

## NORMAS INTERNACIONAIS PARA A PRÁTICA PROFISSIONAL DE AUDITORIA INTERNA (NORMAS)

### Introdução às Normas

A auditoria interna é conduzida em diversos ambientes jurídicos e culturais; para organizações que variam em propósito, porte, complexidade e estrutura; e por pessoas internas ou externas à organização. Embora diferenças possam afetar a prática de auditoria interna em cada ambiente, a conformidade com as *Normas Internacionais para a Prática Profissional de Auditoria Interna* do The IIA (*Normas*) é essencial para o cumprimento das responsabilidades dos auditores internos e da atividade de auditoria interna.

Os propósitos das *Normas* são:

1. Orientar a conformidade com os elementos mandatórios do *International Professional Practices Framework*.
2. Fornecer um *framework* para a execução e a promoção de um amplo espectro de serviços de auditoria interna de valor agregado.
3. Estabelecer as bases para a avaliação do desempenho da auditoria interna.
4. Promover a melhoria dos processos e operações das organizações.

As *Normas* formam um conjunto de requisitos mandatórios, baseados em princípios, que compreende:

- Declarações dos requisitos fundamentais para a prática profissional de auditoria interna e para a avaliação da eficácia do desempenho, que são internacionalmente aplicáveis nos níveis organizacional e individual.
- Interpretações que esclarecem termos ou conceitos contidos nas *Normas*.

As *Normas*, em conjunto com o Código de Ética, abrangem todos os elementos mandatórios do *International Professional Practices Framework*; portanto, a conformidade com o Código de Ética e com as *Normas* demonstra a conformidade com todos os elementos mandatórios do *International Professional Practices Framework*.

As *Normas* empregam termos especificamente definidos no Glossário. É necessário considerar os significados específicos do Glossário para entender e aplicar corretamente as *Normas*. Além disso, as *Normas* utilizam a palavra “deve” para especificar um requisito incondicional e a palavra “deveria” quando se espera conformidade, a não ser que, ao aplicar o julgamento profissional, as circunstâncias justifiquem o desvio.

As *Normas* compreendem duas categorias principais: Normas de Atributos e Normas de Desempenho. As Normas de Atributos abordam as características das organizações e dos indivíduos que exerçam auditoria interna. As Normas de Desempenho descrevem a natureza da auditoria interna e fornecem critérios de qualidade em comparação com os quais o desempenho desses serviços possa ser mensurado. As Normas de Atributos e de Desempenho aplicam-se a todos os serviços de auditoria interna.

As Normas de Implantação expandem as Normas de Atributos e de Desempenho, fornecendo os requisitos aplicáveis aos serviços de avaliação (.A) ou de consultoria (.C).

Os serviços de avaliação envolvem a avaliação objetiva das evidências pelo auditor interno, a fim de fornecer opiniões ou conclusões a respeito de uma entidade, operação, função, processo, sistema ou outros temas. A natureza e o escopo de um trabalho de avaliação são determinados pelo auditor interno. Geralmente, três partes participam dos serviços de avaliação: (1) a pessoa ou o grupo diretamente envolvido com a entidade, operação, função, processo, sistema ou outro tema – o responsável pelo processo, (2) a pessoa ou grupo que realiza a avaliação – o auditor interno, (3) a pessoa ou grupo que utiliza a avaliação – o usuário.

Os serviços de consultoria são, por natureza, de assessoria e, geralmente, são realizados a partir da solicitação específica de um cliente do trabalho. A natureza e o escopo dos trabalhos de consultoria estão sujeitos a um acordo com o cliente do trabalho. Geralmente, os serviços de consultoria envolvem duas partes: (1) a pessoa ou grupo que oferece a assessoria – o auditor interno, e (2) a pessoa ou grupo que busca e recebe a assessoria – o cliente do trabalho de auditoria. Ao prestar serviços de consultoria, o auditor interno deveria manter a objetividade e não assumir responsabilidade de gestão.

As *Normas* aplicam-se a auditores internos individualmente e à atividade de auditoria interna. Todos os auditores internos são responsáveis pela conformidade com as normas relacionadas à objetividade, proficiência e zelo profissional devido individuais e com as normas que sejam relevantes para o desempenho das suas responsabilidades profissionais. Adicionalmente, os chefes executivos de auditoria são responsáveis pela conformidade geral da atividade de auditoria interna com as *Normas*.

Se os auditores internos ou a atividade de auditoria interna estiverem proibidos, pela lei ou por regulamentos, de seguir determinadas partes das *Normas*, a conformidade com todas as demais partes das *Normas* e as divulgações apropriadas são necessárias.

Se as *Normas* forem usadas em conjunto com requisitos emitidos por outros órgãos competentes, as comunicações de auditoria interna também podem citar o uso de outros requisitos, conforme apropriado. Nesse caso, se a atividade de auditoria interna indicar a conformidade com as *Normas* e existirem inconsistências entre as *Normas* e outros requisitos, os auditores internos e a atividade de auditoria interna devem estar em conformidade com as *Normas* e podem estar em conformidade com outros requisitos, se tais requisitos forem mais restritivos.

A revisão e o desenvolvimento das *Normas* é um processo contínuo. O *International Internal Audit Standards Board* realiza extensa consulta e discussão antes de publicar as *Normas*. Isso inclui a solicitação de comentários do público de todas as partes do mundo através de um processo de exposição de rascunho. Todos os rascunhos de exposição são postados no website do The IIA e distribuídos a todos os institutos afiliados ao The IIA.

Sugestões e comentários em relação às *Normas* podem ser enviados para:

The Institute of Internal Auditors  
*Standards and Guidance*  
1035 Greenwood Blvd, Suite 401  
Lake Mary, FL 32746 USA

E-mail: [guidance@theiia.org](mailto:guidance@theiia.org)

Site: [www.globaliia.org](http://www.globaliia.org)

\*\*\*

## **NORMAS DE ATRIBUTOS**

### **1000 – Propósito, Autoridade e Responsabilidade**

O propósito, a autoridade e a responsabilidade da atividade de auditoria interna devem estar formalmente definidos em um estatuto de auditoria interna, consistente com a Missão da Auditoria Interna e os elementos mandatários do International Professional Practices Framework (os Princípios Fundamentais para a Prática Profissional de Auditoria Interna, o Código de Ética, as Normas e a Definição de Auditoria Interna). O chefe executivo de auditoria deve revisar periodicamente o estatuto de auditoria interna e submetê-lo à aprovação da alta administração e do conselho.

#### **Interpretação:**

*O estatuto de auditoria interna é um documento formal, que define o propósito, a autoridade e a responsabilidade da atividade de auditoria interna. O estatuto de auditoria interna estabelece a posição da atividade de auditoria interna dentro da organização, incluindo a natureza do reporte funcional do chefe executivo de auditoria ao conselho; autoriza o acesso aos registros, ao pessoal e às instalações físicas relevantes para o desempenho dos trabalhos de auditoria; e define o escopo das atividades de auditoria interna. A aprovação final do estatuto de auditoria interna é de responsabilidade do conselho.*

**1000.A1** – A natureza dos serviços de avaliação prestados à organização deve ser definida no estatuto de auditoria interna. Se for necessária a prestação de serviços de avaliação a partes externas à organização, a natureza dessas avaliações também deve ser definida no estatuto de auditoria interna.

**1000.C1** – A natureza dos serviços de consultoria deve ser definida no estatuto de auditoria interna.

### **1010 – Reconhecendo as Orientações Mandatórias no Estatuto de Auditoria Interna**

A natureza mandatória dos Princípios Fundamentais para a Prática Profissional de Auditoria Interna, do Código de Ética, das Normas e da Definição de Auditoria Interna deve ser reconhecida no estatuto de auditoria interna. O chefe executivo de auditoria deveria discutir a Missão da Auditoria Interna e os elementos mandatários do *International Professional Practices Framework* com a alta administração e com o conselho.

