

Metodologia de Auditoria e Certificação de Informações

2018

Sumário

1. INTRODUÇÃO.....	5
2. O QUE É AUDITORIA?	10
2.1. RISCOS	15
2.1.1. <i>Fraude</i>	17
2.2. CONTROLE INTERNO	19
2.3. AUDITORIA EXTERNA	21
2.3.1. <i>Lei Sarbanes-Oxley</i>	24
2.4. AUDITORIA INTERNA.....	26
3. METODOLOGIAS DE GERENCIAMENTO DE RISCOS	31
3.1. COSO	31
3.2. COBIT 5.....	36
3.3. AS TRÊS LINHAS DE DEFESA.....	40
3.4. ISO 31000: GESTÃO DE RISCOS	44
3.5. ISO 19011: DIRETRIZES PARA AUDITORIAS DE SISTEMA E GESTÃO DA QUALIDADE.....	47
3.6. ISO 27001: SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI).....	48
4. METODOLOGIA	51
4.1. ENTENDIMENTO E MAPEAMENTO DE PROCESSOS E SUBPROCESSOS	51
5.1.1. <i>Levantamento de dados</i>	52
5.1.2. <i>Metodologia para elaboração de fluxograma</i>	52
4.2. IDENTIFICAÇÃO DE RISCOS E CONTROLE	54
4.3. REPORTAR AUSÊNCIAS DE CONTROLES INTERNOS	55
4.4. PLANO DE TESTE DOS CONTROLES IDENTIFICADOS	56
4.5. CLASSIFICAÇÃO FINAL DOS CONTROLES INTERNOS.....	61
5. REFERÊNCIAS	64

Lista de Figuras

Figura 1: Práticas de Gerenciamento de Riscos	16
Figura 2: Formas de Detecção Inicial de Fraudes.....	18
Figura 3: Diferença entre Auditoria Externa e Auditoria Interna.....	23
Figura 4: Funções da Equipe de Auditoria Interna	28
Figura 5: Interação entre objetivos, componentes e estrutura	32
Figura 6: Integração COSO I e COSO ERM	34
Figura 7: Princípios Básicos do COBIT 5	38
Figura 8: Estrutura de Três Linhas de Defesa	41
Figura 9: Processo de Auditoria Interna para ISO 31000	47
Figura 12: Etapas da Metodologia.....	51
Figura 13: Símbolos do Fluxograma	53
Figura 14: Exemplo de Cálculo de Materialidade.....	59
Figura 15: Exemplo de Cálculo do Múltiplo	60

Lista de Tabelas

Tabela 1 - Tipos de fiscalização, níveis e objetivos	6
Tabela 1: Exemplo de Identificação de Riscos e Controles	54
Tabela 2: Princípios do COSO	54
Tabela 3: Classificação dos Controles Internos	56
Tabela 4: Exemplo de Classificação dos Controles Internos	56
Tabela 5: Classificação da Avaliação de Confiança	56
Tabela 6: Definição da Amostra	57
Tabela 7: Exemplo de Teste Substantivo e Percentual de Desvio	58
Tabela 8: Classificação da Avaliação de Exatidão.....	58
Tabela 9: Exemplo de Benchmark	59
Tabela 10: Definição do Percentual de Redução	59
Tabela 11: Matriz de Classificação Final.....	61



INTRODUÇÃO

1. Introdução

A Regulação, surge, em geral, quando existem falhas de mercado em algum setor, a exemplo do que ocorre com os serviços de abastecimento de água e esgotamento sanitário que se configuram como mercados monopolistas por sua natureza, de forma que a regulação desempenha o papel de balancear um setor no qual os mecanismos de mercado falham em se auto ajustar.

Além de corrigir desvios do mercado, a regulação, para além da visão puramente econômica, serve também para garantir que os serviços sejam prestados com qualidade e equidade a toda a população.

Na esteira dessa visão mais ampla de regulação, a Lei nacional nº 11.445 de 5 de janeiro de 2007, também conhecida como marco regulatório do saneamento básico, trouxe em seu artigo 22 os objetivos da regulação, a seguir descritos:

I - estabelecer padrões e normas para a adequada prestação dos serviços e para a satisfação dos usuários;

II - garantir o cumprimento das condições e metas estabelecidas;

III - prevenir e reprimir o abuso do poder econômico, ressalvada a competência dos órgãos integrantes do sistema nacional de defesa da concorrência;

IV - definir tarifas que assegurem tanto o equilíbrio econômico e financeiro dos contratos como a modicidade tarifária, mediante mecanismos que induzam a eficiência e eficácia dos serviços e que permitam a apropriação social dos ganhos de produtividade.

Em consonância com disposto na legislação supracitada, foi criada a Agência Reguladora de Águas e Saneamento do Distrito Federal – ADASA/DF em 16 de junho de 2004, pela Lei Distrital n. 3.365/2004 e alterada pela Lei n. 4.285, de 26 de dezembro de 2008, que ampliou suas competências, passando a se chamar Agência Reguladora de Águas, Energia e Saneamento Básico do Distrito Federal – ADASA. Tem como missão institucional a regulação dos usos das águas e dos serviços públicos desse ente federado,

com o intuito de promover a gestão sustentável dos recursos hídricos e a qualidade dos serviços de energia e saneamento básico em benefício de sua sociedade.

Em 23 de fevereiro de 2006, foi assinado o Contrato de Concessão nº 001/2006 - ADASA entre a Agência Reguladora de Águas, Energia e Saneamento Básico do Distrito Federal – ADASA e a Companhia de Saneamento Ambiental do Distrito Federal – CAESB.

Esse contrato regula a exploração do serviço público de saneamento básico, constituído pelo abastecimento de água e pelo esgotamento sanitário, objeto da concessão do qual a CAESB é a prestadora dos serviços, para toda a área do Distrito Federal, consoante o que estabelece a Lei do Distrito Federal nº 2.954, de 22 de abril de 2002.

Compete à Superintendência de Abastecimento de Água e Esgoto (SAE) da agência a verificação do cumprimento das normas estabelecidas no Contrato de Concessão por meio das atividades de fiscalização.

No escopo da avaliação da prestação dos serviços podem ser identificados dois tipos de fiscalização: fiscalização direta e fiscalização indireta. (**Tabela 1**)

Tabela 1 - Tipos de fiscalização, níveis e objetivos

Tipo de Fiscalização	Nível	Objetivo específico
Direta	Avaliação Operacional	- verificar as instalações físicas visando avaliar o estado de conservação e operação dos sistemas
		- monitorar o cumprimento do plano de investimentos da concessionária
		- validar a base de ativos regulatória da Caesb
		- apurar situações emergenciais ou eventuais
Indireta	Monitoramento Regular	- monitorar aspectos da prestação dos serviços considerados críticos para sua qualidade e continuidade, descritos no Contrato de Concessão e em Resoluções da Adasa, bem como direcionar a ações de fiscalização de nível estratégico e operacional.
		- realizar auditorias e certificação de informações

	Avaliação Estratégica	- avaliar o alcance das metas estabelecidas no Manual de Indicadores de Desempenho e no Plano de Saneamento Básico.
--	-----------------------	---

Fonte: Adasa

As ações de fiscalização direta possuem nível de avaliação operacional e caracterizam-se pela inspeção física nos sistemas da concessionária objetivando: verificar as instalações físicas para avaliação do estado de conservação e operação dos sistemas; monitorar o cumprimento do plano de investimentos da concessionária; apurar situações emergenciais ou eventuais; validar a base de ativos regulatória.

Por sua vez, as ações de fiscalização indireta caracterizam-se em dois níveis: monitoramento regular e avaliação estratégica. As ações do monitoramento regular são intermediárias entre os níveis operacional e estratégico e objetivam monitorar aspectos da prestação dos serviços considerados críticos para sua qualidade e continuidade, descritos no contrato de concessão e em resoluções da Adasa, realizar auditorias e certificação de informações, além de fornecer insumos para o direcionamento das ações dos demais níveis.

Por fim, as ações de fiscalização indireta de nível estratégico, com resultados constantes neste relatório, têm por finalidade avaliar o alcance das metas estabelecidas no Manual de Avaliação de Desempenho estabelecidas pela Resolução n. 8/2016, assim como verificar o cumprimento das metas presentes no Plano Distrital de Saneamento Básico.

No tocante à fiscalização indireta, as ações de monitoramento regular e de implementação de indicadores de desempenho são baseadas nos dados produzidos pela Concessionária e repassados à Adasa para a análise das informações.

Nesse íterim, grande parte do trabalho do regulador é pautado por informações de fonte secundária, as quais podem apresentar limitações em relação à confiabilidade, já que não se tem controle do fluxo dos dados. Esse inconveniente alcança também o Sistema Nacional de Informações sobre Saneamento (SNIS) que recebe dados auto declaratórios das prestadoras dos serviços de saneamento básico de todo o Brasil.

Diante dessa necessidade de melhorar a qualidade da informação sobre o saneamento básico, e, aperfeiçoar e certificar o SNIS, surgiu o Projeto Acertar, capitaneado pelo Ministério das Cidades, que com financiamento do Banco Mundial, por meio do Programa de Desenvolvimento do Setor Água – INTERÁGUAS, desenvolveu metodologia para certificação dos dados relacionados à prestação dos serviços de abastecimento de água e esgotamento sanitário. A ser aplicada pelas agências reguladoras.

O Projeto foi finalizado e estabelecido o guia de Auditoria e Certificação utilizando como base metodologias consolidadas no mercado de auditoria, quais sejam:

- COSO Enterprise Risk Management 2016;
- SO 27001: Sistemas de Gestão de Segurança da Informação;
- COBIT 5: Governança de Tecnologia da Informação

Nesse sentido, objetivando-se melhorar a qualidade da informação repassada à Adasa, e utilizando a metodologia estabelecida pelo projeto Acertar, de alcance nacional, idealizou-se o Manual de Certificação e Auditoria das Informações produzidas pela Concessionária e repassadas à Adasa, bem como àquelas encaminhadas ao SNIS.



O QUE É AUDITORIA?

2.0 que é Auditoria?

A abrangência da auditoria faz com que sua conceituação seja complexa e amplamente debatida, visto que falta um consenso para determinar uma única definição. Para INTOSAI¹ (*International Organization of Supreme Audit Institutions*) a auditoria:

[..] é o exame das operações, atividades e sistemas de determinada entidade, com vistas a verificar se são executados ou funcionam em conformidade com determinados objetivos, orçamentos, regras e normas

Para Reuters (2009) a auditoria geral é aquela exercida sobre todos os elementos componentes do patrimônio e sobre todas as operações do exercício auditado, sendo a mais completa em extensão, podendo apenas variar em profundidade, fundamentando o trabalho realizado no exame integral ou por testes das operações registradas e ser eventual ou permanente, neste último caso, sendo realizada de forma continuada ou periódica.

Com base nas definições acima citadas, temos que a auditoria se caracteriza por um processo de exame sistemático das atividades desenvolvidas em determinada empresa ou setor, que tem o objetivo de averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas, certificando a qualidade e veracidade das informações disponibilizadas.

Quando aplicada ao setor público, a auditoria possui um caráter maior de avaliação das informações que buscam determinar o objeto do setor em questão, a fim de corroborar com este entendimento, as Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI) citam:

¹ *The International Organisation of Supreme Audit Institutions (INTOSAI) operates as an umbrella organisation for the external government audit community. For more than 50 years it has provided an institutionalised framework for supreme audit institutions to promote development and transfer of knowledge, improve government auditing worldwide and enhance professional capacities, standing and influence of member SAIs in their respective countries.*

“Em geral, a auditoria do setor público pode ser descrita como um processo sistemático de obter e avaliar objetivamente evidência para determinar se a informação ou as condições reais de um objeto estão de acordo com critérios estabelecidos. A auditoria do setor público é essencial, pois, fornece aos órgãos legislativos e de controle, bem como aos responsáveis pela governança e ao público em geral, informações e avaliações independentes e objetivas acerca da gestão e do desempenho de políticas, programas e operações governamentais.”

A relevância do trabalho da auditoria é percebida desde 4500 a.C., comprovada por inspeções e verificações arqueológicas, com os primeiros indícios na Suméria. Posteriormente, houve relatos de práticas similares em cidades europeias, como na Roma que era utilizada para o controle do antigo império. (SÁ, 2010).

De acordo com Oliveira e Diniz (2009), tem-se que o desenvolvimento das práticas de auditoria mais consistentes veio somente no século XVIII, com a Revolução Industrial Inglesa. A expansão do capitalismo, provinda do advento do desenvolvimento técnico-industrial, que possibilitou o surgimento de grandes fábricas e o uso intensivo de capital monetário, contribuiu para a efetiva necessidade de utilização constante e aprimorada das atividades de auditoria.

Almeida (2010, p. 01) explica que a auditoria veio como uma necessidade daquele momento da história, contribuindo para “aprimorar os controles e procedimentos internos em geral, principalmente visando à redução de custos e, portanto, tornando mais competitivos seus produtos e serviços do mercado.”

A auditoria surgiu como uma ramificação da contabilidade e seu desenvolvimento se deu simultaneamente ao desenvolvimento dos mercados. A partir da inserção de complexidades nas instituições, o trabalho de auditoria também foi se modernizando, a fim de atender as necessidades das instituições, assegurando uma validação contínua dos dados (IBRACON).

No Brasil, já no século XIX foi instituído o cargo de “perito contábil”² que tinha como função descobrir erros e fraudes. Contudo, somente durante a II Guerra Mundial, com o alinhamento brasileiro aos Estados Unidos e a expansão das relações de

² IBRACON – Auditoria: Registros de uma Profissão p.51

mercado, influenciadas por filiais estrangeiras, e, por meio da criação da *Security and Exchange Commission (SEC)*³ nos EUA, que as instituições brasileiras passaram a adotar com maior rigor os processos de auditoria.

