CENTRO “PAULA SOUZA”
FACULDADE DE TECNOLOGIA DE AMERICANA “MINISTRO RALPH BIASI”
CURSO SUPERIOR DE TECNOLOGIA EM
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

RENATO PUNJILO

AS FUNÇÕES DA GOVERNANÇA CORPORATIVA E DA TECNOLOGIA DA INFORMAÇÃO NO PROCESSO DE ADEQUAÇÃO ÀS DIRETRIZES DA LEI SARBANES-OXLEY PARA AS EMPRESAS DE CAPITAL ABERTO: UMA ANÁLISE HISTÓRICO-BIBLIOGRÁFICA DESTES IMPLICANTES

AMERICANA,
2025

CENTRO “PAULA SOUZA”
FACULDADE DE TECNOLOGIA DE AMERICANA “MINISTRO RALPH BIASI”
CURSO SUPERIOR DE TECNOLOGIA EM
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

RENATO PUNJILO

AS FUNÇÕES DA GOVERNANÇA CORPORATIVA E DA TECNOLOGIA DA INFORMAÇÃO NO PROCESSO DE ADEQUAÇÃO ÀS DIRETRIZES DA LEI SARBANES-OXLEY PARA AS EMPRESAS DE CAPITAL ABERTO: UMA ANÁLISE HISTÓRICO-BIBLIOGRÁFICA DESTES IMPLICANTES

Trabalho de Graduação apresentado como requisito parcial para a obtenção do grau de Tecnólogo no Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, pela Faculdade de Tecnologia de Americana, sob a orientação metodológica do Prof. Me. Benedito Luciano Antunes de França.

AMERICANA,
2025

FICHA CATALOGRAFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

PUNJILO, Renato

As funções da Governança Corporativa e da Tecnologia da Informação no processo de adequação às diretrizes da Lei Sarbanes-Oxley para as empresas de capital aberto: uma análise histórico-bibliográfica destes implicantes. / Renato PUNJILO – Americana, 2025.

109f.

Monografia (Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Luciano Antunes de FRANÇA

1. Auditoria em sistemas de informação 2. Gestão de risco 3. Sistemas de informação - governança. I. PUNJILO, Renato II. FRANÇA, Benedito Luciano Antunes de III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.3
658.788.48
681.518.3

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Renato Punjilo

As Funções da Governança Corporativa e da Tecnologia da Informação no Processo de Adequação às Diretrizes da Lei Sarbanes-Oxley para as Empresas de Capital Aberto: Uma Análise Histórico-Bibliográfica destes Implicantes

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Análise e Desenvolvimento de Sistemas.

Americana, 2 de dezembro de 2025.

Banca Examinadora:

Benedito Luciano Antunes de França
Mestre
Fatec Americana "Ministro Ralph Biasi"

André de Lima
Doutor
Fatec Americana "Ministro Ralph Biasi"

Jonas Bodê
Mestre
Fatec Americana "Ministro Ralph Biasi"

Dedico o presente Trabalho de Graduação para a minha família, amigos e professores da Fatec Americana, especialmente ao mestre e professor Benedito França, por todo o incentivo, conselhos e suporte prestado.

RESUMO EM LÍNGUA VERNÁCULA

Este Trabalho de Graduação ressalta a relação e a importância da Tecnologia da Informação (TI) no apoio à Governança Corporativa e no atendimento às diretrizes e seções da Lei Sarbanes-Oxley (SOX), descrevendo, inicialmente, a definição destes dois temas, para, posteriormente, realizar o entendimento de como as operações, os departamentos e os *frameworks* de TI garantem a preservação da integridade das informações e subsidiam o suporte às operações das áreas de negócios das empresas, sobretudo às Sociedades Anônimas, ou seja, aquelas de capital aberto. Este Trabalho de Graduação reflete como a integridade dos dados tornou-se um fator fundamental para a tomada de decisões e, por conseguinte, para o sucesso operacional das empresas, cujos objetivos tornam-se possíveis na medida em que atendem às diretrizes expedidas pela SOX que, com a sua coletânea de diretrizes, estabelece responsabilidades e a gestão de boas práticas, que garantem a integridade das informações constantes nos relatórios financeiros e contábeis. Dessa forma, para que as empresas consigam atender à SOX, o departamento de Governança Corporativa, em conjunto com o departamento de Tecnologia da Informação, por meio do uso de *frameworks,* tais como COSO, COBIT e ITIL, são essenciais para o alcance destes objetivos. Por fim, este Trabalho de Graduação esclarece que a TI não é apenas um suporte operacional, mas sim um agente estratégico para o atendimento à SOX, por meio de uma boa estruturação, potencialmente possibilita às empresas mitigarem os riscos envolvidos com o advento de novas tecnologias e do fator humano, além de preservar a integridade e segurança de suas informações, além do bom relacionamento com os seus acionistas e as entidades governamentais.