### **1100 – Independência e Objetividade**

A atividade de auditoria interna deve ser independente e os auditores internos devem ser objetivos ao executar seus trabalhos.

#### **Interpretação:**

*A independência é a liberdade de condições que ameacem a habilidade da atividade de auditoria interna de cumprir com as responsabilidades de auditoria interna de maneira imparcial. Para atingir o grau de independência necessário para cumprir com eficácia com as responsabilidades da atividade de auditoria interna, o chefe executivo de auditoria tem acesso direto e irrestrito à alta administração e ao conselho. Isso pode ser alcançado por meio de uma relação de duplo reporte. As ameaças à independência devem ser gerenciadas nos níveis do auditor individual, do trabalho de auditoria, funcional e organizacional.*

*A objetividade é uma atitude mental imparcial que permite que os auditores internos executem os trabalhos de auditoria de forma que confiem no resultado de seu trabalho e que não haja qualquer prejuízo à qualidade. A objetividade requer que os auditores internos não subordinem a outros o seu julgamento em assuntos de auditoria. As ameaças à objetividade devem ser gerenciadas nos níveis do auditor individual, do trabalho de auditoria, funcional e organizacional.*

### **1110 – Independência Organizacional**

O chefe executivo de auditoria deve reportar a um nível dentro da organização que permita à atividade de auditoria interna cumprir com suas responsabilidades. O chefe executivo de auditoria deve confirmar junto ao conselho, pelo menos anualmente, a independência organizacional da atividade de auditoria interna.

**Interpretação:**

*A independência organizacional é alcançada de forma eficaz quando o chefe executivo de auditoria reporta funcionalmente ao conselho. Exemplos de reporte funcional ao conselho implicam que o conselho:*

- *Aprove o estatuto de auditoria interna.*
- *Aprove o plano de auditoria baseado em riscos.*
- *Aprove o orçamento e o plano de recursos da auditoria interna.*
- *Receba comunicações do chefe executivo de auditoria sobre o desempenho da atividade de auditoria interna em relação ao seu plano e outros assuntos.*
- *Aprove as decisões referentes à nomeação e demissão do chefe executivo de auditoria.*
- *Aprove a remuneração do chefe executivo de auditoria.*
- *Faça os devidos questionamentos à gestão e ao chefe executivo de auditoria, para determinar se há limitações inapropriadas de escopo ou de recursos.*

**1110.A1** – A atividade de auditoria interna deve estar livre de interferências na determinação do escopo da auditoria interna, na execução do trabalho e na comunicação dos resultados. O chefe executivo de auditoria deve divulgar tal interferência ao conselho e discutir as consequências.

**1111 – Interação Direta com o Conselho**

O chefe executivo de auditoria deve se comunicar e interagir diretamente com o conselho.

**1112 – Papéis do Chefe Executivo de Auditoria Além da Auditoria Interna**

Nos casos em que o chefe executivo de auditoria assumir, ou houver a expectativa de que assuma, papéis e/ou responsabilidades que vão além da auditoria interna, devem existir salvaguardas em prática para limitar o prejuízo à independência ou à objetividade.

**Interpretação:**

*Pode-se solicitar ao chefe executivo de auditoria que assuma outros papéis e responsabilidades além da auditoria interna, tais como a responsabilidade pelas atividades de conformidade ou gerenciamento de riscos. Esses papéis e responsabilidades podem prejudicar, ou parecer prejudicar, a independência organizacional da atividade de auditoria interna ou a objetividade individual do auditor interno. Salvaguardas são aquelas atividades de supervisão, frequentemente realizadas pelo conselho, para lidar com esses prejuízos potenciais, e podem incluir atividades como a avaliação periódica das linhas de reporte e das responsabilidades, assim como o desenvolvimento de processos alternativos para obtenção de avaliações relacionadas às áreas de responsabilidade adicional.*

**1120 – Objetividade Individual**

Os auditores internos devem ter uma atitude imparcial e isenta, e evitar qualquer conflito de interesses.

**Interpretação:**

*O conflito de interesses é uma situação na qual um auditor interno, que esteja em uma posição de confiança, tenha um interesse profissional ou pessoal conflitante. Tais interesses conflitantes podem dificultar o exercício imparcial de seus deveres. Um conflito de interesses pode existir, mesmo sem resultar em qualquer ato antiético ou impróprio. Um conflito de interesses pode criar uma aparência de impropriedade que pode abalar a confiança no auditor interno, na atividade de auditoria interna e na profissão. Um conflito de interesses poderia prejudicar a habilidade do indivíduo de cumprir com seus deveres e responsabilidades de forma objetiva.*

**1130 – Prejuízo à Independência ou à Objetividade**

Caso a independência ou a objetividade seja prejudicada de fato ou aparentemente, os detalhes de tal prejuízo devem ser divulgados às partes apropriadas. A natureza da divulgação dependerá do tipo de prejuízo.

**Interpretação:**

*O prejuízo à independência organizacional e à objetividade individual pode incluir, mas não se limita a um conflito de interesses pessoal, limitações de escopo, restrições de acesso aos registros, pessoal e instalações, e limitações de recursos, tais como verbas.*

*A determinação das partes apropriadas às quais os detalhes do prejuízo à independência ou à objetividade devem ser divulgados depende das expectativas relativas à responsabilidade da atividade de auditoria interna e do chefe executivo de auditoria junto à alta administração e ao conselho, conforme descritas no estatuto de auditoria interna, assim como da natureza do prejuízo.*

**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.

**1130.A2** – Os trabalhos de avaliação de funções pelas quais o chefe executivo de auditoria seja responsável devem ser supervisionados por uma parte externa à atividade de auditoria interna.

**1130.A3** – A atividade de auditoria interna pode prestar serviços de avaliação onde anteriormente tenha executado serviços de consultoria, desde que a natureza da consultoria não tenha prejudicado a objetividade e que a objetividade individual seja gerenciada ao designar recursos ao trabalho de auditoria.

**1130.C1** – Os auditores internos podem prestar serviços de consultoria em relação a operações pelas quais tenham sido responsáveis anteriormente.

**1130.C2** – Caso os auditores internos tenham prejuízos em potencial à independência ou à objetividade em relação aos serviços de consultoria propostos, deve ser feita divulgação ao cliente do trabalho de auditoria antes da aceitação do trabalho de auditoria.

## **1200 – Proficiência e Zelo Profissional Devido**

Os trabalhos de auditoria devem ser executados com proficiência e zelo profissional devido.

### **1210 – Proficiência**

Os auditores internos devem possuir o conhecimento, as habilidades e outras competências necessárias ao desempenho de suas responsabilidades individuais. A atividade de auditoria interna deve possuir ou obter coletivamente o conhecimento, as habilidades e outras competências necessárias ao desempenho de suas responsabilidades.

#### **Interpretação:**

*Proficiência é um termo coletivo que se refere ao conhecimento, às habilidades e a outras competências exigidas dos auditores internos para que cumpram com suas responsabilidades profissionais com eficácia. Ela engloba a consideração de atividades atuais, tendências e questões emergentes, para possibilitar a assessoria e recomendações relevantes. Os auditores internos são encorajados a demonstrar sua proficiência por meio da obtenção das certificações e qualificações profissionais apropriadas, tais como a designação de Certified Internal Auditor e outras certificações oferecidas pelo The Institute of Internal Auditors e por outras organizações profissionais apropriadas.*

**1210.A1** – O chefe executivo de auditoria deve obter assessoria e assistência qualificadas, caso os auditores internos não possuam o conhecimento, as habilidades ou outras competências necessárias à realização de todo ou de parte do trabalho de auditoria.