Com passar dos anos, principalmente em mercados de capitais mais maduros e desenvolvidos, e nesse caso, sempre citando o maior e mais tradicional mercado de capitais do mundo, o norte-americano, passou-se a valorizar cada vez mais as atividades de auditoria, visto a importância de manutenção da confiança dos *stakeholders* nas informações que são divulgadas periodicamente pelas empresas participantes desse mercado.

O fortalecimento da auditoria teve contribuição, direta e indireta, de marcos históricos como a Crise do sistema financeiro americano em 1929, mundialmente conhecida como a Grande Depressão, que resultou na quebra da Bolsa de Valores de Nova Iorque.

A economia americana passava por um período de alta produção e exponencial oferta de crédito, contudo, em momentos de pequenas recessões, havia intervenção estatal para suprimir este decréscimo, criando uma taxa de juros artificial. Ou seja, faltavam validações de dados de caráter razoavelmente seguros para os investidores da Bolsa americana, os quais acreditavam nas falsas divulgações que apontavam para um falso desempenho econômico elevado e expandiam seus negócios, aumentando seus investimentos. Assim, a falta de transparência na transmissão das informações foi crucial para a eclosão da crise.

Segundo o professor Dr. Renê Coppe Pimentel, como resposta direta à Crise, foram criadas entidades nos Estados Unidos como a SEC, mecanismos de proteção aos agentes do mercado de capitais por meio de controles e fiscalização mais rigorosos, formação e fortalecimento do que viria a ser no presente o *American Institute of*

³ SEC atua um órgão regulador do mercado de capitais americano, tendo como missão proteger os investidores; manter mercados justos, ordenados e eficientes; e facilitar a formação de capital. A SEC se esforça para promover um ambiente de mercado que seja digno da confiança do público. Definição disponível em <<https://www.sec.gov>>

Certified Public Accountants (AICPA), criação de um Comitê de Procedimentos Contábeis, etc.

A ampliação das relações de mercado, com o surgimento de novas formas de investimentos e empréstimos, traz consigo a necessidade de demonstrar relatórios contábeis e demais registros da empresa que reflitam fidedignidade e transparência à realidade dos negócios da entidade a fim de aumentar sua credibilidade com os *stakeholders* e, por conseguinte, aumentar a sua capacidade de expansão. Para complementar este entendimento tem-se o parecer do Instituto de Auditores Independentes do Brasil, que relata o motivo do surgimento da profissão:

“[...] a auditoria independente foi criada a partir do crescimento das empresas, que, em decorrência das novas tecnologias, do aprimoramento dos procedimentos internos e do esforço para manterem-se em um mercado mais competitivo, passaram a investir mais recursos em suas operações e, conseqüentemente, buscaram novas formas de investimento, como empréstimos bancários e abertura de capital.”

Ainda, segundo o IBRACON, a profissão destina-se a aumentar o grau de confiança nas demonstrações contábeis e examinar se estas, no seu conjunto, representam adequadamente a posição patrimonial e financeira da companhia auditada. O resultado do trabalho do auditor é um importante instrumento para orientar o trabalho de diferentes usuários das demonstrações contábeis.

Para atrair investimentos, por meio de emissões de dívida ou venda de uma parcela do patrimônio líquido (ações), é necessário que as empresas de capital aberto (sociedades anônimas de capital aberto) cumpram regras específicas quanto a necessidade de divulgação de informações financeiras. Estas regras estão descritas na Lei nº 11.638/2007⁴.

O profissional de auditoria externa deve seguir uma série de regulamentações para a execução de seu trabalho. Além das Leis nº 6.404/76 e a Lei nº 11.638/07, anteriormente citadas, há outros órgãos que regem suas funções, como o Conselho Federal de Contabilidade e outras entidades internacionais, como ISA (*International*

⁴ Detalhada na seção 2.4.

Standards on Auditing), que buscam a melhoria da prática das atividades de auditoria, a fim de evitar erros e fraudes que prejudiquem os principais envolvidos. Isto mostra a importância de certificar as informações divulgadas, bem como de que o parecer da auditoria deve expressar clara e objetivamente todos os aspectos que julgar relevantes, com o intuito de contribuir para melhorias do controle interno, visando aumentar a confiabilidade das informações apresentadas pela instituição.

Nos anos 2000, ficou famoso o escândalo contábil protagonizado por umas das maiores empresas da Bolsa de Nova Iorque que com a conivência de uma das principais empresas de auditoria do mundo: a Enron, empresa de exploração de gás natural, produção e comercialização de energia, reportou por vários anos lucros muito maiores que os obtidos na realidade. A maior e mais tradicional empresa de auditoria dos Estados Unidos, a Arthur Andersen, envolvida nestas fraudes de demonstrativos financeiros, deixou de existir juntamente com a Enron. Este escândalo resultou na criação da *Lei Sarbanes & Oxley* (2002), que criou um órgão, específico, com competência para supervisionar os trabalhos de Auditoria Externa, o PCAOB (*Public Company Accounting Oversight Board*).⁵

Dentre as várias alterações trazidas pela *Lei Sarbanes-Oxley* destaca-se que a auditoria começou a fazer um processo de complementação à análise de demonstrações financeiras, verificando a eficácia do sistema de controles internos, ou seja, passou-se a entender que a eficácia das demonstrações financeiras e seu grau de assertividade, precedem e dependem diretamente da qualidade do sistema de controles internos que essa empresa possui.

Tem-se a partir desse caso, um aumento da importância de trabalhos de Auditoria Interna como papel fundamental para a análise da eficácia do ambiente de controles internos. Vejamos o que Attie (2011) cita sobre a importância da auditoria interna:

“A importância que a auditoria interna tem em suas atividades de trabalho serve para a administração como meio de identificação de que todos os procedimentos internos e políticas

⁵ Lei *Sarbanes-Oxley* é detalhada na seção 2.3.1.

definidas pela companhia, os sistemas contábeis e de controle interno estão efetivamente seguidos, e todas as transações realizadas estão refletidas contabilmente em concordância com os critérios previamente definidos.”

Assim, temos que a auditoria interna se caracteriza por um processo contínuo e rigoroso, a fim de corroborar com apontamentos de eventuais falhas e vulnerabilidades às quais a organização está sujeita, além do que, segundo Franco (1991, p. 218), o auditor interno tem vínculo direto com a instituição, o que facilita a gestão de questões peculiares à empresa visto seu conhecimento sobre a entidade.

2.1. Riscos

O risco está diretamente ligado a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades. Ao receber uma informação, a veracidade dos fatos descritos está submetida a riscos de falhas e erros que podem interferir nos dados relatados aos interessados, ou seja, uma variação dos resultados esperados.

Para o *The Institute of Internal Auditor - IIA*⁶ risco é "a possibilidade de ocorrência de um evento que pode ter um impacto no alcance de objetivos. Os riscos são mensurados em termos de impacto e ocorrência".

Mais ainda, segundo AVALOS (2009, p.65):

“[...] os riscos são fatos ou acontecimentos cuja probabilidade de ocorrência é incerta. Os riscos interferem na possibilidade de a organização sobreviver, concorrer com êxito para manter seu poder financeiro e a qualidade de seus produtos e serviços. O risco é inerente aos negócios e não existe forma prática de reduzi-lo a zero.”

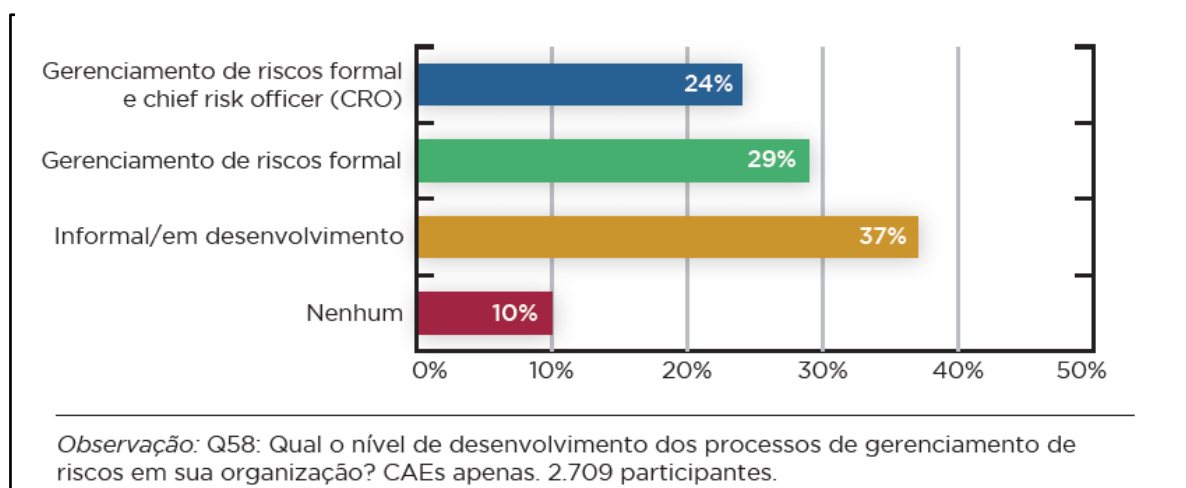
Com base nas definições, os riscos podem afetar diretamente a organização, e para evitar ou minimizar os danos, eles devem ser tratados e categorizados,

⁶Fundado em 1941, *The Institute of Internal Auditors* (IIA) é uma associação internacional de profissionais com sede global em Lake Mary, Florida, USA. O IIA é a voz global da profissão de auditoria interna, autoridade reconhecida, líder reconhecido, advogado-chefe e educador principal. Geralmente, os membros trabalham em auditoria interna, gerenciamento de riscos, governança, controle interno, auditoria de tecnologia da informação, educação e segurança. O IIA tem mais de 185.000 membros ao redor do mundo.

identificando sua origem e a sua natureza. Muito se tem estudado sobre como gerir riscos de uma economia que sofre mudanças rapidamente.

Os riscos afetam diretamente a instituição, podendo ser agravados pela falta de uma prática continuada de gerenciamento bem estabelecida dentro da organização. O CBOK (*Common Body of Knowledge*), que é um documento mantido pela associação internacional ABPMP⁷ e contém uma visão sobre todas as fases para a realização de um projeto de gerenciamento de processos ideal, realizou uma pesquisa em 2015 sobre a práticas de gerenciamento de riscos:

Figura 1: Práticas de Gerenciamento de Riscos



Fonte: CBOK 2015

O resultado da pesquisa demonstra que apenas 10% das empresas entrevistadas não possuem nenhum tipo de gerenciamento de risco, enquanto 53% admitem possuir “processos e procedimentos de riscos formais em prática”, destes 24% possuem um CRO (Gerenciamento de risco formal e *chief risk officer*) ou equivalente.

O uso da Tecnologia da Informação traz consigo um risco que é constantemente discutido por executivos, auditores internos e demais áreas da governança: o risco de violação de dados delicados ou sigiloso, mais de 70% dos pesquisados consideram que este risco possua um grau de moderado ou alto dentro de suas instituições (FLORA e RAI, CBOK 2015).

⁷ABPMP – Association of Business Process Management Professionals

O uso de um gerenciamento de riscos robusto aumenta a credibilidade dos demonstrativos das empresas, que são os documentos que o mercado tem acesso para as ações proeminentes de suas necessidades, tal como calcular índices, tomar decisões sobre investimentos, direcionar os objetivos da governança corporativa, etc., e que podem ser afetados por distorções, erros materiais ou falhas provenientes do sistema de informação. Manter estes riscos sob monitoramento constante e buscando sempre minimizar seus efeitos, garante maior confiabilidade aos usuários destas informações.

2.1.1. Fraude

As Fraudes Corporativas têm um impacto significativo para as organizações, pois, em busca de obtenção de benefícios próprios, os agentes fraudadores podem manipular as informações contábeis, gerando prejuízos inestimáveis a empresa em questão e, por conseguinte, afetando também a sociedade usuária do serviço.

O termo 'fraude' aplica-se a ato intencional de omissão e/ou manipulação de transações e operações, adulteração de documentos, registros, relatórios, informações e demonstrações contábeis, tanto em termos físicos quanto monetários. (CFC 986/03)

Para o The IIA (*The Institute of Internal Auditors*), o conceito de fraude é:

“Ato ilegal baseado no dolo, encobrimento ou violação de confiança. Esse ato não depende em aplicar ameaças de violência ou força física. Fraudes são realizadas por indivíduos e organizações para obter dinheiro, propriedades e serviços; evitar pagamentos ou perdas de serviços; ou assegurar vantagens pessoais ou comerciais.”

A utilização dos ativos ou recursos da organização para ganhos próprios também pode ser considerada fraude para a ACFE (*The Association of Certified Fraud Examiners*). Os componentes da fraude podem ser motivados por dificuldades financeiras ou insatisfações, atração pelos valores, em geral, a ação fraudulenta se vale de falhas no controle que permitem a ocultação por meio de “maquiagens contábeis” e falsificações dos dados.

Segundo o estudo publicado pelo ACFE realizado em 2014, a fraude, do início de sua descoberta até o final, dura em média 18 meses. As denúncias tem sido o meio mais comum de detecção, conforme figura abaixo:

Figura 2: Formas de Detecção Inicial de Fraudes

Método de Detecção	% de casos
Denúncias	42%
Revisão da Administração	16%
Auditoria Interna	14%
Outros métodos, tais como por acidente, auditoria externa, agências de aplicação da lei, etc.	28%

Fonte: ACFE 2014 *Report to the Nations on Occupational Fraud and Abuse*

Como visto na pesquisa acima, a auditoria interna não é o meio mais frequente de detecção de fraudes, as denúncias estão em maioria, com 42% dos relatos. Para o Dr. Al Faddagah, a gestão de riscos deve ser pensada como um processo, que mantém responsabilidades tanto ao controle interno como na auditoria interna, alta administração e setores de conformidade.

Fraudes no mundo, segundo ACFE⁸:

- Estima-se que as empresas percam anualmente 5% de suas receitas com fraudes;
- Apenas 14% dos pesquisados conseguiram reaver 100% dos valores perdidos com fraudes;
- Fraudes ocupacionais podem ser classificadas em 3 categorias: desvio de bens e ativos da empresa, corrupção e fraudes em demonstrações financeiras.

