Threat Report*. Industry report on global cyber threats, adversary trends, and defense strategies. CrowdStrike, Inc. URL: https://www.crowdstrike.com/resources/reports/global-threat-report/ [acesso em 16/06/2025].

Ferreira, Lucas Vinicius Andrade et al. [2025]. "Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions". Em: *Applied Sciences* 15.10, p. 5715. DOI: 10.3390/app15105715. URL: https://doi.org/10.3390/app15105715 [acesso em 16/06/2025].