**1210.A2** – Os auditores internos devem possuir conhecimento suficiente para avaliar o risco de fraude e a forma como esse risco é gerenciado pela organização, mas não se espera que possuam a expertise de uma pessoa cuja principal responsabilidade seja detectar e investigar fraudes.

**1210.A3** – Os auditores internos devem possuir conhecimento suficiente sobre os principais riscos e controles de tecnologia da informação e sobre as técnicas de auditoria baseadas em tecnologia disponíveis para a execução de seus trabalhos. Entretanto, não se espera que todos os auditores internos tenham a expertise de um auditor interno cuja principal responsabilidade seja a auditoria de tecnologia da informação.

**1210.C1** – O chefe executivo de auditoria deve recusar o trabalho de consultoria, ou obter assessoria e assistência competentes, caso os auditores internos não possuam o conhecimento, as habilidades ou outras competências necessárias à realização de todo ou de parte do trabalho de auditoria.

### **1220 – Zelo Profissional Devido**

Os auditores internos devem empregar o zelo e as habilidades esperados de um auditor interno razoavelmente prudente e competente. O zelo profissional devido não implica infalibilidade.

**1220.A1** – Os auditores internos devem exercer o zelo profissional devido, ao considerar:

- A extensão de trabalho necessária para alcançar os objetivos do trabalho de auditoria.
- A relativa complexidade, materialidade ou significância das questões às quais os procedimentos de avaliação são aplicados.
- A adequação e a eficácia dos processos de governança, de gerenciamento de riscos e de controle.
- A probabilidade de erros, fraudes ou não conformidades significantes.
- O custo da avaliação em relação aos potenciais benefícios.

**1220.A2** – No exercício do zelo profissional devido, os auditores internos devem considerar a utilização da auditoria baseada em tecnologia e de outras técnicas de análise de dados.

**1220.A3** – Os auditores internos devem estar alertas aos riscos significantes que poderiam afetar os objetivos, as operações ou os recursos. Entretanto, os procedimentos de avaliação isoladamente, mesmo quando realizados com o zelo profissional devido, não garantem que todos os riscos significantes sejam identificados.

**1220.C1** – Os auditores internos devem exercer o zelo profissional devido durante um trabalho de consultoria, ao considerar:

- As necessidades e as expectativas dos clientes, incluindo a natureza, a ocasião e a comunicação dos resultados do trabalho de auditoria.
- A relativa complexidade e extensão do trabalho necessárias para alcançar os objetivos do trabalho.
- O custo do trabalho de consultoria em relação aos potenciais benefícios.

### **1230 – Desenvolvimento Profissional Contínuo**

Os auditores internos devem aperfeiçoar seus conhecimentos, habilidades e outras competências através do desenvolvimento profissional contínuo.

### **1300 – Programa de Avaliação e Melhoria da Qualidade**

O chefe executivo de auditoria deve desenvolver e manter um programa de avaliação e melhoria da qualidade que cubra todos os aspectos da atividade de auditoria interna.

#### **Interpretação:**

*Um programa de avaliação e melhoria da qualidade é criado para permitir uma avaliação da conformidade da atividade de auditoria interna com as Normas e se os auditores internos seguem o Código de Ética. O programa também avalia a eficiência e a eficácia da atividade de auditoria interna e identifica oportunidades de melhoria. O chefe executivo de auditoria deveria encorajar a supervisão do programa de avaliação e melhoria da qualidade por parte do conselho.*

### **1310 – Requisitos do Programa de Avaliação e Melhoria da Qualidade**

O programa de avaliação e melhoria da qualidade deve incluir avaliações internas e externas.

#### **1311 – Avaliações Internas**

As avaliações internas devem incluir:

- Monitoramento contínuo do desempenho da atividade de auditoria interna.
- Autoavaliações, ou avaliações realizadas por outras pessoas de dentro da organização com conhecimento suficiente das práticas de auditoria interna, periódicas.

#### **Interpretação:**

*O monitoramento contínuo é uma parte integrante da rotina diária de supervisão, revisão e mensuração da atividade de auditoria interna. O monitoramento contínuo está incorporado às políticas e às práticas rotineiras utilizadas para gerenciar a atividade de auditoria interna e usa os processos, as ferramentas e as informações considerados necessários para avaliar a conformidade com o Código de Ética e com as Normas.*

*As avaliações periódicas são conduzidas para avaliar a conformidade com o Código de Ética e com as Normas.*

*O conhecimento suficiente das práticas de auditoria interna requer, pelo menos, a compreensão de todos os elementos do International Professional Practices Framework.*

### **1312 – Avaliações Externas**

As avaliações externas devem ser realizadas pelo menos uma vez a cada cinco anos, por um avaliador ou equipe de avaliação qualificada e independente, externa à organização. O chefe executivo de auditoria deve discutir com o conselho:

- A forma e a frequência da avaliação externa.
- A qualificação e a independência do avaliador externo, ou equipe de avaliação, incluindo qualquer potencial conflito de interesses.

#### **Interpretação:**

*As avaliações externas podem ser realizadas por meio de uma avaliação externa completa ou por uma autoavaliação com validação externa independente. O avaliador externo deve concluir quanto à conformidade com o Código de Ética e com as Normas; a avaliação externa pode também incluir comentários operacionais ou estratégicos.*

*Um avaliador ou equipe de avaliação qualificada demonstra sua competência em duas áreas: a prática profissional de auditoria interna e o processo de avaliação externa. A competência pode ser demonstrada por meio de uma combinação de experiência e aprendizado teórico. A experiência obtida em organizações similares em porte, complexidade, setor ou indústria e questões técnicas tem maior valor que experiências menos relevantes. No caso de uma equipe de avaliação, não é necessário que todos os membros da equipe possuam todas as competências; e sim que a equipe como um todo seja qualificada. O chefe executivo de auditoria utiliza o julgamento profissional para avaliar se o avaliador ou equipe de avaliação apresenta competência suficiente para que seja considerada qualificada.*

*Avaliador (ou equipe de avaliação) independente significa não ter qualquer conflito de interesses real ou aparente, e não fazer parte ou não estar sob o controle da organização à qual a atividade de auditoria interna pertence. O chefe executivo de auditoria deveria encorajar a supervisão da avaliação externa por parte do conselho, para reduzir conflitos de interesses percebidos ou em potencial.*

### **1320 – Divulgações do Programa de Avaliação e Melhoria da Qualidade**

O chefe executivo de auditoria deve comunicar os resultados do programa de avaliação e melhoria da qualidade à alta administração e ao conselho. A divulgação deveria incluir:

- O escopo e a frequência das avaliações internas e externas.
- As qualificações e a independência do(s) avaliador(es) ou equipe de avaliação, incluindo potenciais conflitos de interesses.
- As conclusões dos avaliadores.
- Planos de ações corretivas.

#### **Interpretação:**

*A forma, o conteúdo e a frequência da comunicação dos resultados do programa de avaliação e melhoria da qualidade são estabelecidos através de discussões com a alta administração e com o conselho e consideram as responsabilidades da atividade de auditoria interna e do chefe executivo de auditoria, como dispostas no estatuto de auditoria interna. Para demonstrar a conformidade com o Código de Ética e com as Normas, os resultados das avaliações externas e das avaliações internas periódicas são comunicados tão logo essas avaliações sejam concluídas e os resultados*

do monitoramento contínuo são comunicados pelo menos anualmente. Os resultados incluem o parecer do avaliador, ou da equipe de avaliação, quanto ao grau de conformidade.