Dentre as fraudes ocorridas, 61% são praticadas por funcionários da própria empresa⁹, ou seja, os controles internos precisam ser bem definidos, compactuando

⁸ 2014

⁹ Dados KMPG, 2009.

com a ética e os valores da entidade, a fim de promover uma melhoria na segurança antifraudes.

Um caso recente de fraude foi o da empresa Toshiba que ampliou seus lucros em mais de US\$ 1,1 bilhão ao longo de sete anos para atingir as metas. Após o anúncio do relatório de investigações realizadas por um comitê de especialistas independentes, o CEO e demais executivos da gigante em tecnologia renunciaram seus cargos.

Uma pesquisa da Ernst & Young a pedido da revista Exame¹⁰, afirma que muitas empresas entrevistadas não sabem dimensionar as perdas com fraudes e, por vezes, nem se quer conseguem afirmar se sofrem com fraudes ou não. Assim, temos que a natureza deste delito é complexa e exige que as organizações tomem medidas efetivas.

O sócio da consultoria da pesquisa acima citada, José Compagno, afirmou à revista Exame que para a ocorrência da fraude, o agente causador pode ter a seu favor:

“[...] a fragilidade nos processos de controles internos e nas políticas de controle de risco, o que pode causar a percepção para o fraudador de que existe facilidade para execução da fraude e para acobertá-la.”

O fortalecimento das atividades do controle interno, como o monitoramento sistemático das operações realizadas pela empresa e do ambiente de TI e código de ética claro e bem definido são as principais formas de mitigar este risco, visando a assegurar as informações transmitidas.

2.2. Controle Interno

O Controle Interno é uma ferramenta de uso comum às grandes empresas que buscam mitigar riscos, por meio do monitoramento do controle de suas ações. Objetivando a proteção de ativos, produção de dados contábeis confiáveis e auxiliar na condução das diretrizes para atingir os objetivos corporativos com eficiência. Segundo o Instituto dos Auditores Internos (The IIA), os controles internos podem ser definidos como:

“Qualquer ação tomada pela Gerência, Conselho e outras partes para gerenciar o risco e aumentar a probabilidade em

¹⁰ Realizada em 2011

estabelecer que os objetivos e metas sejam alcançadas. A Gerência planeja, organiza e direciona a performance de ações suficientes para dar uma certeza razoável de que os objetivos e metas sejam alcançados pela empresa ou instituição.”

Fayol (1981, p.139) sintetiza os objetivos do controle interno afirmando que seu dever é apontar as faltas e os erros, para repará-los, evitando sua repetição. O reporte da identificação de falhas é crucial para a correção, portanto, a comunicação eficaz neste setor é primordial.

Dentre os objetivos que devem ser alvo de interesse das instituições, temos a precisão e a confiabilidade dos informes e relatórios contábeis, financeiros e operacionais. Para atingir esta meta, as informações geradas devem ser adequadas para que haja a compreensão de fatos e eventos realizados na organização. Para complementar o entendimento deste fator, Attie¹¹ reforça como as informações podem auxiliar:

“Uma empresa necessita constituir, para si, sistemas que lhe garantam conhecer os atos e eventos ocorridos em cada um dos seus segmentos. Os efeitos ocorridos através da realização de cada ato devem ser escriturados e levados, em tempo hábil, ao conhecimento dos administradores.”

O mesmo autor ainda complementa, estabelecendo componentes que podem ser usados a fim de possibilitar sua realização como: uso de documentação confiável, conciliação entre as fontes, análise sistemática de documentos, estrutura formal de contas e tempo hábil para, em casos de adversidades, poder administrá-las. Além disso, adotar padrões de verificação continuada é uma medida que visa diminuir as falhas.

O Controle Interno pode ser classificado em diferentes tipos, como controle preventivo, detectivo e diretivo, a integração de todos eles faz com que o controle interno possa ter solidez para gerir a organização. Esses controles podem ter três tipos de natureza¹²: manual, que não dependem de Tecnologia da Informação e objetivam manter um certo grau de fluxo e funcionamento do sistema; automática, executados

¹¹ 2011

¹² Chiavenato (1993)

por aplicações informatizadas; e semiautomática, que relaciona as duas naturezas anteriores.

Organizações munidas de controle interno eficiente expressam aos principais interessados e envolvidos, confiabilidade nas informações a serem apresentadas (como os demonstrativos financeiros) pois a implantação deste setor na entidade coíbe e/ou elimina desvios indesejáveis ou comportamentos que infringem as regulações, bem como o Código de Ética.

2.3. Auditoria Externa

As primeiras auditorias externas do Brasil, ou auditorias independentes, tiveram início pela atuação de empresas ligadas às associações internacionais, fato que se deu em razão da necessidade legal dos investimentos no exterior serem auditados.

Em 1976, foi criada no Brasil, a Lei da Sociedade por Ações nº. 6.404 que determinava a obrigatoriedade de as demonstrações financeiras e contábeis de empresas de capital aberto serem auditadas por auditores independentes associados a CVM (Comissão de Valores Mobiliários)¹³. Esta lei foi revogada em 2007 pela lei nº. 11.638 que a modernizou, fazendo alterações a fim de harmonizar as formalizações internacionais com as brasileiras.

Nesta lei estão estabelecidos os padrões de quais divulgações financeiras devem ser apresentadas, quais sejam:

- a) Balanço Patrimonial
- b) Demonstração do Resultado do Exercício (DRE)
- c) Demonstração do Fluxo de Caixa (DFC)
- d) Demonstração do Valor Adicionado (DVA)

¹³ A CVM é uma entidade autárquica em regime especial, vinculada ao Ministério da Fazenda, com personalidade jurídica e patrimônio próprios, dotada de autoridade administrativa independente, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes, e autonomia financeira e orçamentária. Disponível em < www.cvm.gov.br>.

Cada uma das divulgações financeiras deve seguir padrões, que também estão descritos na lei, seguindo ordens tais quais subestruturas determinadas a cada e liquidez dos ativos e passivos. Quanto à obrigatoriedade, a lei cita:

“Art. 3º - Aplicam-se às sociedades de grande porte¹⁴, ainda que não constituídas sob a forma de sociedades por ações, as disposições da Lei nº. 6.404, de 15.12.76, sobre escrituração e elaboração de demonstrações financeiras e a obrigatoriedade de auditoria independente por auditor registrado na Comissão de Valores Mobiliários.”

A lei traz como principais mudanças a substituição da obrigatoriedade de apresentação da Demonstração de Origens e Aplicações de Recursos (DOAR) pela Demonstração de Fluxo de Caixa (DFC), inclui a Demonstração do Valor Adicionado e reestrutura a forma de apresentação do Balanço Patrimonial. Além da obrigatoriedade das divulgações financeiras às empresas de grande porte de capital aberto e fechado, também é exigido que as empresas de capital fechado com Patrimônio Líquido acima de R\$2 milhões apresentem a DFC.

Todas estas demonstrações são alvos de uma auditoria independente, estabelecida no art. 3 da lei nº. 11.638/07, para as empresas de capital aberto. O trabalho do auditor tem um viés autônomo, agindo majoritariamente com o objetivo de fornecer informações para que o investidor e os principais interessados pelas ações da companhia possam fazer sua tomada de decisão com segurança a fim de garantir a rentabilidade de seu investimento. PICKETT (2005) divide as tarefas do auditor independente em duas fases:

1. Fase preliminar: visita a entidade antes do encerramento do exercício social inicial, objetivando obter mais conhecimento sobre suas operações, coordenando junto à empresa, as informações e dados necessários à auditoria, iniciando a análise de demonstrações financeiras.
2. Fase final: visita do auditor após o término do exercício social complementando sua análise das demonstrações e emitindo seu parecer.

¹⁴ Consideram-se de grande porte as sociedades ou conjunto de sociedades sob controle comum que tenham ativo total superior a R\$240 milhões ou receita bruta anual superior a R\$300 milhões (art. 3º da lei 11.638/07).

Por vezes, a auditoria interna e a externa podem ser confundidas, pois são atividades que se complementam. A auditoria externa considera a auditoria interna como parte do sistema de controle de uma empresa, enquanto a auditoria externa atua como um perito contábil responsável pela qualidade das informações divulgadas ao mercado por empresas de grande porte ou que participem do mercado de bolsa de valores. O quadro abaixo demonstra as principais características que diferenciam suas funções:

Figura 3: Diferença entre Auditoria Externa e Auditoria Interna.

	AUDITORIA INTERNA	AUDITORIA EXTERNA
Propósito do Trabalho	Análise do ambiente de Controles internos das empresas (Amplitude Geral)	Emissão de opinião sobre demonstrações contábeis.
Parâmetros para a execução do trabalho	Normas de controle interno, políticas e procedimentos da empresa.	Princípios fundamentais de contabilidade.
Preocupação com os controles internos	Eficiência e eficácia dos controles internos.	Foco nas demonstrações contábeis.
Dependência Profissional	Independência Funcional	Independência profissional.
Forma de Relatórios	Não padronizados (depende das regras definidas em cada empresa).	Padronizados por Reguladores
Principais Usuários	Comitê de Auditoria, Diretoria e Gestores.	Acionistas, mercado de capitais e credores.

Fonte: Elaboração Própria.

A presença de uma auditoria externa numa corporação, embora obrigatória, solidifica sua participação no mercado de ações e transmite aos credores a imagem de que a entidade está disposta a disponibilizar uma análise transparente de sua posição patrimonial e financeira, aumentando a credibilidade para a conferência dos futuros investidores e instituições bancárias, o que assegura às organizações maior possibilidade de captação de recursos com terceiros e expansão.

2.3.1. Lei Sarbanes-Oxley

A Lei *Sarbanes Oxley*, também conhecida por sua abreviação SOx, foi criada pelos senadores Paul Sarbanes e Michael Oxley em 2002, motivada por escândalos de adulteração e falsidade nos demonstrativos financeiros divulgados ao mercado. Dentre eles, destaca-se o escândalo proporcionado pela empresa Enron e WorldCom, que ainda contou com o envolvimento da empresa de auditoria externa, Arthur Andersen.

Seu principal objetivo é garantir que as demonstrações financeiras estejam livres de erros materiais, restaurando a confiança dos investidores no mercado de capitais, depois dos escândalos de maquiagem das demonstrações contábeis-financeiras. Outros objetivos associados são: promover o fortalecimento do controle de governança corporativa, aumentar o nível de responsabilidade e comprometimento das prestações de contas, responsabilizando CEO e CFO, bem como, auditores externos na qualidade das informações financeiras divulgadas ao mercado.

Foi ainda criado pela lei o *Public Company Accounting Oversight Board (PCAOB)* que supervisiona as auditorias das empresas públicas a fim de proteger os interesses dos investidores e promover o interesse público na elaboração de relatórios de auditoria informativos, precisos e independentes. O PCAOB também supervisiona as auditorias dos corretores, incluindo os relatórios de conformidade arquivados de acordo com as leis federais de valores mobiliários dos Estados Unidos, para promover a proteção dos investidores¹⁵.

Este órgão tem a autoridade para aplicar medidas punitivas às entidades que falhem com o cumprimento da Lei SOx, como meio de garantir a veracidade da apresentação das demonstrações financeiras. O Conselho pode impor uma série de sanções a um auditor ou a empresas de contabilidade, incluindo censuras, penalidades monetárias, revogação do registro de uma empresa e de um auditor.

Entre as várias boas práticas e padrões de trabalhos a serem cumpridos pelas empresas de auditoria externa, o PCAOB corrobora a posição de promover maiores responsabilidades e independência dos comitês de auditoria. Além disso, o PCAOB

¹⁵ Fonte: <<https://pcaobus.org/>>. Acesso em setembro

restringiu tipos de trabalhos das firmas de auditoria independente dentro das empresas, estabeleceu novos padrões para as divulgações financeiras de empresas registradas na SEC e desenvolveu leis criminais relativas as condutas corporativas e práticas da profissão de auditor.

Síntese dos principais pontos da Lei *Sarbanes-Oxley*

Emissão de Relatórios:

- a) Certificação os DFs (Demonstrativos Financeiros) pela administração.
- b) Certificação dos controles internos e relatório da certificação da administração e do auditor (20F, 10Q e 10K).

Governança Corporativa:

- a) Políticas e procedimentos de contabilização
- b) O Comitê de auditoria é responsável pela seleção e acompanhamento dos auditores externos, independentes e *experts* em conhecimentos financeiros.
- c) Orçamento destinado à auditoria, consultoria e outros.
- d) Proibição de empréstimos futuros para a administração e gerência.

Expansão de Responsabilidades:

- a) Ilegalidade para qualquer diretor em influência fraudulenta, coerção ou manipulação de auditores independentes.
- b) Rápido reporte de negociações.
- c) Divulgação do código de ética.

Monitoramento e Acompanhamento:

- a) Todas as firmas de contabilidade sejam registradas no PCAOB
- b) Expansão da revisão da SEC, no mínimo a cada 3 anos.

Penalidades e Principais Sanções:

- a) Restituição dos bônus
- b) Penalidades criminais para CEO/CFO, para destruição, alteração, mutilação consensual de registros ou documentos.

- c) Aumento de penalidade para contadores que produzirem documentações com falhas.

Aumento da Independência do Auditor:

- a) Proibição de auditor prover 9 serviços específicos diferentes de auditoria.
- b) Pré-aprovação pelo Comitê de Auditoria para todos os serviços prestados.
- c) Rotação do sócio líder de auditoria a cada 5 anos.

A metodologia chamada *Internal Control*, também conhecida como COSO I¹⁶, é utilizada em escala global para adequação de Controles Internos *Section SOx 404*. Seu foco principal são as demonstrações financeiras obrigatórias para empresas de capital aberto na Bolsa de Nova Iorque, além da ênfase na prevenção de fraudes.

A lei rege as companhias abertas no mercado de Bolsa de Valores de Nova Iorque, o que afeta também as grandes companhias brasileiras que mantém ADRs (*American Depositary Receipts*) negociadas na NYSE¹⁷. Tornando os demonstrativos mais complexos com medidas punitivas e regras para evitar fraudes, garantindo a veracidade das informações econômico-financeiras a serem transmitidas aos principais interessados.

2.4. Auditoria Interna

A auditoria interna auxilia a alta administração a gerir seu planejamento estratégico por meio de avaliações constantes dos procedimentos, com ênfase no cumprimento das normas, tendo em vista as necessidades corporativas e os valores da empresa. O trabalho do auditor também deve colaborar com a melhoria da eficácia do gerenciamento de riscos por meio da análise sistêmica dos procedimentos executados, garantindo a confiabilidade das informações geradas pelos mecanismos de controle.

Para o IIA - *The Institute Internal Auditor*, baseando-se em sua norma IPPF (Estrutura Internacional de Práticas Profissionais), a auditoria interna é definida como:

“[...] uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma

¹⁶ Explicitada no capítulo 3

¹⁷ NYSE – *New York Stock Exchange* – Bolsa de valores de Nova Iorque.

organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.”

As atribuições da auditoria interna estão diretamente relacionadas ao tipo em que ela atua, como financeiro, contábil, operacional, de sistemas de informação, de gestão, entre outros necessários a entidade. Ainda assim, a auditoria interna possui características comuns a todos os tipos realizáveis, tendo como princípio a aderência da auditoria aos objetivos e atribuições previamente delimitadas pela organização.

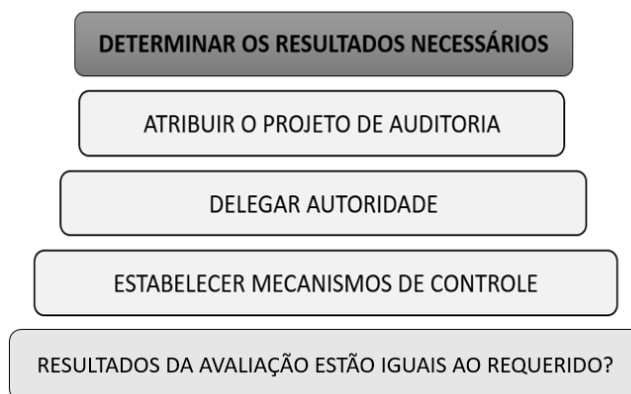
A importância da auditoria interna como ferramenta de supervisão da eficácia dos controles internos para elevar o nível de confiabilidade nas instituições é cada vez mais notável no ambiente corporativo, o que tem elevado o papel da auditoria interna nos ambientes de controles internos. Para que a auditoria interna execute seus procedimentos de modo a contribuir sumariamente com as necessidades da alta governança, PICKETT (2005) expõe um manual que delimita as principais características do time de auditoria e elabora uma estrutura organizacional para o trabalho:

- (i) **Equipe:** O resultado final de um processo de auditoria é dependente dos profissionais que o conduziram o trabalho, pois, é a equipe quem define como a auditoria deverá ser executada e quem determina como esta avaliação deverá ser constituída, ou seja, como os resultados serão analisados e reportados à governança.

Em características gerais, a composição do time depende do tamanho do projeto e do seu prazo de reporte ao CEO (*Chief Executive Officer*) ou demais gestores, após aprovação do Comitê de Auditoria.

A escolha do líder também é fundamental para o processo. Qualidades como: ter uma boa relação com executivos, boas habilidades interpessoais e analíticas, possibilitando a assimilação de grandes montantes de dados complexos, conhecimento da área e tipos de processos a serem auditados, e, comunicação clara e efetiva de ideias, podem favorecer a equipe em circunstâncias difíceis, levando ao sucesso do trabalho.

Delegar funções à equipe também é parte do processo, a delimitação do que deve ser feito e de que modo a auditoria como um todo deve ser conduzida, vejamos abaixo um diagrama sobre as principais funções que devem ser atribuídas à equipe de



auditoria:

Figura 4: Funções da Equipe de Auditoria Interna

Fonte: PICKETT, *'The Essential Handbook of Internal Auditor'*, 2005

Estas funções certificam que os resultados da auditoria, requeridos previamente, serão cumpridos de modo adequado, com resultados precisos, e que trarão informações úteis para auxiliar a governança na tomada de decisões.

(ii) Competências da Equipe de Auditoria Interna: Ao escolher a equipe de auditoria interna deve-se considerar a qualificação dos profissionais garantindo que eles possuam habilidades e conhecimentos sobre os melhores padrões internacionais em auditoria. Também devem ser estimadas as experiências e compreensões de:

- a) Funcionamento de sistemas financeiros e operacionais;
- b) Riscos e como eles podem afetar o desenvolvimento da empresa;
- c) Estruturas, autorizações e rotinas específicas de controle interno;
- d) Regulações, leis, obrigações e políticas;
- e) Identificação e agrupamento de evidências confiáveis para melhorias do gerenciamento de riscos;
- f) Como entrevistar, analisar, examinar e avaliar dados, fatos e sistemas;

- g) Resolver problemas e desenvolver respostas viáveis, baseadas nos riscos e nos custos;
- h) Saber lidar com ambientes de escolhas que podem exigir resistência.

Além dessas habilidades a equipe deve considerar as necessidades e expectativas dos principais interessados, incluindo a natureza, o tempo e a comunicação dos resultados, além da complexidade e extensão que o trabalho precisa para alcançar o seu objetivo, custo do procedimento em relação aos benefícios.

(iii) Estrutura da Auditoria Interna: a auditoria é um trabalho que depende de organização, estruturação, desenvolvimento de habilidades e técnicas que estejam atualizadas e de acordo com os padrões internacionais estabelecidos, para a solidez de um processo eficaz e de maior objetividade.

Visto isso, manter planos abrangentes, como um modelo básico de estrutura, para a execução do trabalho de auditoria também se faz necessário. Para PICKETT (2005), os estágios de planejamento são:

- a) **Objetivos organizacionais:** o gerenciamento das metas para obtenção dos objetivos que são almejados pela corporação deve se basear em metas claras e aspirações antes da formulação do plano, podendo se dar através da boa comunicação do time.
- b) **Avaliação de prioridades de riscos:** identificação dos riscos de cada área auditada
- c) **Áreas de priorização de recursos:** o CAE (*Chief Audit Executive*) deve garantir que os recursos do auditor interno sejam apropriados, suficientes e efetivamente implantados para alcançar o plano. (Performace Standard 2030). Os recursos são determinados através do nível de cobertura do estado de gerenciamento de risco e controle.
- d) **Plano estratégico:** desenvolvimento de uma estratégia formal de auditoria interna, que deve iniciar com os próprios objetivos da entidade, baseando-se nos riscos e reflexos importantes de suas causas e consequências.
- e) **Plano anual:** formalização de um plano anual e de entendimento entre auditor e comitê. Listando as tarefas que a auditoria deve realizar durante o



**METODOLOGIAS DE
GERENCIAMENTO DE RISCOS**

3. Metodologias de Gerenciamento de Riscos

3.1. COSO¹⁸

O *Committee of Sponsoring Organization of the Treadway Commission* (COSO) é uma iniciativa privada de cinco organizações: *American Accounting Association* (AAA), *American Institute of Certified Public Accountants* (AICPA), *Financial Executives International* (FEI), *The Association of Accountants And Financial Professionals in Business* (IMA) e *The Institute Of Internal Auditors* (IIA), e se dedica a melhoria dos relatórios financeiros, fornecendo orientações sobre gerenciamento de riscos corporativos, controle interno e dissuasão de fraude.

Em 1985 o Comitê foi criado como Comissão Nacional de Relatórios Financeiros Fraudulentos, uma associação independente composta por profissionais ligados à área financeira, voltado ao desenvolvimento do Controle Interno, com intuito de identificar os fatores causais que podem levar a relatórios financeiros fraudulentos. Durante sua atuação, o COSO tem feito publicações a fim de fornecer orientações às corporações.

Dentre as publicações mais utilizadas tem-se “Controle Interno – Estrutura Integrada”, publicado em 1992, revisado e reeditado em 2013. Para o gerenciamento de riscos tem-se “*Enterprise Risk Management - Integrated Framework*”, publicado em 2004. A dissuasão de fraude teve dois estudos de pesquisa publicados, intitulados “Relatório Financeiro Frauduloso: 1987-1997” e uma continuação de 1998-2007.

COSO I – Controle Interno – Estrutura Integrada

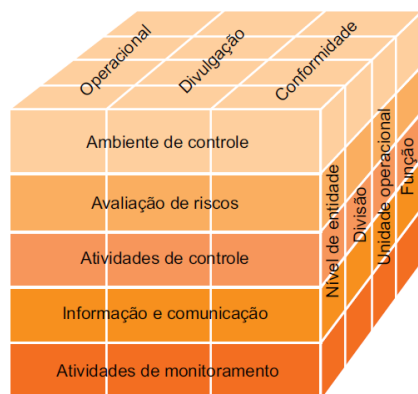
Na publicação de Controles Internos do COSO, há uma relação direta entre os objetivos, componentes e a estrutura organizacional da entidade. O primeiro visa as metas que a organização busca alcançar, o seguinte dispõe sobre as demandas impostas

¹⁸ O texto desta seção se baseia nas informações disponíveis em <http://www.coso.org>. Acesso em setembro de 2017.

por estas metas. Para promover um melhor entendimento, vejamos a figura abaixo, que ilustra em forma de cubo:

Figura 5: Interação entre objetivos, componentes e estrutura

Fonte: Adaptado de *Committee of Sponsoring Organization of the Treadway Commission*



Nas colunas temos os objetivos, nas linhas os componentes e em terceira dimensão a estrutura organizacional. A relação do cubo busca demonstrar que todos os componentes devem estar em interação constante e continuada.

O COSO define controle interno como “um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.”

A metodologia COSO (*Internal Controls*) é separada em cinco componentes integrados:

Ambiente de Controle:

O ambiente de controle é um conjunto de normas, processos e estruturas que fornece a base para a condução do controle interno por toda a organização. A estrutura de governança e a alta administração estabelecem uma diretriz sobre a importância do controle interno, inclusive das normas de conduta esperadas.

Avaliação de Riscos:

Toda entidade enfrenta vários riscos de origem tanto interna quanto externa. Define-se risco como a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos. A avaliação de riscos envolve um processo dinâmico e iterativo para identificar e avaliar os riscos à realização dos objetivos. Esses riscos de não atingir os objetivos em toda a entidade são considerados em relação às tolerâncias aos riscos estabelecidos. Dessa forma, a avaliação de riscos estabelece a base para determinar a maneira como os riscos serão gerenciados.

Uma condição prévia à avaliação de riscos é o estabelecimento de objetivos, ligados aos diferentes níveis da entidade. A administração especifica os objetivos dentro das categorias: operacional, divulgação e conformidade, com clareza suficiente para identificar e analisar os riscos à realização desses objetivos. A administração também considera a adequação dos objetivos à entidade. A avaliação de riscos requer ainda que a administração considere o impacto de possíveis mudanças no ambiente externo e dentro de seu próprio modelo de negócio que podem tornar o controle interno ineficaz.

Atividades de Controle:

Atividades de controle são ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos. As atividades de controle são desempenhadas em todos os níveis da entidade, em vários estágios dentro dos processos corporativos e no ambiente tecnológico. Podem ter natureza preventiva ou de detecção e abranger uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio. A segregação de funções é geralmente inserida na seleção e no desenvolvimento das atividades de controle.

Informação e Comunicação:

A informação é necessária para que a entidade cumpra responsabilidades de controle interno a fim de apoiar a realização de seus objetivos. A administração obtém ou gera e utiliza informações importantes e de qualidade, originadas tanto de fontes internas quanto externas, a fim de apoiar o funcionamento de outros componentes do controle interno. A comunicação é o processo contínuo e iterativo de proporcionar, compartilhar e obter as informações necessárias. A comunicação interna é o meio pelo qual as informações são transmitidas para a organização, fluindo em todas as direções da entidade. Ela permite que os funcionários recebam uma mensagem clara da

alta administração de que as responsabilidades pelo controle devem ser levadas a sério. A comunicação externa apresenta duas vertentes: permite o recebimento, pela organização, de informações externas significativas e proporciona informações a partes externas em resposta a requisitos e expectativas.

Atividades de Monitoramento:

Uma organização utiliza avaliações contínuas, independentes, ou uma combinação das duas, para se certificar da presença e do funcionamento de cada um dos cinco componentes de controle interno, inclusive a eficácia dos controles nos princípios relativos a cada componente. As avaliações contínuas, inseridas nos processos corporativos nos diferentes níveis da entidade, proporcionam informações oportunas. As avaliações independentes, conduzidas periodicamente, terão escopos e frequências diferentes, dependendo da avaliação de riscos, da eficácia das avaliações contínuas e de outras considerações da administração. Os resultados são avaliados em relação a critérios estabelecidos pelas autoridades normativas, órgãos normalizadores reconhecidos ou pela administração e a estrutura de governança, sendo que as deficiências são comunicadas à estrutura de governança e administração, conforme aplicável.

Em decorrência da padronização internacional das técnicas de auditoria, as recomendações do COSO são amplamente difundidas e tida como modelo para o Brasil e para a maioria dos países do mundo, visto que as orientações do comitê seguem as principais regulações internacionais como a Lei SOx, que é referência para as práticas de regulamentações do setor financeiro em todo o mundo.