### **1321 – Uso de “Em Conformidade com as Normas Internacionais para a Prática Profissional de Auditoria Interna”**

A indicação de que a atividade de auditoria interna está em conformidade com as *Normas Internacionais para a Prática Profissional de Auditoria Interna* é apropriada somente se for corroborada pelos resultados do programa de avaliação e melhoria da qualidade.

#### **Interpretação:**

*A atividade de auditoria interna está em conformidade com o Código de Ética e com as Normas quando atinge os resultados neles descritos. Os resultados do programa de avaliação e melhoria da qualidade incluem os resultados das avaliações internas e externas. Todas as atividades de auditoria interna terão resultados de avaliações internas. As atividades de auditoria interna com no mínimo cinco anos de existência também terão resultados de avaliações externas.*

### **1322 – Divulgação de Não Conformidade**

Quando a não conformidade com o Código de Ética ou com as *Normas* impactar o escopo geral ou a operação da atividade de auditoria interna, o chefe executivo de auditoria deve divulgar a não conformidade e seu impacto à alta administração e ao conselho.

## **NORMAS DE DESEMPENHO**

### **2000 – Gerenciamento da Atividade de Auditoria Interna**

O chefe executivo de auditoria deve gerenciar de forma eficaz a atividade de auditoria interna, para garantir que agregue valor à organização.

#### **Interpretação:**

*A atividade de auditoria interna é gerenciada de forma eficaz quando:*

- *Cumpra com o propósito e a responsabilidade incluídos no estatuto de auditoria interna.*
- *Está em conformidade com as Normas.*
- *Seus membros, individualmente, demonstram conformidade com o Código de Ética e com as Normas.*
- *Considera tendências e questões emergentes que poderiam impactar a organização.*

*A atividade de auditoria interna agrega valor à organização e aos seus stakeholders quando considera estratégias, objetivos e riscos; empenha-se para oferecer formas de melhorar os processos de governança, gerenciamento de riscos e controle; e presta, de forma objetiva, serviços relevantes de avaliação.*

### **2010 – Planejamento**

O chefe executivo de auditoria deve estabelecer um plano baseado em riscos para determinar as prioridades da atividade de auditoria interna, de forma consistente com as metas da organização.

#### **Interpretação:**

*Para desenvolver o plano baseado em riscos, o chefe executivo de auditoria se reúne com a alta administração e com o conselho e adquire um entendimento das estratégias, principais objetivos de negócios, riscos associados e processos de gerenciamento de riscos da organização. O chefe executivo de auditoria deve revisar e ajustar o plano conforme necessário, em resposta às mudanças no negócio, nos riscos, nas operações, nos programas, nos sistemas e nos controles da organização.*

**2010.A1** – O plano dos trabalhos da atividade de auditoria interna deve ser baseado em uma avaliação de riscos documentada, realizada pelo menos anualmente. As contribuições da alta administração e do conselho devem ser consideradas nesse processo.

**2010.A2** – O chefe executivo de auditoria deve identificar e considerar as expectativas da alta administração, do conselho e de outros stakeholders em relação às opiniões e outras conclusões da auditoria interna.

**2010.C1** – O chefe executivo de auditoria deveria considerar aceitar trabalhos de consultoria propostos, de acordo com o potencial desses trabalhos de melhorar o gerenciamento dos riscos, agregar valor e melhorar as operações da organização. Os trabalhos aceitos devem ser incluídos no plano.

#### **2020 – Comunicação e Aprovação**

O chefe executivo de auditoria deve comunicar os planos e requisitos de recursos da atividade de auditoria interna, incluindo mudanças intermediárias significantes, à alta administração e ao conselho para revisão e aprovação. O chefe executivo de auditoria também deve comunicar o impacto das limitações de recursos.

#### **2030 – Gerenciamento de Recursos**

O chefe executivo de auditoria deve assegurar que os recursos de auditoria interna sejam apropriados, suficientes e aplicados de forma eficaz para o cumprimento do plano aprovado.

#### **Interpretação:**

*O termo “apropriado” refere-se à combinação de conhecimentos, habilidades e outras competências necessários para executar o plano. O termo “suficiente” refere-se à quantidade de recursos necessária para cumprir com o plano. Os recursos são “aplicados de forma eficaz” quando são utilizados de forma a otimizar o cumprimento do plano aprovado.*

#### **2040 – Políticas e Procedimentos**

O chefe executivo de auditoria deve estabelecer políticas e procedimentos para orientar a atividade de auditoria interna.

#### **Interpretação:**

*A forma e o conteúdo das políticas e procedimentos dependem do porte e da estrutura da atividade de auditoria interna e da complexidade de seu trabalho.*

#### **2050 – Coordenação e Confiança**

O chefe executivo de auditoria deveria compartilhar informações, coordenar atividades e considerar depositar confiança no trabalho de outros prestadores internos e externos de serviços de avaliação e consultoria, para assegurar a cobertura apropriada e minimizar a duplicação de esforços.

#### **Interpretação:**

*Ao coordenar as atividades, o chefe executivo de auditoria pode usar, por confiança, o trabalho de outros prestadores de serviços de avaliação e consultoria. Deveria ser estabelecido um processo consistente para embasar essa confiança e o chefe executivo de auditoria deveria considerar a competência, a objetividade e o zelo profissional devido dos prestadores de serviços de avaliação e consultoria. O chefe executivo de auditoria também deveria ter um entendimento claro do escopo, dos objetivos e dos resultados do trabalho realizado por outros prestadores de serviços de avaliação e consultoria. Quando alguma confiança for depositada no trabalho de outros, o chefe executivo de auditoria continua sujeito a prestar contas e responsável por assegurar a devida corroboração das conclusões e opiniões da atividade de auditoria interna.*

#### **2060 – Reportando à Alta Administração e ao Conselho**

O chefe executivo de auditoria deve reportar periodicamente à alta administração e ao conselho sobre o propósito, a autoridade, a responsabilidade e o desempenho da atividade de auditoria interna em relação ao plano e à conformidade com o Código de Ética e com as *Normas*. O reporte também deve incluir questões significantes de riscos e de controle, incluindo riscos de fraude, questões de governança e outros temas que exijam a atenção da alta administração e/ou do conselho.

#### **Interpretação:**

*A determinação da frequência e do conteúdo do reporte é feita de forma colaborativa pelo chefe executivo de auditoria, pela alta administração e pelo conselho. A frequência e conteúdo do reporte dependem da importância da informação a ser comunicada e da urgência das relativas ações a serem tomadas pela alta administração e/ou pelo conselho.*

*O reporte e a comunicação do chefe executivo de auditoria à alta administração e ao conselho devem incluir informações sobre:*

- *O estatuto de auditoria.*
- *A independência da atividade de auditoria interna.*
- *O plano de auditoria e o progresso em relação ao plano.*
- *Os requisitos de recursos.*
- *Os resultados das atividades de auditoria.*
- *A conformidade com o Código de Ética e com as Normas, e os planos de ação para abordar quaisquer questões significantes de conformidade.*
- *A resposta da gestão ao risco que, no julgamento do chefe executivo de auditoria, pode ser inaceitável para a organização.*

*Esses e outros requisitos de comunicação do chefe executivo de auditoria são referenciados ao longo das Normas.*

## **2070 – Prestadores Externos de Serviços e a Responsabilidade da Organização pela Auditoria Interna**

Quando um prestador externo de serviços atua como a atividade de auditoria interna, o prestador deve manter a organização ciente de que a organização continua responsável por manter uma atividade de auditoria interna eficaz.