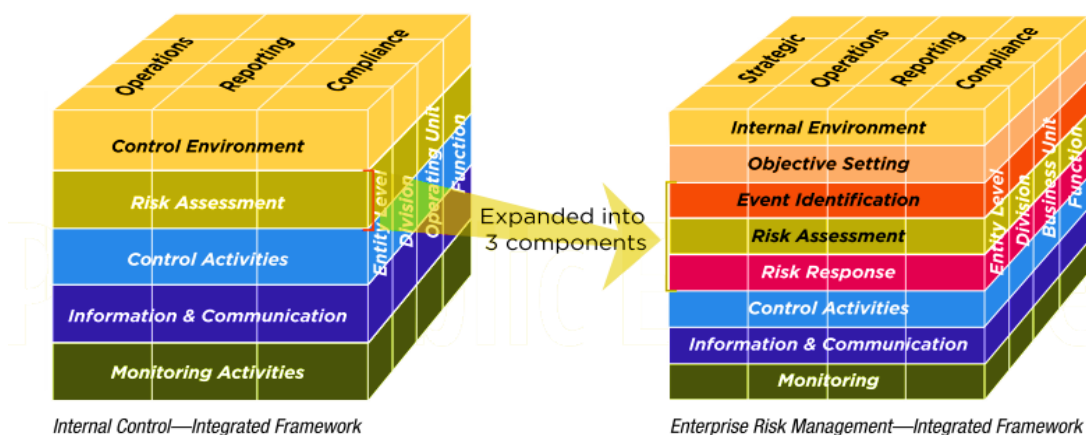
COSO II – Gerenciamento de Riscos – Estrutura Integrada

A metodologia COSO II (*Enterprise Risk Management - ERM*) visa criar uma abordagem mais específica e efetiva sobre os riscos, expandindo os componentes e objetivos existentes no modelo anterior.

Na coluna do cubo (figura abaixo) é notável a inclusão de mais um objetivo que a instituição deve aderir: a estratégia. Para as entidades que adotam o modelo COSO ERM, devem incluir como objetivo para assegurar o funcionamento da metodologia com

Figura 6: Integração COSO I e COSO ERM

eficiência e eficácia, visto que há uma integração mais minuciosa dos objetivos e componentes voltados ao risco.



Fonte: Adaptado de *Committee of Sponsoring Organization of the Treadway Commission*

A ilustração nos mostra como o gerenciamento de riscos é tratado no modelo COSO ERM. O componente de Avaliação de Risco se expande para três componentes: Identificação, Avaliação e Resposta de Risco. Desta forma, a segurança em gerir os riscos se torna mais sólida, envolvendo a responsabilidade em mais setores do controle interno.

Os componentes anexados à esta estrutura, com base na publicação do COSO II (2009), são definidos como:

Identificação de Eventos:

[...]a administração identifica os eventos em potencial que, se ocorrerem, afetarão a organização e determina se estes representam oportunidades ou se podem ter algum efeito adverso na sua capacidade de implementar adequadamente a estratégia e alcançar os objetivos. Eventos de impacto negativo representam riscos que exigem avaliação e resposta da administração. Os eventos de impacto positivo representam oportunidades que são canalizadas de volta aos processos de fixação das estratégias e dos objetivos. Ao identificar eventos, a administração considera uma variedade de fatores internos e externos que podem dar origem a riscos e a oportunidades no contexto de toda a organização.

Resposta ao Risco:

Após ter conduzido uma avaliação dos riscos pertinentes, a administração determina como responderá aos riscos. As respostas incluem evitar, reduzir, compartilhar ou aceitar os riscos. Ao considerar a própria resposta, a administração avalia o efeito sobre a probabilidade de ocorrência e o impacto do risco, assim como os custos e benefícios, selecionando, dessa forma, uma resposta que mantenha os riscos residuais dentro das tolerâncias a risco desejadas. A administração identifica as oportunidades que possam existir e obtêm, assim, uma visão dos riscos em toda organização ou de portfólio, determinando se os riscos residuais gerais são compatíveis com o apetite a riscos da organização.

Esta metodologia, que visa estabelecer uma cultura de gestão de riscos mais sólida dentro dos controles internos da entidade, além de garantir o tratamento dos riscos de modo a mitigar seus impactos na organização, quando negativos, e saber como e quando aproveitá-los, quando positivos, torna o objetivo central do COSO de “identificar os fatores que levam aos relatórios fraudulentos” mais fácil de ser atingido. O uso destes modelos, recomendados e elaborados pelo Comitê, portanto, eleva a credibilidade dos relatórios, visto que o modelo busca atingir a maior eficiência e eficácia neste quesito.

3.2. COBIT 5

A segurança da informação é um tópico importante para as corporações, pois com o desenvolvimento da tecnologia, seus dados e recursos são mantidos sob uma base de dados, a fim de agilizar as ações cotidianas e mitigar os riscos, como ações fraudulentas. Manter esta estrutura segura é primordial para garantir a qualidade das informações geradas.

A *Information Systems Audit and Control Foundation* (ISACA) desenvolveu um modelo de boas práticas de tecnologia da informação (TI) em 1996, o COBIT, para orientar o controle de dados à alta governança. A primeira versão constitui em uma orientação para a auditoria do sistema, que ao longo do tempo foi se evoluindo às

necessidades geradas pelas novas modernizações, voltando-se às práticas de orientação de gestão de TI à governança.

A versão 4, lançada em 2005, foi a primeira totalmente voltada para a gestão de TI, e não mais um *framework* para orientar as auditorias de sistema, que era o objetivo central da ISACA quando da sua primeira publicação. Este modelo atua com foco na orientação da gestão, com publicações que abordam os processos e as responsabilidades relacionados à TI na criação de valor (Val IT) e sobre gerenciamento de riscos (Risk IT). Essas características surgiram na versão 4 e tiveram suas abordagens aprofundadas na última versão (COBIT 5).

Esta última publicação, também chamada COBIT 5, é a versão utilizada como parte do desenvolvimento da metodologia criada neste produto (P1), tendo em vista que nesta versão estão inseridos, de modo mais uniforme e contínuo, os elementos abordados sobre a gestão de TI contidos em todas as publicações da ISACA.

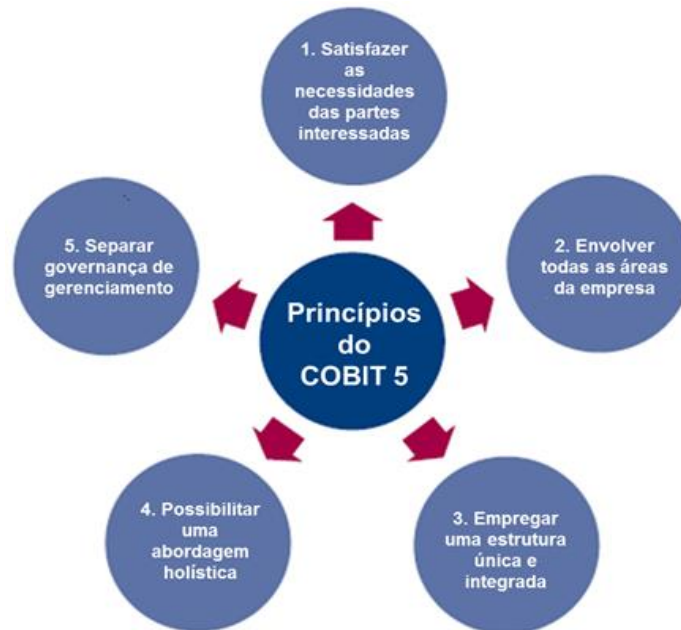
O uso do COBIT 5 objetiva atingir a criação de valor para a organização, através do uso eficiente e inovador de TI na organização, com cobertura de ponta-a-ponta para proporcionar a melhoria das relações entre as necessidades corporativas e o uso de tecnologia da informação, colaborando para a precisão dos dados gerados pela CAESB.

Um estudo estimou que falhas de software custam às empresas de \$50 a \$80 bilhões anualmente¹⁹. Para diminuir estas perdas, o COBIT 5 auxilia no mapeamento de riscos especificamente voltados ao gerenciamento de TI e na discriminação de controles para gerir a tecnologia da informação.

Para que a gestão do gerenciamento de TI seja integrada e satisfatória às corporações, o COBIT 5 estabelece cinco princípios básicos que são os pilares para as orientações do modelo:

¹⁹ CIO *Journal*, citado no *The Wall Street Journal* em janeiro de 2014.

Figura 7: Princípios Básicos do COBIT 5



Fonte: ISACA – COBIT 5

Com base na publicação “COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização”, temos as seguintes definições:

- **Atender às Necessidades das Partes interessadas:**

Organizações existem para criar valor para suas Partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 5 fornece todos os processos necessários e demais habilitadores para apoiar a criação de valor para a organização com o uso de TI. Como cada organização tem objetivos diferentes, o COBIT 5 pode ser personalizado de forma a adequá-lo ao seu próprio contexto por meio da cascata de objetivos, ou seja, traduzindo os objetivos corporativos em alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos.

- **Cobrir a Organização de Ponta a Ponta:**

O COBIT 5 integra a governança corporativa de TI organização à governança corporativa:

-Cobre todas as funções e processos corporativos. O COBIT 5 não se concentra somente na ‘função de TI’, mas considera a tecnologia da informação e tecnologias relacionadas como

ativos que devem ser tratados como qualquer outro ativo por todos na organização.

-Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, de ponta a ponta, ou seja, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização.

- **Aplicar Um Modelo Único Integrado:**

Há muitas normas e boas práticas relacionadas a TI, cada qual provê orientações para um conjunto específico de atividades. O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como um modelo unificado para a governança e gestão de TI da organização.

- **Permitir uma Abordagem Holística:**

Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização.

Habilitadores são geralmente definidos como qualquer coisa que possa ajudar a atingir os objetivos corporativos. O modelo do COBIT 5 define sete categorias de habilitadores: Princípios, Políticas e Modelos, Processos, Estruturas Organizacionais, Cultura, Ética e Comportamento, Informação, Serviços, Infraestrutura e Aplicativos e Pessoas, Habilidades e Competências.

- **Distinguir a governança da gestão:**

O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciadas e servem a propósitos diferentes. A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:

-A governança garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.

-A gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.

A versão COBIT 5 integra as demais publicações da ISACA (*Information Systems Audit and Control Foundation*) criando um planejamento que se adapta a entidade e as suas necessidades e objetivos. Este framework busca criar uma consciência de que a TI deve ser parte integrante de toda a estrutura organizacional da entidade, da gestão de risco e políticas. O funcionamento eficaz de TI gera informações mais objetivas e relevantes para a governança.

3.3. As Três Linhas De Defesa

A metodologia de Três Linhas de Defesa foi publicada em 2013 pelo *The Institute of Internal Auditors* (IIA) com o objetivo de auxiliar a governança e a alta administração a estruturar melhor a função de cada funcionário no departamento, delimitando suas funções e responsabilidades a fim de evitar lacunas ou duplicações, buscando a coesão e coordenação das tarefas. Com esta estruturação, que se baseia nas necessidades de cada entidade, há melhora na comunicação do gerenciamento de riscos e controle, o que evita falhas, pois há esclarecimento adequado dos papéis e responsabilidades.

Para manter a qualidade do controle interno da entidade, o método se baseia na integração entre todas as equipes, sejam auditores internos, especialistas em gerenciamento de riscos e em controle interno, e demais profissionais da área de riscos e controle para que os resultados sejam mais eficazes. Cada função possui seu dever dentro da cadeia do controle e apesar de haver uma divisão contínua dos departamentos, elas devem funcionar em sintonia para otimizar riscos.

Mesmo com a governança e a alta administração fora das Três linhas, elas designam um papel de grande importância na orientação dos demais setores, pois possuem a melhor posição para ajudar e garantir que as três linhas de defesa atuem em sua melhor forma. São responsáveis por estabelecer os objetivos a serem cumpridos, bem como a definição da estratégia e a formação de uma estrutura que melhor gerencie os riscos durante a realização dos objetivos.

Vejamos abaixo como a estrutura de Três Linhas de Defesa se organiza setorialmente:

Figura 8: Estrutura de Três Linhas de Defesa



Fonte: Adaptação da *Guidance on the 8th EU Company Law Directive* da ECIIA-FERMA, artigo 41

Conforme a “Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles” de 2013, temos as definições de como as linhas de defesa são gerenciadas:

1ª Linha de Defesa: Gestão Operacional

A linha de frente é responsável pelos processos de monitoramento e controle, através da administração. A gerência operacional deve conduzir procedimentos para gerenciar os riscos continuamente, uma vez que são os responsáveis pelos riscos.

Como primeira linha de defesa, os gerentes operacionais gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

A gestão guia o desenvolvimento dos procedimentos de controle interno, baseando nas políticas da organização, garantindo que as atividades executadas estejam de acordo com as metas e objetivos corporativos.

2ª Linha de Defesa: Funções de Gerenciamento de Riscos e Conformidade

Para evitar falhas em virtude do acúmulo de atividades, há uma segunda linha de defesa que se integra à primeira, apoiando as políticas de gestão já previamente definidas e auxiliando a gerência a desenvolver processos de controle. As principais funções desta linha são:

- a) Facilitar e monitorar a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional e auxiliar os proprietários dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas aos riscos em toda a organização.
- b) Monitorar diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis. Nesse quesito, a função separada reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade.
- c) Monitorar os riscos financeiros e questões de reporte financeiro.

3ª Linha de Defesa: Auditoria Interna

O pilar da terceira linha é a auditoria interna que avalia se os processos de controle interno estão sendo eficazes e eficientes para com as metas definidas pela alta governança, e busca identificar as falhas, a fim de que haja uma correção célere para que não afete o desenvolvimento das informações geradas pelo controle interno.

Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização. Esse alto nível de independência não está disponível na segunda linha de defesa. A auditoria interna provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle.

Fonte: Disponível em:

http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf. Acesso em: setembro de 2017

O relatório da auditoria interna deve incluir a verificação de eficiência e eficácia das operações, salvaguarda de ativos, procedimentos e contratos e demais elementos da estrutura de gerenciamento de riscos que são reportados à governança e a alta administração, vez que todos esses processos devem atuar sob normas internacionais, preservando a independência do auditor interno. (IIA, 2013). O IIA vê a atividade do auditor interno como sendo indispensável a qualquer tipo ou porte de organização, pois esta função “garante a eficácia de seus processos de governança e gerenciamento de riscos”.

Muitas organizações utilizam as Três Linhas de Defesa por meio de uma abordagem misturada, como exemplo, a combinação ou consolidação da segunda linha de defesa com a auditoria interna. Deste modo, algumas tarefas passam a ser designadas por auditores que, na falta do setor específico, podem se responsabilizar por revisões de empréstimos, *compliance* e coordenação de gerenciamento de riscos (Burke e Jameson - CBOK, 2015), salvo que esta atuação do auditor não pode interferir em sua função principal de reporte do CAE ao comitê de auditoria da instituição.

A Declaração de Posicionamento do IIA (2013) diz que *“já que cada situação é única e situações específicas variam, não há uma forma ‘certa’ de coordenar as Três Linhas De Defesa”*. Cada sociedade corporativa tem suas próprias características e suas próprias necessidades. O método das Três Linhas de Defesa possibilita que o gerenciamento de risco seja mais sólido, uma vez que sua estrutura conta com 3 linha de defesa, que quando separadas e claramente identificadas se tornam mais robustas ao gerenciamento de riscos.

Para a certificação dos dados, além da facilidade de adaptação do método, este sistema possibilita às entidades maior solidez em suas análises, pois o controle interno se torna mais sólido em virtude da nítida delegação das funções e atividades de cada colaborador da entidade, aumentando o rendimento e a produtividade de seus funcionários, mitigando as chances de falhas.

3.4. ISO 31000: Gestão de Riscos

O ISO 31000 tem como objetivo oferecer diretrizes, de modo amplo, para a gestão de riscos, podendo ser utilizado em qualquer estrutura empresarial (empresa, pública, privada, associações ou indivíduos), embora não pretenda promover a uniformidade da gestão, pois esta está diretamente relacionada às necessidades específicas de cada organização. A pretensão da norma é harmonizar os processos de gestão de riscos, apoiando demais Normas que tratem de riscos.

Princípios da Norma ISO 31000:

A base da Norma está voltada para a gestão de risco que deve:

- a) Contribuir para a realização dos objetivos e para a melhoria do desempenho em âmbito total referente a entidade, sendo uma atividade que integra todos os procedimentos organizacionais.
- b) Auxiliar os tomadores de decisão a fazer escolhas conscientes, considerando as incertezas e suas naturezas, mantendo uma abordagem sistemática, oportuna e estruturada que deve ser baseada em fontes de informação, alinhadas ao contexto interno e externo da organização.
- c) Reconhecer os fatores humanos e culturais que podem determinar a realização dos objetivos da organização, identificando as mudanças. Visto que após eventos externos e internos, riscos podem surgir ou desaparecer, melhorias contínuas na organização devem ser desenvolvidas.

Processo:

O processo de gestão de riscos deve ser parte integrante da gestão, coligado às boas práticas culturais da entidade e aos processos de negócio da organização. Há pontos de extrema relevância para que o processo seja integrado e eficaz.

Comunicação e consulta:

Convém que os planos de comunicação e consulta sejam desenvolvidos em um estágio inicial. Convém que estes planos abordem questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-los. Convém que comunicação e consulta interna e externa eficazes sejam

realizadas a fim de assegurar que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas.

Estabelecimento do contexto

Ao estabelecer o contexto, a organização articula seus objetivos, define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e estabelece o escopo e os critérios de risco para o restante do processo. [...] ao se estabelecer o contexto para o processo de gestão de riscos, eles precisam ser considerados com mais detalhe. Em particular, como eles se relacionam com o escopo do respectivo processo de gestão de riscos.

Avaliação de riscos: este processo é separado em três outras etapas:

a) Identificação:

Convém que a organização identifique as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. A identificação abrangente é crítica, pois um risco que não é identificado nesta fase não será incluído em análises posteriores.

b) Análise:

[...] envolve desenvolver a compreensão dos riscos. A análise de riscos fornece uma entrada para a avaliação de riscos e para as decisões sobre a necessidade de os riscos serem tratados, e sobre as estratégias e métodos mais adequados de tratamento de riscos. A análise de riscos também pode fornecer uma entrada para a tomada de decisões em que escolhas precisam ser feitas e as opções envolvem diferentes tipos e níveis de risco.

c) Avaliação:

A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de

risco estabelecidos quando o contexto foi considerado. Com base nesta comparação, a necessidade do tratamento pode ser considerada.

Tratamento de riscos:

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes. Tratar riscos envolve um processo cíclico composto por: avaliação do tratamento de riscos já realizado, decisão se os níveis de risco residual são toleráveis, se não forem toleráveis, a definição e implementação de um novo tratamento para os riscos e avaliação da eficácia desse tratamento.

Monitoramento e análise crítica:

Convém que o monitoramento e a análise crítica sejam planejados como parte do processo de gestão de riscos e envolvam a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico. Convém que as responsabilidades relativas ao monitoramento e à análise crítica sejam claramente definidas.

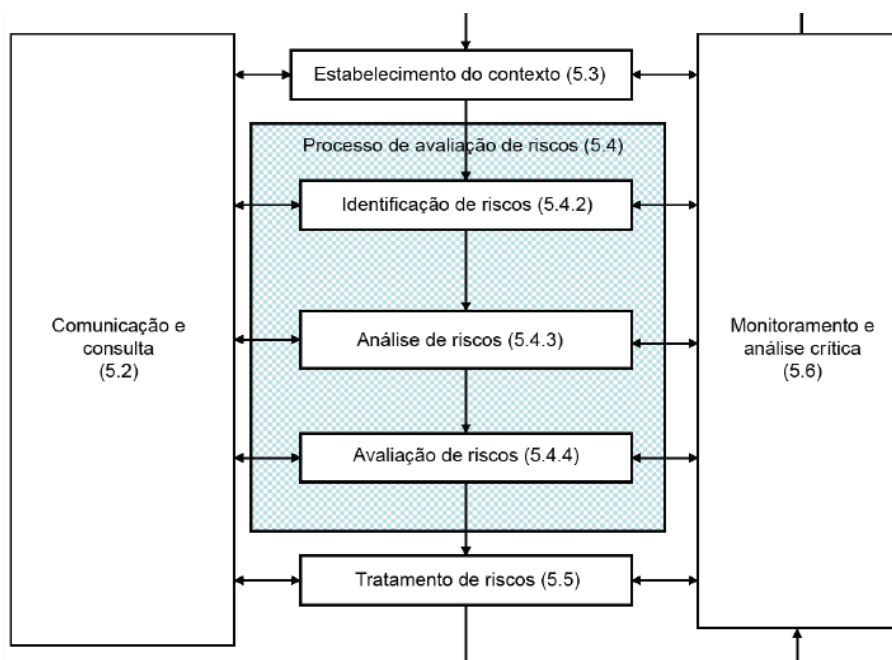
Convém que os processos de monitoramento e análise crítica da organização abranjam todos os aspectos do processo da gestão de riscos com a finalidade de: garantir que os controles sejam eficazes e eficientes no projeto e na operação, obter informações adicionais para melhorar o processo de avaliação dos riscos, analisar os eventos, mudanças, tendências, sucessos e fracassos e aprender com eles, detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos dos riscos e suas prioridades e identificar os riscos emergentes.

Registros do processo de gestão de riscos:

Convém que as atividades de gestão de riscos sejam rastreáveis. No processo de gestão de riscos, os registros fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo. Convém que as decisões relativas à criação de registros levem em consideração: a necessidade da organização de aprendizado contínuo, os custos e os esforços envolvidos na criação e manutenção de registros, as necessidades de registros legais, regulatórios e operacionais, o método de acesso, facilidade de recuperação e meios de armazenamento e a sensibilidade das informações.

A figura abaixo mostra o processo num organograma:

Figura 9: Processo de Auditoria Interna para ISO 31000



Fonte: ABNT - ISO 31000

O ISO 31000 fornece uma padronização básica de controle, de forma ampla, que tem como fundamento um processo cíclico cujo qual, todos os processos devem estar interligados e funcionando de modo a complementar os processos anteriores, criando uma rede que assegura o funcionamento contínuo do controle interno, o que gera mais segurança para a governança, em especial, quando se faz necessário o uso das informações providas deste setor.

3.5. ISO 19011: Diretrizes para Auditorias de Sistema e Gestão da Qualidade

A Norma estabelece uma direção para os princípios de auditoria, gestão de programas de auditoria, realização de auditorias de sistema de gestão de qualidade e auditorias de sistema de gestão ambiental e quanto às habilidades requeridas dos auditores de sistemas de gestão da qualidade ambiental em todos os níveis de organização.

São estabelecidas definições baseadas na NBR ISO 9000 e ISO 14050 para termos que estão descritos em NBR ISO 19011, dentre os principais, estão a definição

de auditoria, evidência, conclusão, plano e escopo de auditoria e competência. Com base na publicação da Associação Brasileira de Normas Técnicas (ABNT), temos:

Princípios de auditoria:

A auditoria é caracterizada pela confiança em alguns princípios. Eles fazem da auditoria uma ferramenta eficaz e confiável em apoio a políticas de gestão e controles, fornecendo informações sobre as quais uma organização pode agir para melhorar seu desempenho. A aderência a estes princípios é um pré-requisito para se fornecer conclusões de auditoria que são relevantes e suficientes.

Gerenciamento:

Um programa de auditoria pode incluir uma ou mais auditorias, dependendo do tamanho, natureza e complexidade da organização a ser auditada. Estas auditorias podem ter uma variedade de objetivos e podem também incluir auditorias combinadas ou auditorias em conjunto.

Um programa de auditoria também inclui todas as atividades necessárias para planejar e organizar os tipos e números de auditorias e para fornecer os recursos para conduzi-las eficaz e eficientemente dentro do espaço de tempo especificado. Uma organização pode estabelecer mais de um programa de auditoria.

Atividades de auditoria: “planejar e gerenciar atividades de auditoria como parte de um programa de auditoria. A abrangência na qual as providências desta seção são aplicáveis depende do escopo e complexidade da auditoria específica e o uso pretendido para as conclusões da auditoria.” Nesta seção temos uma delimitação de processos que devem ser executados pela auditoria, ordenados pela definição da equipe de auditoria, análise de documentos, fundamentando o plano de auditoria, com comunicação aberta para com os auditados e, por fim, concluir o relatório de auditoria.

3.6. ISO 27001: Sistema de Gestão de Segurança da Informação (SGSI)

A Norma foi elaborada com o objetivo de estabelecer diretrizes para implementar um Sistema de Gestão de Segurança e Informação (SGSI), a fim de proteger

os dados financeiros e confidenciais, minimizando os riscos de serem acessados irregularmente.

Os principais benefícios com o uso da Norma acontecem com a identificação de riscos e modos para gerenciá-los além de fornecer uma estrutura flexível que se adapta aos controles de diferentes naturezas empresariais, atendendo às expectativas mais sensíveis do mercado por meio da demonstração de conformidade.

A ISO 27001 possui focos separados pelos seguintes grupos: política de segurança, organização da segurança da informação, gerenciamento de ativos, segurança de recursos humanos, prevenção de que pessoas não autorizadas tenham acesso a informações confidenciais, gerenciamento de comunicação e operações e conformidade regulatória.

The image features a 3D grid of blue cubes, with some cubes missing or offset, creating a sense of depth and structure. In the upper right corner, there is a stylized blue flame icon. The background is a dark blue gradient with a fine, repeating pattern of small squares or dots.

METODOLOGIA

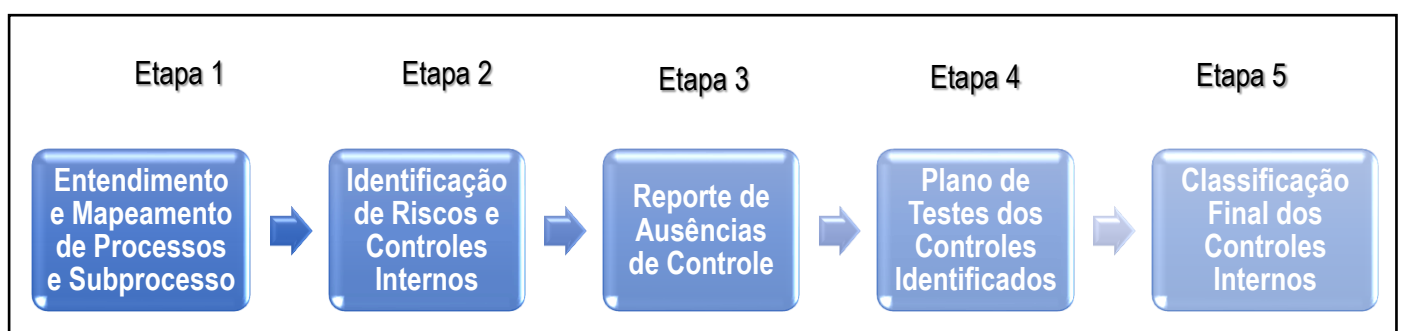
4. Metodologia

O presente trabalho integra as metodologias mais utilizadas e reconhecidas no mercado nacional e internacional. Como pilar do desenvolvimento temos o COSO: *Internal Controls* que desde sua criação tem por objetivo a certificação de informações e relatórios. Complementarmente ao COSO, para ações de gerenciamento de riscos foram adotados: o ISO 27001, ISO 31000 e COBIT 5, que tratam de diretrizes para gerir riscos amplos, gestão de riscos e riscos de Tecnologia da Informação, respectivamente.

Para classificação dos controles internos, será utilizada a metodologia estabelecida pelo Projeto Acertar, com o intuito de certificar as informações do SNIS (Sistema Nacional de Informações sobre Saneamento) estabelecendo um índice para classificação de acordo com a confiança e exatidão das informações obtidas.

A execução da metodologia COSO seguirá de acordo com as seguintes etapas: Entendimento e Mapeamento de Processos e Subprocessos, Identificação de Riscos e Controles Internos, Reporte de Ausências de Controle, Plano de Testes dos Controles Identificados e Classificação Final dos Controles Internos.

Figura 10: Etapas da Metodologia



4.1. Entendimento e Mapeamento de Processos e Subprocessos

A primeira etapa da execução da metodologia consiste no mapeamento dos processos efetuados pela Concessionária para a geração das informações repassadas à ADASA. Esta etapa busca identificar os riscos que o procedimento utilizado pelo agente

prestador está submetido, podendo comprometer a qualidade e fidedignidade dos dados.