### **Interpretação:**

*Essa responsabilidade é demonstrada através do programa de avaliação e melhoria da qualidade, que avalia a conformidade com o Código de Ética e com as Normas.*

## **2100 – Natureza do Trabalho**

A atividade de auditoria interna deve avaliar e contribuir para a melhoria dos processos de governança, gerenciamento de riscos e controle da organização, usando uma abordagem sistemática, disciplinada e baseada em riscos. A credibilidade e o valor da auditoria interna são aperfeiçoados quando os auditores são proativos, e suas avaliações oferecem novos pontos de vista e consideram o impacto futuro.

## **2110 – Governança**

A atividade de auditoria interna deve avaliar e propor recomendações apropriadas para melhorar os processos de governança da organização para:

- Tomar decisões estratégicas e operacionais.
- Supervisionar o gerenciamento de riscos e o controle.
- Promover a devida ética e valores dentro da organização.
- Garantir gerenciamento e prestação de contas eficazes quanto ao desempenho da organização.
- Comunicar informações de riscos e controle às áreas apropriadas da organização.
- Coordenar as atividades e a comunicação das informações entre o conselho, os auditores externos e internos, outros prestadores de serviços de avaliação e a gestão.

**2110.A1** – A atividade de auditoria interna deve avaliar a criação, implantação e eficácia dos objetivos, programas e atividades de ética da organização.

**2110.A2** – A atividade de auditoria interna deve avaliar se a governança de tecnologia da informação da organização apoia as estratégias e os objetivos da organização.

## **2120 – Gerenciamento de Riscos**

A atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos.

### **Interpretação:**

*Determinar se os processos de gerenciamento de riscos são eficazes é um julgamento que resulta da avaliação do auditor interno quanto a se:*

- *Os objetivos da organização apoiam e estão alinhados à missão da organização.*
- *Riscos significantes são identificados e avaliados.*
- *Respostas apropriadas aos riscos são selecionadas de forma a alinhar os riscos ao apetite a risco da organização.*
- *As informações relevantes de riscos são capturadas e comunicadas de forma tempestiva através da organização, permitindo que colaboradores, a gestão e o conselho cumpram com suas responsabilidades.*

*A atividade de auditoria interna pode coletar, ao longo de múltiplos trabalhos de auditoria, as informações para apoiar essa avaliação. Os resultados desses trabalhos de auditoria, vistos em conjunto, proporcionam uma compreensão dos processos de gerenciamento de riscos da organização e da eficácia desses processos.*

*Os processos de gerenciamento de riscos são monitorados através de atividades contínuas de gerenciamento, avaliações independentes ou ambos.*

**2120.A1** – A atividade de auditoria interna deve avaliar as exposições a risco relacionadas à governança, operações e sistemas de informação da organização, em relação à:

- Realização dos objetivos estratégicos da organização.
- Confiabilidade e integridade das informações financeiras e operacionais.
- Eficácia e eficiência das operações e dos programas.
- Salvaguarda de ativos.
- Conformidade com leis, regulamentos, políticas, procedimentos e contratos.

**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.

**2120.C1** – Durante trabalhos de consultoria, os auditores internos devem abordar o risco de forma consistente com os objetivos do trabalho de auditoria e estar alertas à existência de outros riscos significantes.

**2120.C2** – Os auditores internos devem incorporar o conhecimento sobre riscos adquirido nos trabalhos de consultoria à sua avaliação dos processos de gerenciamento de riscos da organização.

**2120.C3** – Ao auxiliar a gestão no estabelecimento ou na melhoria dos processos de gerenciamento de riscos, os auditores internos devem abster-se de assumir qualquer responsabilidade de gestão, de verdadeiramente gerenciar os riscos.

### **2130 – Controle**

A atividade de auditoria interna deve auxiliar a organização a manter controles eficazes, avaliando a eficácia e eficiência desses controles e promovendo melhorias contínuas.

**2130.A1** – A atividade de auditoria interna deve avaliar a adequação e a eficácia dos controles implantados em resposta aos riscos que afetam a governança, as operações e os sistemas de informação da organização, em relação à:

- Realização dos objetivos estratégicos da organização.
- Confiabilidade e integridade das informações financeiras e operacionais.
- Eficácia e eficiência das operações e dos programas.
- Salvaguarda de ativos.
- Conformidade com leis, regulamentos, políticas, procedimentos e contratos.

**2130.C1** – Os auditores internos devem incorporar o conhecimento sobre controles adquirido nos trabalhos de consultoria à sua avaliação dos processos de controle da organização.

### **2200 – Planejamento do Trabalho de Auditoria**

Os auditores internos devem desenvolver e documentar um plano para cada trabalho de auditoria, incluindo os objetivos, o escopo, o período e a alocação de recursos do trabalho de auditoria. O plano deve considerar as estratégias, objetivos e riscos da organização que sejam relevantes para o trabalho de auditoria.

### **2201 – Considerações de Planejamento**

No planejamento de trabalhos de auditoria, os auditores internos devem considerar:

- As estratégias e os objetivos da atividade que está sendo revisada e os meios pelos quais a atividade controla seu desempenho.
- Os riscos significantes aos objetivos, recursos e operações da atividade e os meios pelos quais o impacto potencial do risco é mantido em um nível aceitável.
- A adequação e a eficácia dos processos de governança, de gerenciamento de riscos e de controle da atividade, em comparação com um framework ou modelo relevante.
- As oportunidades de melhorias significantes nos processos de governança, gerenciamento de riscos e controle da atividade.

**2201.A1** – Ao planejar um trabalho de auditoria para partes externas à organização, os auditores internos devem estabelecer com elas um entendimento por escrito em relação aos objetivos, ao escopo, às respectivas responsabilidades e a outras expectativas, incluindo restrições na distribuição dos resultados do trabalho de auditoria e acesso aos registros do trabalho de auditoria.

**2201.C1** – Os auditores internos devem estabelecer um entendimento com os clientes do trabalho de consultoria em relação aos objetivos, ao escopo, às respectivas responsabilidades e a outras expectativas do cliente. Para trabalhos significativos, esse entendimento deve ser documentado.

## **2210 – Objetivos do Trabalho de Auditoria**

Os objetivos devem ser estabelecidos para cada trabalho de auditoria.

**2210.A1** – Os auditores internos devem conduzir uma avaliação preliminar dos riscos relevantes para a atividade sob revisão. Os objetivos do trabalho de auditoria devem refletir os resultados dessa avaliação.

**2210.A2** – Ao desenvolver os objetivos do trabalho de auditoria, os auditores internos devem considerar a probabilidade de erros, fraudes e não conformidades significantes, além de outras exposições.

**2210.A3** – São necessários critérios adequados para avaliar a governança, o gerenciamento de riscos e os controles. Os auditores internos devem determinar até que ponto a gestão e/ou o conselho estabeleceu critérios adequados para determinar se os objetivos e metas foram alcançados. Se forem adequados, os auditores internos devem utilizar tais critérios em sua avaliação. Se inadequados, os auditores internos devem identificar critérios de avaliação apropriados, por meio de discussão com a gestão e/ou com o conselho.

### **Interpretação:**

*Os tipos de critérios podem incluir:*

- *Internos (p. ex.: políticas e procedimentos da organização).*
- *Externos (p. ex.: leis e regulamentos impostos por órgãos reguladores).*
- *Principais práticas de mercado (p. ex.: orientações da indústria e da profissão).*

**2210.C1** – Os objetivos dos trabalhos de consultoria devem abordar os processos de governança, gerenciamento de riscos e controle na extensão previamente acordada com o cliente.