O *Business Process Management Commom Body Knowlegde* – BPM CBOK, define processo como “uma agregação de atividades e comportamentos executados por humanos ou máquinas para alcançar um ou mais resultados”. Visto que, execução pode conter falhas e erros, submeter todos os procedimentos à análise da qualidade de seus respectivos controles internos é crucial para as demais etapas da metodologia. Para tal, o auditor deve coletar as informações que julgar necessárias e desenvolver um método de representação gráfica facilitando o entendimento da organização quanto a geração dos dados.

4.1.1. Levantamento de dados

Para iniciar a coleta de informações, o auditor pode se respaldar na busca de dados desde os mais genéricos, como os dados que são de livre acesso à todo o público, como também obter informações por meio de cada etapa executada pelo controle interno, a fim de gerar maiores detalhes do gerenciamento do processo, otimizando a busca por riscos que podem impactar no resultado final da execução do processo.

Para que o levantamento dos dados seja preciso e objetivo, há diversos métodos que o auditor pode utilizar para maximizar a segurança da análise, tal como fazer uso do fluxograma, que é a opção representativa mais indicada para esta análise.

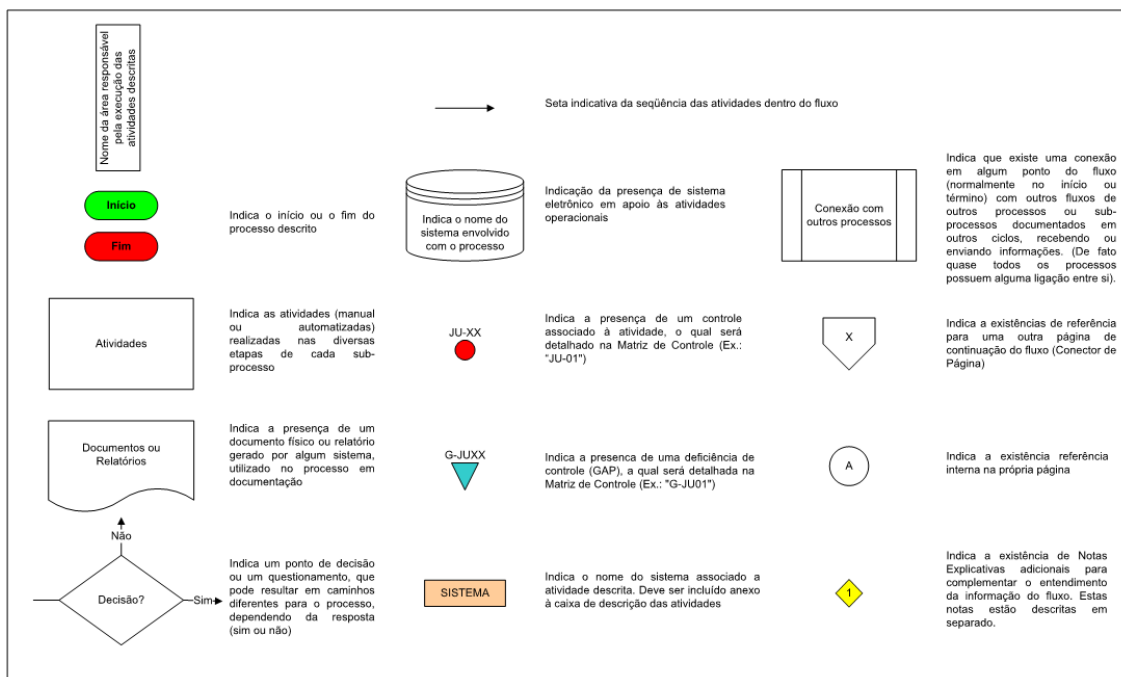
4.1.2. Metodologia para elaboração de fluxograma

O fluxograma é uma representação ilustrativa didática que demonstra, de modo simplificado, as etapas de processos e podem ser usados para todas as finalidades, visto que seus símbolos, que são os componentes essenciais para sua elaboração, têm características genéricas utilizando formas geométricas para representar o início ou o fim e setas indicativas de direcionamento.

Esta representação é muito adequada para iniciar um mapeamento, pois tal instrumento visual auxilia numa rápida captura dos elementos básicos do processo pelos

envolvidos na análise. Na Figura 13 temos os principais símbolos empregados na elaboração do fluxograma, bem como suas definições mais usuais.

Figura 11: Símbolos do Fluxograma



O mapeamento de processos é uma etapa importante, inclusive para a metodologia COSO, pois procura retratar o ambiente de controle da empresa em estudo. O auditor utiliza este recurso para entender e delimitar quais atividades são executadas para a geração de informações, como são feitas, quem as realiza, possibilitando a checagem do fluxo de dados e seus riscos, e quais os controles já existentes. Para que o mapeamento seja eficiente deve conter:

- Atividades de controles executados
- Quem realiza as atividades
- Qual a seqüência efetiva
- Como as atividades são realizadas (manualmente/ automaticamente)
- Periodicidade da realização da atividade
- Riscos existentes no Processo analisado

4.2. Identificação de Riscos e Controle

Conforme a análise dos procedimentos realizados pela fase anterior, deve-se identificar a quais riscos os controles estão submetidos, possibilitando, assim, a criação de um levantamento de possíveis falhas na geração das informações, conforme exemplo a seguir:

Tabela 2: Exemplo de Identificação de Riscos e Controles

Ref.	Controle Identificado	Risco
CC-34	Mensalmente o assistente contábil prepara a conciliação do Contas a pagar, por meio do relatório contábil do sistema Oracle "Balancete de contas a pagar", comparando com o relatório financeiro do sistema Oracle "Saldo de contas a pagar". Ao final da conciliação o assistente imprime a conciliação e assina enviando para gerente que revisa e assina a conciliação.	Pagamentos duplicados devido à realização de adiantamento aos fornecedores.

Desde a primeira publicação do COSO – *Internal Controls* em 1992, seu objetivo central era a verificação fidedigna das informações geradas pelas entidades. Partindo deste pressuposto, a fim de atender as necessidades da ADASA, a metodologia foi desenvolvida a partir da publicação atualizada em 2013²⁰ que fornece dezessete princípios fundamentais para a efetividade do *framework*, que serão utilizados para a criação dos estágios e para análise dos procedimentos de geração de informação através do controle interno.

Tabela 3: Princípios do COSO

Componente	Princípio
Ambiente de Controle	1 - Comprometimento com integridade e valores éticos
	2 - Reforçar responsabilidades de supervisão
	3 - Estabelecer estrutura de responsabilidades e autoridade
	4 - Demonstrar compromisso com a competência
	5 - Reforçar responsabilidade por prestação de contas
Avaliação de Riscos	6 - Especifica objetivos relevantes
	7 - Identifica e avalia os riscos
	8 - Avalia riscos de fraudes
	9 - Identifica e avalia mudanças relevantes

²⁰ Este *framework* é detalhado na seção 3.1

Componente	Princípio
Atividades de Controle	10 – Seleciona e desenvolve atividades de controle
	11 – Seleciona e desenvolve atividades de controle em TI
	12 – Estabelecimento através de políticas e procedimentos
Comunicação e Informação	13 - Obtém, gera ou utiliza informações relevantes
	14 – Comunicação interna
	15 – Comunicação externa
Monitoramento	16 – Realiza avaliações contínuas ou independentes
	17 – Avalia e comunica deficiências a alta administração

Fonte: Adaptado de COSO – *Internal Control*

Com base nestes princípios, buscou-se estruturar a metodologia a partir das características peculiares à ADASA formando, assim, uma metodologia focada no aprimoramento do controle interno: identificando os riscos, estabelecendo atividades sistemáticas de controle, padrões de comunicação e informação e mantendo avaliações contínuas para monitoramento.

Para auxiliar a identificação dos riscos, foram utilizadas mais três metodologias, complementarmente ao COSO, em busca do aperfeiçoamento deste estágio, que são: as normas ISO 27001, ISO 31000 e COBIT 5, descritas anteriormente.

4.3. Reportar ausências de controles internos

Após a finalização dos estágios anteriores, estarão delimitados quais procedimentos são realizados pela Concessionária para propiciar as informações de interesse. Deste modo, com todos os riscos já devidamente identificados, se faz necessário o reporte das lacunas onde o controle interno não atua. Para tal, esta ausência de controle deve ser reportada a fim de que o agente prestador possa tomar medidas para preencher estas ausências maximizando o nível de confiança de seus dados.

Essas informações farão parte da Matriz de Risco dos Processos analisados, onde serão consolidadas as informações de: atividades, riscos, controles e *gaps* identificados, bem como, o resultado dos testes realizados para validação da eficácia dos controles internos.

4.4. Plano de Teste dos Controles Identificados

Com o fluxograma dos controles internos existentes já elaborado, é preciso avaliar a efetividade de cada controle, para isso mais de um atributo deve ser testado e com base no resultado destes testes, o auditor deve definir uma classificação do nível de implementação para cada controle interno. A Tabela 3 sugere uma classificação:

Tabela 4: Classificação dos Controles Internos

Sigla	Descrição	Peso
NI	Não Implementado	0%
PI	Parcialmente Implementado	50%
IM	Implementado	100%

Com todos os controles internos devidamente classificados, a média ponderada do peso de cada controle presente na atividade em questão resulta num **percentual de confiança**:

Tabela 5: Exemplo de Classificação dos Controles Internos

Informação da CAESB	CT 001	CT 002	CT 003	CT 004	Percentual de Confiança = 38%
Volume de água faturado	NI	IM	PI	NI	
Peso	0%	100%	50%	0%	

O percentual de confiança é um índice entre 0 e 100%, este indicador é convertido a uma classificação de uma a três estrelas, conforme tabela abaixo:

Tabela 6: Classificação da Avaliação de Confiança

Nível de Confiança	Avaliação
Alto Maior que 75%	★ ★ ★
Médio Entre 75% e 50%	★ ★
Baixo Menor que 50%	★

A maturidade do procedimento pode levar a Agência a alterar os indicadores de confiança, ou seja, a abrangência da avaliação entre alto, médio e baixo conforme novos controles forem inseridos e/ou modificados. No trabalho do auditor devem constar todas as atividades e procedimentos realizados para testar os níveis de implementação dos controles internos. Estes testes devem estar descritos em relatório, pois assim, em caso de alteração dos controles já testados, estes relatórios facilitam a compreensão de tal avaliação, contribuindo para a melhoria dos procedimentos e sua possível readaptação de abrangência.

Dentre os testes dos controles existentes, alguns necessitam de uma **seleção de amostras** para serem realizados, que pode variar conforme o tamanho da população e a periodicidade das ações de controle. Importante ressaltar que a amostragem deve ser feita de forma aleatória, com objetivo de não criar viés na amostragem, para que se possa valer de critérios estatísticos posteriores para a interferência sobre a população analisada.

Tabela 7: Definição da Amostra

Periodicidade	População	Amostra
Várias vezes ao dia	Acima de 250	45
Diário	250	25
Semanal	52	10
Mensal	12	3
Trimestral	4	2
Semestral	2	1
Anual	1	1
Automático	1	N/A*

(*) controles automáticos deverão ser testados
uma vez ao ano

A população em questão é o objeto analisado, por exemplo, em um teste de controle de pagamentos em que são efetuados mais de 250, a população em questão são os pagamentos realizados que, conforme a tabela, devem ter selecionadas 45 amostras aleatórias para avaliação.

Para que o controle obtenha a classificação de “Implementado” é desejável que não haja nenhum tipo de desvio na amostra analisada. Caso a avaliação da amostra seja

inconsistente para que o auditor tome sua avaliação, amostras maiores podem ser selecionadas para realizar uma avaliação mais abrangente.

Os procedimentos e testes substantivos são utilizados, também, para avaliar o **nível de exatidão** das informações. Para compor esta avaliação, o nível de confiabilidade previamente estabelecido no estágio anterior define a extensão dos procedimentos que devem ser aplicados nesta nova fase.

Tabela 8: Exemplo de Teste Substantivo e Percentual de Desvio

Informação da CAESB	Teste Substantivo	Valor Declarado	Valor Recalculado	% de desvio
Volume de Esgoto Coletado	Realizar recálculo, tendo em vista que o volume de esgoto coletado é considerado como sendo de 80% a 85% do volume de água consumido.	135.241.105	137.945.927	2

O percentual de desvio representa a diferença entre os valores declarados e os recalculados, assim, com base neste percentual calculado deve enquadrá-lo num nível de exatidão, conforme tabela abaixo.

Tabela 9: Classificação da Avaliação de Exatidão

Nível de Exatidão	Desvio	Avaliação
Alto	Entre 0% e 2%	★ ★ ★
Médio	Maior que 2% e menor ou igual a 5%	★ ★
Baixo	Maior que 5%	★

Os índices de desvio tolerados para cada classificação podem ser modificados conforme o apetite ao risco da ADASA, como por exemplo aumentar a aceitação de desvio para até 5% na classificação de “Alto” / três estrelas do nível de exatidão, contanto que o nível mais baixo de classificação de avaliação não supere 10% de desvio.

Para definir o **tamanho da amostragem** a ser utilizada nos testes substantivos, o primeiro passo é definir a materialidade, ou seja, o limite em que os desvios identificados na Segunda Etapa se tornam relevantes, para isso é necessário definir um

*benchmark*²¹, que pode ser definido através do grupo de informação, como no exemplo a seguir.

Tabela 10: Exemplo de Benchmark

Grupo	Benchmark
Consumo	Consumo de energia elétrica nos sistemas de água 2.000.000


Assim, aplica-se um percentual de redução a este valor, que se relaciona diretamente com a classificação da Avaliação de Confiança realizada anteriormente, conforme tabela.

Tabela 11: Definição do Percentual de Redução

Avaliação de Confiança	Percentual de Redução
★ ★ ★	4%
★ ★	3%
★	2%

A materialidade de cada grupo é definida por meio da multiplicação do percentual de redução, conforme Avaliação de Confiança, e a população.