**2210.C2** – Os objetivos dos trabalhos de consultoria devem ser consistentes com os valores, estratégias e objetivos da organização.

## **2220 – Escopo do Trabalho de Auditoria**

O escopo estabelecido deve ser suficiente para alcançar os objetivos do trabalho de auditoria.

**2220.A1** – O escopo do trabalho de auditoria deve incluir considerações sobre sistemas, registros, pessoal e instalações físicas relevantes, incluindo aqueles(as) sob o controle de terceiros.

**2220.A2** – Se oportunidades significantes de consultoria surgirem durante um trabalho de avaliação, deveria ser produzido um entendimento específico e por escrito quanto aos

objetivos, escopo, respectivas responsabilidades e outras expectativas, e os resultados do trabalho de consultoria deveriam ser comunicados em conformidade com as normas de consultoria.

**2220.C1** – Ao executar trabalhos de consultoria, os auditores internos devem assegurar que o escopo do trabalho seja suficiente para abordar os objetivos previamente acordados. Caso os auditores internos tenham ressalvas quanto ao escopo durante o trabalho, essas ressalvas devem ser discutidas com o cliente, para se determinar se o trabalho de auditoria continuará.

**2220.C2** – Durante trabalhos de consultoria, os auditores internos devem abordar os controles de forma consistente com os objetivos do trabalho de auditoria e devem estar alertas a questões significantes de controle.

### **2230 – Alocação de Recursos ao Trabalho de Auditoria**

Os auditores internos devem determinar recursos apropriados e suficientes para alcançar os objetivos do trabalho de auditoria, com base em uma avaliação da natureza e complexidade de cada trabalho de auditoria, restrições de tempo e recursos disponíveis.

#### **Interpretação:**

*O termo “apropriado” refere-se à combinação de conhecimentos, habilidades e outras competências necessárias para executar o trabalho de auditoria. O termo “suficiente” refere-se à quantidade de recursos necessária para realizar o trabalho de auditoria com zelo profissional devido.*

### **2240 – Programa de Trabalho de Auditoria**

Os auditores internos devem desenvolver e documentar programas de trabalho que atinjam os objetivos do trabalho de auditoria.

**2240.A1** – Os programas de trabalho devem incluir procedimentos para identificar, analisar, avaliar e documentar as informações durante o trabalho de auditoria. O programa de trabalho deve ser aprovado antes de ser implantado e quaisquer ajustes devem ser prontamente aprovados.

**2240.C1** – Os programas de trabalho para trabalhos de consultoria podem variar na forma e no conteúdo, dependendo da natureza do trabalho de auditoria.

### **2300 – Realizando o Trabalho de Auditoria**

Os auditores internos devem identificar, analisar, avaliar e documentar informações suficientes para atingir os objetivos do trabalho de auditoria.

#### **2310 – Identificando Informações**

Os auditores internos devem identificar informações suficientes, confiáveis, relevantes e úteis para atingir os objetivos do trabalho de auditoria.

#### **Interpretação:**

*Informações suficientes são factuais, adequadas e convincentes, de forma que uma pessoa prudente e informada chegaria às mesmas conclusões do auditor. Informações confiáveis são as melhores informações possíveis de se obter através da utilização de técnicas apropriadas de trabalho. Informações relevantes apoiam as observações e recomendações do trabalho de auditoria e são consistentes com os objetivos do trabalho de auditoria. Informações úteis auxiliam a organização a atingir suas metas.*

#### **2320 – Análise e Avaliação**

Os auditores internos devem fundamentar as conclusões e os resultados do trabalho de auditoria com base em análises e avaliações apropriadas.

#### **2330 – Documentando Informações**

Os auditores internos devem documentar informações suficientes, confiáveis, relevantes e úteis para apoiar as conclusões e resultados do trabalho de auditoria.

**2330.A1** – O chefe executivo de auditoria deve controlar o acesso aos registros dos trabalhos de auditoria. O chefe executivo de auditoria deve obter a aprovação da alta administração

e/ou do assessor jurídico antes de liberar tais registros para partes externas, conforme apropriado.

**2330.A2** – O chefe executivo de auditoria deve desenvolver requisitos de retenção para os registros do trabalho de auditoria, independentemente do meio no qual cada registro está armazenado. Esses requisitos de retenção devem ser consistentes com as diretrizes da organização e com quaisquer outros regulamentos ou requisitos pertinentes.

**2330.C1** – O chefe executivo de auditoria deve desenvolver políticas para reger a custódia e a retenção dos registros dos trabalhos de consultoria, bem como sua liberação para partes internas e externas. Essas políticas devem ser consistentes com as diretrizes da organização e com quaisquer outros regulamentos ou requisitos pertinentes.

#### **2340 – Supervisão do Trabalho de Auditoria**

Os trabalhos de auditoria devem ser devidamente supervisionados, para assegurar que os objetivos sejam atingidos, que a qualidade seja garantida e que a equipe seja desenvolvida.

##### **Interpretação:**

*A extensão de supervisão necessária dependerá da proficiência e experiência dos auditores internos e da complexidade do trabalho de auditoria. O chefe executivo de auditoria tem a responsabilidade geral pela supervisão do trabalho de auditoria, seja ele executado por ou para a atividade de auditoria interna, mas pode designar membros da atividade de auditoria interna com a experiência apropriada para realizar a revisão. As devidas evidências da supervisão são documentadas e mantidas.*

#### **2400 – Comunicando os Resultados**

Os auditores internos devem comunicar os resultados dos trabalhos de auditoria.

#### **2410 – Critérios para as Comunicações**

As comunicações devem incluir os objetivos, escopo e resultados do trabalho de auditoria.

**2410.A1** – A comunicação final dos resultados do trabalho de auditoria deve incluir as conclusões aplicáveis, assim como recomendações e/ou planos de ação aplicáveis. Quando apropriado, a opinião dos auditores internos deveria ser fornecida. Uma opinião deve levar em consideração as expectativas da alta administração, do conselho e de outros stakeholders, e deve ser apoiada por informações suficientes, confiáveis, relevantes e úteis.

##### **Interpretação:**

*As opiniões no nível do trabalho de auditoria podem estar na forma de classificações, conclusões ou outras descrições dos resultados. Tal trabalho de auditoria pode ser relativo aos controles associados a um processo, risco ou unidade de negócios especificamente. A formulação de tais opiniões requer a consideração dos resultados do trabalho de auditoria e de sua importância.*

**2410.A2** – Os auditores internos são encorajados a reconhecer o desempenho satisfatório nas comunicações dos trabalhos de auditoria.

**2410.A3** – Ao divulgar os resultados do trabalho de auditoria para partes externas à organização, a comunicação deve incluir limitações sobre a distribuição e uso dos resultados.

**2410.C1** – A comunicação do progresso e dos resultados de um trabalho de consultoria variará em relação à forma e ao conteúdo, dependendo da natureza do trabalho e das necessidades do cliente.

#### **2420 – Qualidade das Comunicações**

As comunicações devem ser precisas, objetivas, claras, concisas, construtivas, completas e tempestivas.

##### **Interpretação:**

*Comunicações precisas são livres de erros e distorções e são fiéis aos fatos que as fundamentam. Comunicações objetivas são justas, imparciais e livres de preconceitos e são o resultado de uma*

*avaliação justa e equilibrada de todos os fatos e circunstâncias relevantes. Comunicações claras são facilmente compreendidas e lógicas, evitam linguagem técnica desnecessária e fornecem todas as informações significativas e relevantes. Comunicações concisas são objetivas e evitam elaboração desnecessária, detalhes supérfluos, redundância e prolixidade. Comunicações construtivas são úteis ao cliente do trabalho de auditoria e à organização e levam a melhorias onde sejam necessárias. Comunicações completas não omitem o que é essencial ao público-alvo e incluem todas as informações e observações significativas e relevantes que apoiam as recomendações e conclusões. Comunicações tempestivas são oportunas e convenientes, dependendo da importância da questão, permitindo à gestão tomar as ações corretivas apropriadas.*

#### **2421 – Erros e Omissões**

Se uma comunicação final contiver erro ou omissão significativa, o chefe executivo de auditoria deve comunicar a informação corrigida a todas as partes que tenham recebido a comunicação original.

#### **2430 – Uso de “Conduzido em Conformidade com as Normas Internacionais para a Prática Profissional de Auditoria Interna”**

Indicar que os trabalhos de auditoria são “conduzidos em conformidade com as Normas Internacionais para a Prática Profissional de Auditoria Interna” é apropriado somente se apoiado pelos resultados do programa de avaliação e melhoria da qualidade.

#### **2431 – Divulgação de Não Conformidade do Trabalho de Auditoria**

Quando a não conformidade com o Código de Ética ou com as Normas impactar um trabalho de auditoria específico, a comunicação dos resultados deve divulgar:

- O(s) princípio(s) ou regra(s) de conduta do Código de Ética ou Norma(s) com que não houve conformidade plena.
- A(s) razão(ões) para a não conformidade.
- O impacto da não conformidade sobre o trabalho de auditoria e sobre os resultados do trabalho de auditoria comunicados.

#### **2440 – Disseminação dos Resultados**

O chefe executivo de auditoria deve comunicar os resultados às partes apropriadas.

##### **Interpretação:**

*O chefe executivo de auditoria é responsável por revisar e aprovar a comunicação final do trabalho de auditoria antes da sua emissão e por decidir a quem e como ela será disseminada. Quando o chefe executivo de auditoria delegar essas tarefas, ele mantém a responsabilidade geral.*

**2440.A1** – O chefe executivo de auditoria é responsável pela comunicação dos resultados finais às partes que possam assegurar que os resultados recebam a devida consideração.

**2440.A2** – Se não houver exigências legais, estatutárias ou regulatórias em contrário, antes de se divulgar os resultados para partes externas à organização, o chefe executivo de auditoria deve:

- Avaliar o potencial risco à organização.
- Consultar a alta administração e/ou assessor jurídico, conforme apropriado.
- Controlar a disseminação através da restrição da utilização dos resultados.

**2440.C1** – O chefe executivo de auditoria é o responsável por comunicar os resultados finais dos trabalhos de consultoria aos clientes.

**2440.C2** – Durante trabalhos de consultoria, questões de governança, gerenciamento de riscos e controle podem ser identificadas. Sempre que essas questões forem significativas para a organização, devem ser comunicadas à alta administração e ao conselho.

#### **2450 – Opiniões Gerais**

Quando for emitida uma opinião geral, ela deve considerar as estratégias, objetivos e riscos da organização; e as expectativas da alta administração, do conselho e de outros stakeholders. A opinião geral deve estar corroborada por informações suficientes, confiáveis, relevantes e úteis.

**Interpretação:**

*A comunicação incluirá:*

- *O escopo, incluindo o período a que se refere a opinião.*
- *As limitações de escopo.*
- *A consideração de todos os projetos relacionados, incluindo a confiança em outros prestadores de serviços de avaliação.*
- *Um resumo das informações que apoiam a opinião.*
- *O framework de riscos ou controle, ou outros critérios utilizados como base para a opinião geral.*
- *A opinião, julgamento ou conclusão geral.*

*As razões para uma opinião geral desfavorável devem ser declaradas.*

**2500 – Monitorando o Progresso**

O chefe executivo de auditoria deve estabelecer e manter um sistema para monitorar a disposição dos resultados comunicados à gestão.

**2500.A1** – O chefe executivo de auditoria deve estabelecer um processo de acompanhamento para monitorar e assegurar que as ações da gestão tenham sido implantadas com eficácia ou que a alta administração tenha aceitado o risco de não se tomar qualquer ação.

**2500.C1** – A atividade de auditoria interna deve monitorar a disposição dos resultados dos trabalhos de consultoria, na extensão previamente acordada com o cliente.

**2600 – Comunicando a Aceitação de Riscos**

Quando o chefe executivo de auditoria concluir que a gestão aceitou um nível de risco que pode ser inaceitável para a organização, o chefe executivo de auditoria deve discutir a questão com a alta administração. Se o chefe executivo de auditoria determinar que a questão não foi resolvida, deve comunicá-la ao conselho.

**Interpretação:**

*A identificação de um risco aceito pela gestão pode ser observada a partir de um trabalho de avaliação ou consultoria, do monitoramento do progresso das ações adotadas pela gestão como resultado de trabalhos de auditoria anteriores ou por outros meios. Não é responsabilidade do chefe executivo de auditoria tomar decisões quanto ao risco.*

## **Glossário**

### **Agregar Valor**

A atividade de auditoria interna agrega valor à organização (e aos seus stakeholders) quando presta serviços objetivos e relevantes de avaliação, e contribui para a eficácia e eficiência dos processos de governança, gerenciamento de riscos e controle.

### **Ambiente de Controle**

A atitude e ações do conselho e da gestão em relação à importância do controle dentro da organização. O ambiente de controle proporciona a disciplina e a estrutura para o atingimento dos principais objetivos do sistema de controle interno. O ambiente de controle inclui os seguintes elementos:

- Integridade e valores éticos.
- Filosofia e estilo operacional da gestão.
- Estrutura organizacional.
- Atribuição de autoridade e responsabilidade.
- Políticas e práticas de recursos humanos.
- Competência do pessoal.

### **Apetite a Risco**

O nível de risco que uma organização está disposta a aceitar.

### **Atividade de Auditoria Interna**

Um departamento, divisão, equipe de consultores ou outros profissionais que prestem serviços independentes e objetivos de avaliação e de consultoria, criados para agregar valor e melhorar as operações de uma organização. A atividade de auditoria interna auxilia a organização a atingir seus objetivos, aplicando uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, gerenciamento de riscos e controle.

### **Chefe Executivo de Auditoria**

Chefe executivo de auditoria descreve a função de uma pessoa em posição sênior, responsável pelo gerenciamento eficaz da atividade de auditoria interna, de acordo com o estatuto de auditoria interna e com os elementos mandatários do *International Professional Practices Framework*. O chefe executivo de auditoria ou outros que reportem a ele devem ter certificações e qualificações profissionais apropriadas. O título específico do cargo e/ou responsabilidades do chefe executivo de auditoria podem variar entre as organizações.

### **Código de Ética**

O Código de Ética do *The Institute of Internal Auditors (The IIA)* é composto por Princípios relevantes à profissão e à prática de auditoria interna e por Regras de Conduta que descrevem o comportamento esperado dos auditores internos. O Código de Ética aplica-se tanto às partes quanto às entidades que prestam serviços de auditoria interna. O propósito do Código de Ética é promover uma cultura ética na profissão global de auditoria interna.

### **Conflito de Interesses**

Qualquer relacionamento que não seja, ou que aparente não ser, em prol do melhor interesse da organização. Um conflito de interesses prejudicaria a habilidade de um indivíduo de desempenhar de forma objetiva suas obrigações e responsabilidades.

### **Conformidade**

Cumprimento com as políticas, planos, procedimentos, leis, regulamentos, contratos ou outros requisitos.