Figura 12: Exemplo de Cálculo de Materialidade

	<i>Benchmark</i>	2.000.000
	Percentual de Redução	3%
	(=) Materialidade	60.000

Para definir o tamanho da amostra, deve-se dividir a população pela materialidade obtendo, assim, um múltiplo que por meio da integração à Avaliação de Confiança, define o tamanho da amostra, como no exemplo a seguir.

²¹ *Benchmark* é um banco de teste, em tradução literal, que se relacionam ao teste a ser executado e a natureza das informações

Figura 13: Exemplo de Cálculo do Múltiplo

População	1.000.000
Materialidade	60.000
(=) Múltiplo Calculado	17
Múltiplo mais próximo na Tabela	15

Em resumo, temos:

Seleção de Amostras - Procedimentos Substantivos	
Benchmark	2.000.000
Avaliação de Confiança	
Percentual de Redução	3%
Materialidade	60.000
População	1.000.000
Múltiplo Calculado	17
Múltiplo mais Próximo na Tabela	15
Tamanho da Amostra	23

Múltiplo	Avaliação de Confiança		
	★ ★ ★	★ ★	★
1x	1	2	3
2x	2	3	6
3x	3	5	9
4x	3	6	12
5x	4	8	15
6x	5	9	18
7x	5	1	21
8x	6	12	24
9x	7	14	27
10x	7	15	30
15x	11	23	45
20x	14	30	60
25x	18	38	75
30x	21	45	75
40x	28	60	75
50x	35	75	75
100x	70	75	75
200x ou mais	75	75	75

A partir do cálculo de definição da amostra, é possível observar que o nível de Confiança obtido no teste influencia diretamente no tamanho da amostra, pois quanto maior o nível, menor o tamanho dos dados a serem testados. Salienta-se, ainda, que esta definição deve ser feita por meio de um *software* ou uma ferramenta que permita uma seleção aleatória, para garantir a equidade de que toda a população tenha as mesmas chances de ser selecionada.

A aplicação dos testes substantivos tem o objetivo de verificar as informações do prestador fornecidas para a Agência, a fim de estabelecer se os dados refletem de

fato os eventos ocorridos. Quando a confiança for definida como um índice baixo, não deve ter sua exatidão avaliada pois este resultado demonstra que o prestador não possui instrumentos suficientes de controle para garantir a fidedignidade das informações.

Tal como a baixa avaliação de confiança implica em uma insuficiência para avaliar a exatidão das informações, a impossibilidade de aplicar os testes substantivos deve ter sua exatidão classificada como baixa.

4.5. Classificação final dos Controles Internos

A classificação dos controles internos existentes é obtida por meio da combinação das Avaliações de Confiança e de Exatidão a fim de obter uma única classificação, como demonstrado na matriz a seguir.

Tabela 12: Matriz de Classificação Final

Exatidão	★ ★ ★	N/A	6	7
	★ ★	N/A	4	5
	★	1	2	3
		★	★ ★	★ ★ ★
		Confiança		

A unificação dos resultados dos estágios anteriores resulta numa classificação de 1 a 7, com suas respectivas descrições:

- NC

Não Certificado: a informação não passou pelo processo de auditoria e certificação
- 1

A informação possui baixo nível de confiança e, portanto, não teve exatidão avaliada.
- 2

A informação possui um médio nível de confiança e teve sua exatidão avaliada como baixa ou não avaliada
- 3

A informação possui um alto nível de confiança e teve sua exatidão avaliada como baixa ou não avaliada

4

A informação possui níveis médios de confiança e exatidão

5

A informação possui um alto nível de confiança e médio nível de exatidão

6

A informação possui um médio nível de confiança e alto nível de exatidão

7

A informação possui os níveis máximos de confiança e exatidão

Deste modo, entende-se que quando um controle é classificado com avaliação de confiança mínima, este não deve ter sua exatidão avaliada, visto que os controles internos são incapazes de gerar informações que mantenham os padrões de confiabilidade para que se execute os testes substantivos.

The background is a complex 3D composition. At the top, a blue keyboard is shown from an isometric perspective. To its right is a large, stylized blue flame icon. Below these elements is a green grid pattern that appears to be a top-down view of a cube or a similar 3D structure. The overall color palette is dominated by blues and greens, with a textured, grid-like appearance throughout.

REFERÊNCIAS BIBLIOGRÁFICAS

5.Referências

ABES e BIS - Associação Brasileira de Engenharia Sanitária e Ambiental e Banco Interamericano de Desenvolvimento. **Diagnóstico Setorial e Proposta de Ações do Projeto de Regulação do Setor de Água e Saneamento.** Disponível em <<http://abes-dn.org.br/pdf/DiagSetorial.pdf>>. Acesso em setembro de 2017.

ACFE - *The Association of Certified Fraud Examiners.* **Report to the Nations: On occupational fraud and abuse.** 2014. Disponível em: <<https://www.acfe.com/rtnn/docs/2014-report-to-nations.pdf>>. Acesso em: setembro de 2017.

ADASA, Agencia Reguladora de Águas, Energia e Saneamento Básico do Distrito Federal. **Resolução nº08/2016.** Disponível em: <http://www.adasa.df.gov.br/images/stories/anexos/8Legislacao/Res_ADASA/Resolucao008_2016.pdf>. Acesso em 23 de agosto de 2017.

ALKAFAJI, Yass et. Al. **Pesquisa Global de Auditoria Interna do IIA: Um Componente do Estudo CBOK, Características de uma Atividade de Auditoria Interna,** 2010.

ALMEIDA, Marcelo Cavalcanti. **Auditoria: um Curso Moderno e Completo.** 8ª ed. São Paulo: Atlas, 2012.

ARAJ, Farah G. **Reagindo ao Risco de Fraude: Explorando a Posição da Auditoria Interna.** Publicado em CBOK do IIA, 2015.

ATTIE, William. Auditoria. **Conceitos e Aplicações.** 6ª ed. São Paulo: Atlas, 2011.

AVALOS, José Miguel Aguilera. **Auditoria e gestão de riscos.** Instituto Chiavenato (org.). São Paulo. Saraiva, 2009.

BRASIL. Conselho Federal de Contabilidade. **NBC TA – de Auditoria Independente: NBC TA Estrutura Conceitual, NBC TA 200 a 810,** 2012.

BRASIL. Tribunal de Contas da União. **Acórdão TCU 2261/2011.** Ata Nº 35, de 24 de agosto de 2011. Disponível em: <www.tcu.gov.br>. Acesso em setembro de 2017.

BRASILIA. Poder Executivo. **Projeto de Lei PL 3337/2004.** Acresce e altera dispositivos das Leis nº 9.472, de 16 de julho de 1997, nº 9.478, de 6 de agosto de 1997, nº 9.782, de 26 de janeiro de 1999, nº 9.961, de 28 de janeiro de 2000, nº 9.984, de 17 de julho de 2000, nº 9.986, de 18 de julho de 2000, e nº 10.233, de 5 de junho de 2001, da Medida Provisória nº 2.228-1, de 6 de setembro de 2001, e dá outras providências. Disponível em: <<http://www.planalto.gov.br>>. Acesso em setembro de 2017.

BURKE, Jennifer F.; Jameson, Steven E. **Uma Visão Global da Auditoria de Serviços Financeiros: Desafios, Oportunidades E O Futuro.** Publicado em CBOK do IIA, 2015.

CANGEMI, Michael P. **Ficando Um Passo A Frente: O Uso da Tecnologia por Parte da Auditoria Interna**. Publicado em CBOOK do IIAF, 2015.

CASCARINO, Richard. **Auditor's Guide to Information Systems Auditing**. Publicado em John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.

CFC – Conselho Federal de Contabilidade. **Resolução CFC 986/03**. Disponível em: <www.cfc.org.br/sisweb/sre/docs/RES_986.doc>. Acesso em: setembro de 2007.

CGU – Controladoria-Geral da União. **Controles internos – Uma Abordagem da Estrutura Conceitual COSO**.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. **Gerenciamento de riscos na empresa: estrutura integrada**. Jersey City, NJ set, 2007. v. 2.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. **Controle Interno: Estrutura Integrada**. 2013.

DE CASTRO COSTA, Carlos José. **Monopólio natural: a legitimação do Monopólio para Minimizar os Custos de Produção**. Dissertação (mestrado) – Faculdade de Direito de Campos

DELOITTE Touche Tohmatsu. **Projeto Acertar – Desenvolvimento de Metodologias e Guias para Auditoria e Certificação de Informações do Sistema Nacional de Informações sobre Saneamento (SNIS)**. Brasília, 2017.

DI PIETRO, Maria Sylvia Zanella. **Limites da Função Reguladora das Agências Diante do Princípio da Legalidade**. In. DI PIETRO, Maria Sylvia Zanella (coord.). Direito Regulatório: Temas Polêmicos. Belo Horizonte: Fórum, 2003. p. 27-59.

FAYOL, Henri. **Administração industrial e geral**. 9.ed. São Paulo: Atlas, 1981.

FLORA, Philip E.; RAI, Sajay. **Lidando Com Os 10 Principais Riscos Tecnológicos: O Papel Da Auditoria Interna**. Publicado em CBOOK do IIAF, 2015.

FRANCO, Hilário & MARRA, Ernesto. **Auditoria Contábil**. 4ª edição. São Paulo: Atlas, 2001.

FRANCO, Hilário. **Auditoria Contábil**. 2. ed. São Paulo: Atlas, 1991.

GUIMARÃES, Camila. **“Fraudes Corporativas estão mais Sofisticadas”**, entrevista a Compagno em revista Exame. 2011. Disponível em: <<https://exame.abril.com.br/negocios/fraudes-corporativas-estao-mais-sofisticadas-m0079620/>>. Acesso em: setembro de 2017.

IBRACON, Instituto dos Auditores Independentes do Brasil. **Auditoria: Registros de uma Profissão**. Disponível em: <www.ibracon.com.br>. Acesso em Setembro de 2017.

IIA - *The Institute of Internal Auditors. As Três Linhas de Defesa no Gerenciamento Eficaz De Riscos e Controles*, 2013. Disponível em: <http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf>. Acesso em: setembro de 2017.

INTOSAI - Organização Internacional de Entidades Fiscalizadoras Superiores. **Normas de Auditoria da INTOSAI**. Emitido por INTOSAI,1992.

INTOSAI - Organização Internacional de Entidades Fiscalizadoras Superiores. ISSAI - Normas Internacionais das Entidades Fiscalizadoras Superiores. Emitido por INTOSAI, 2013.

ISACA - Information Systems Audit and Control Association. **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**. ISACA, 2012.

ISO, ABNT Norma NBR. 19011 (nov/2002): **Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental**. Rio de Janeiro: ABNT, 2002.

ISO, ABNT Norma NBR. 31000 (ago/2009): **Gestão de Riscos**. Rio de Janeiro: ABNT, 2009.

ISO, *International Organization of Standardization 27001 (nov/2013): Information Security Management Standard (ISO/IEC 27001)*. 2013

JOURAVLEV, Andrei. **Drinking water supply and sanitation services on the threshold of the XXI century**. Santiago do Chile: Cepal, 2004.

KRUGMAN, Paul; WELLS, Robin. **Introdução à economia**. Elsevier Brasil, 2007.

LUZA, Francisco S. **A Administração Estratégica à Luz da Nova Definição de Auditoria interna**. Dissertação (Mestrado) – Universidade Ibirapuera, São Paulo, 2001.

MOREIRA, Vital, **Auto-Regulação Profissional e Administração Pública**. Coimbra, Almedina, 1997.

NICHOLSON, Walter; SNYDER, Christopher M. **Intermediate Microeconomics and its Application**. Cengage Learning, 2014.

OLIVEIRA Luís Martins e DINIZ FILHO André. **Curso Básico De Auditoria**. São Paulo: Atlas; 2001.

PACHECO, Marcela Soares. Et al. **A História da Auditoria e suas novas tendências: um enfoque sobre a governança corporativa**. [Publicado],2010

PARDINI, Eduardo Person. **A Importância do Ambiente no Sistema de Controles Internos**, 2013.

PICKETT, Spencer. **The Essential Handbook of Internal Auditing**. Publicado em John Wiley & Sons, Inc., Hoboken, England, 2005.

PICKETT, Spencer. ***The internal auditor at work: A practical guide to everyday challenges***. John Wiley & Sons, 2004.

PIPER, Arthur. **Auditando o Setor Público**. Publicado em CBOK do IIARF, 2015.

PRESIDÊNCIA DA REPÚBLICA, **Lei 11.445, de 5 de janeiro de 2007**. Brasil, 2007

PRESIDÊNCIA DA REPÚBLICA, **Lei 11.638, de 28 de dezembro de 2007**. Brasil, 2007

PRESIDÊNCIA DA REPÚBLICA, **Lei 6.404, de 15 de dezembro de 1976**. Brasil, 2007

PRESIDÊNCIA DA REPÚBLICA, **Lei 8.987, de 13 de fevereiro de 1995**. Brasil, 2007

REUTERS – FISCOsoft. **Principais formas de auditoria - Roteiro de Procedimentos**, 2009.

Disponível em http://www.fiscosoft.com.br/main_online_frame.php?page=/index.php?PID=135525&key=2755688> Acesso em setembro de 2017.

SÁ, Antônio L. de. **Curso de Auditoria**, 10 Ed. São Paulo: Atlas, 2010. 568 p.

TUMA, Rogério Wagner. **Sobre o monopólio natural e o modelo competitivo no setor elétrico brasileiro**. Rio de Janeiro: IFE 1585, IE-UFRJ, 02 de junho de 2005;

WANDERLEY, Carlos Alexandre N.; DA FONSECA, Ana Carolina P. D.; DE PAULA, Helmut Alexandre. **Controles Internos No Setor Público À Luz Da Estrutura Do Coso: O Caso De Um Órgão De Compra Da Marinha Do Brasil**. ConTexto, v. 15, n. 30.