### **Conselho**

O corpo administrativo de mais alto nível (p. ex.: um conselho de administração, conselho supervisor ou um conselho de gestores ou curadores) que detém a responsabilidade de dirigir e/ou supervisionar as atividades da organização e de cobrar prestação de contas por parte da alta administração. Embora os sistemas de governança variem entre jurisdições e setores, o conselho

normalmente inclui membros que não fazem parte da gestão. Se não houver um conselho, a palavra “conselho” nas *Normas* se refere a um grupo ou pessoa responsável pela governança da organização. Além disso, “conselho” nas *Normas* pode se referir a um comitê ou outro órgão ao qual o corpo administrativo tenha delegado certas funções (p. ex.: um comitê de auditoria).

### **Controle**

Qualquer ação adotada pela gestão, pelo conselho ou por outras partes, para gerenciar riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados. A gestão planeja, organiza e dirige a execução de ações suficientes para fornecer uma garantia razoável de que os objetivos e metas serão alcançados.

### **Controle Adequado**

Está presente se a gestão o tiver planejado e organizado (criado) de maneira que forneça uma garantia razoável de que os riscos da organização foram gerenciados de forma eficaz e que as metas e objetivos da organização serão alcançados eficiente e economicamente.

### **Controles de Tecnologia da Informação**

Controles que dão apoio à gestão e à governança do negócio, bem como fornecem controles gerais e técnicos sobre a infraestrutura de tecnologia da informação, tais como aplicativos, informações, infraestrutura e pessoas.

### **Deve**

As *Normas* utilizam a palavra “deve” para especificar um requisito incondicional.

### **Deveria**

As *Normas* utilizam a palavra “deveria” quando se espera conformidade, a não ser que, ao aplicar o julgamento profissional, as circunstâncias justifiquem o desvio.

### **Estatuto**

O estatuto de auditoria interna é um documento formal que define o propósito, a autoridade e a responsabilidade da atividade de auditoria interna. O estatuto de auditoria interna estabelece a posição da atividade de auditoria interna dentro da organização; autoriza o acesso aos registros, ao pessoal e às instalações físicas relevantes para o desempenho dos trabalhos de auditoria; e define o escopo das atividades de auditoria interna.

### **Fraude**

Qualquer ato ilegal caracterizado por engano, dissimulação ou quebra de confiança. Esses atos independem de ameaça de violência ou de força física. As fraudes são perpetradas por partes e organizações, a fim de se obter dinheiro, propriedades ou serviços; para evitar pagamento ou perda de serviços; ou para garantir vantagem pessoal ou de negócios.

### **Gerenciamento de Riscos**

Processo para identificar, avaliar, gerenciar e controlar potenciais eventos ou situações, para fornecer uma garantia razoável do atingimento dos objetivos da organização.

### **Governança**

Combinação de processos e estruturas implantadas pelo conselho para informar, dirigir, gerenciar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos.

### **Governança da Tecnologia da Informação**

Consiste na liderança, estruturas organizacionais e processos que asseguram que a tecnologia da informação corporativa apoie as estratégias e os objetivos da organização.

### **Independência**

A liberdade de condições que ameacem a capacidade da atividade de auditoria interna de cumprir com as responsabilidades de auditoria interna de maneira imparcial.

### **International Professional Practices Framework (Framework Internacional de Práticas Profissionais – IPPF)**

Framework conceitual que organiza as orientações oficiais promulgadas pelo The IIA. As orientações oficiais são compostas por duas categorias – (1) mandatórias e (2) recomendadas.

#### **Norma**

Um pronunciamento profissional promulgado pelo *International Internal Audit Standards Board* (Conselho Internacional de Normas de Auditoria Interna), que delinea os requisitos para a execução de um amplo espectro de atividades de auditoria interna e para a avaliação do desempenho da auditoria interna.

#### **Objetividade**

Uma atitude mental imparcial que permite que os auditores internos executem os trabalhos de auditoria de forma que confiem no resultado de seu trabalho e que não haja qualquer prejuízo à qualidade. A objetividade requer que os auditores internos não subordinem a outros o seu julgamento em assuntos de auditoria.

#### **Objetivos do Trabalho de Auditoria**

Declarações abrangentes desenvolvidas pelos auditores internos, que definem as realizações desejadas para o trabalho de auditoria.

#### **Opinião do Trabalho de Auditoria**

Classificação, conclusão e/ou outra descrição dos resultados de um trabalho de auditoria interna individual, com relação aos aspectos contidos nos objetivos e no escopo do trabalho de auditoria.

#### **Opinião Geral**

Classificação, conclusão e/ou outra descrição de resultados fornecida pelo chefe executivo de auditoria, abordando, de forma abrangente, os processos de governança, gerenciamento de riscos e/ou controle da organização. Uma opinião geral é o julgamento profissional do chefe executivo de auditoria, com base nos resultados de um conjunto de trabalhos de auditoria individuais e de outras atividades durante um intervalo específico de tempo.

#### **Prejuízo**

O prejuízo à independência organizacional e à objetividade individual pode incluir conflito de interesses pessoais, limitações de escopo, restrições de acesso aos registros, ao pessoal e às instalações, e limitações de recursos (verba).

#### **Prestador Externo de Serviços**

Uma pessoa ou empresa externa à organização, que tenha conhecimentos, habilidades e experiência especiais em uma disciplina em particular.

#### **Princípios Fundamentais para a Prática Profissional de Auditoria Interna**

Os Princípios Fundamentais para a Prática Profissional de Auditoria Interna são o alicerce do *International Professional Practices Framework* e dão apoio à eficácia da auditoria interna.

#### **Processos de Controle**

Políticas, procedimentos (manuais e automatizados) e atividades que fazem parte de um framework de controle, criados e operados para assegurar que os riscos sejam contidos no nível que uma organização esteja disposta a aceitar.

#### **Programa de Trabalho de Auditoria**

Um documento que lista os procedimentos a serem seguidos durante um trabalho de auditoria, criado para cumprir com o plano do trabalho de auditoria.

#### **Risco**

A possibilidade de ocorrer um evento que venha a ter impacto sobre o atingimento dos objetivos. O risco é mensurado em termos de impacto e probabilidade.

### **Serviços de Avaliação**

Um exame objetivo das evidências, com o propósito de fornecer à organização uma avaliação independente sobre os processos de governança, gerenciamento de riscos e controle. Exemplos podem incluir trabalhos financeiros, de desempenho, de conformidade, de segurança de sistemas e de *due diligence*.

### **Serviços de Consultoria**

Atividades de assessoria ao cliente ou serviços relacionados, cuja natureza e escopo são acordados com o cliente e destinam-se a agregar valor e melhorar os processos de governança, gerenciamento de riscos e controle da organização, sem que o auditor interno assuma responsabilidade de gestão. Exemplos incluem orientação, assessoria, facilitação e treinamento.

### **Significância**

A importância relativa de uma questão dentro do contexto no qual está sendo considerada, incluindo fatores quantitativos e qualitativos, tais como magnitude, natureza, efeito, relevância e impacto. O julgamento profissional auxilia o auditor interno a avaliar a significância de questões dentro do contexto dos objetivos relevantes.

### **Técnicas de Auditoria Baseadas em Tecnologia**

Qualquer ferramenta de auditoria automatizada, tais como software de auditoria generalizada, geradores de dados de teste, programas de auditoria computadorizada, utilitários de auditoria especializada e técnicas de auditoria auxiliadas por computador (*computer-assisted audit techniques – CAATs*).

### **Trabalho de Auditoria**

Uma atribuição, tarefa ou atividade de revisão específica de auditoria interna, tais como uma auditoria interna, revisão de autoavaliação de controle, investigação de fraude ou consultoria. Um trabalho de auditoria pode incluir múltiplas tarefas ou atividades, criadas para cumprir com um conjunto específico de objetivos relacionados.

\*\*\*