PALAVRAS-CHAVE: Governança Corporativa; Lei Sarbanes-Oxley; Tecnologia da Informação; Governança de TI; Gerenciamento de Riscos.

ABSTRACT

This undergraduate thesis highlights the relationship and importance of Information Technology (IT) in supporting Corporate Governance and complying with the guidelines and sections of the Sarbanes-Oxley Act (SOX), initially describing the definition of these two themes, and subsequently understanding how IT operations, departments, and frameworks ensure the preservation of information integrity and support the operations of the business areas of companies, especially publicly traded companies. This thesis reflects how data integrity has become a fundamental factor for decision-making and, consequently, for the operational success of companies, whose objectives become possible insofar as they comply with the guidelines issued by SOX, which, with its collection of guidelines, establishes responsibilities and the management of best practices that guarantee the integrity of the information contained in financial and accounting reports. Thus, for companies to comply with SOX, the Corporate Governance department, together with the Information Technology department, through the use of frameworks such as COSO, COBIT, and ITIL, are essential to achieving these objectives. Finally, this thesis clarifies that IT is not only an operational support, but also a strategic agent for compliance with SOX, through good structuring, potentially enabling companies to mitigate the risks involved with the advent of new technologies and the human factor, in addition to preserving the integrity and security of their information, as well as maintaining good relationships with their shareholders and government entities.

KEYWORDS: Corporate Governance; Sarbanes-Oxley Act; Information Technology; IT Governance; Risk Management.

LISTA DE ILUSTRAÇÕES (FIGURAS)

LISTA DE ILUSTRAÇÕES (QUADROS)

SUMÁRIO

1 INTRODUÇÃO

Com o avanço da tecnologia em diversas áreas da sociedade, o uso da informação e dados se tornou fundamental na tomada de decisões. Neste sentido, as mais diferentes organizações, para garantirem o sucesso em suas operações comerciais, a preservação da integridade dos dados torna-se essencial, bem como o bom relacionamento destas com os seus acionistas, especialmente para àquelas empresas de capital aberto. Desta forma, com o objetivo de atenderem esta demanda específica, as empresas prescindem de uma importante coletânea de diretrizes, entre elas a Lei Sarbanes-Oxley (SOX), a qual, através de suas inúmeras seções, impõe responsabilidades e a execução de boas práticas no tocante à integridade das informações presentes nos relatórios financeiros e contábeis destas empresas.

Entretanto, para que as empresas consigam atender as exigências determinadas pela SOX, dois departamentos se fazem absolutamente necessários serem implantados: um relacionado à Governança Corporativa e o outro diretamente vinculado à Gestão da Tecnologia da Informação (TI), visto que estes departamentos serão responsáveis por todas as atividades relacionadas ao gerenciamento dos riscos das operações e pela implementação de controles internos no ambiente empresarial, especialmente nas áreas relacionadas aos negócios. Sendo assim, este Trabalho de Graduação possui como principal objetivo ressaltar a relação e a importância do departamento de TI com a Governança Corporativa no atendimento às exigências prescritas pela SOX, descrevendo, por exemplo, como as operações de TI, os departamentos e a adoção de *frameworks*, garantem a integridade das informações, além de subsidiar o suporte nas atividades de negócios.

A inspiração para o autor deste Trabalho de Graduação sobre este tema se deve ao fato de atuar no departamento de Governança Corporativa em uma Empresa multinacional, de capital aberto, mais especificamente na área de teste e de avaliação de riscos e controles internos de TI. Através das atividades realizadas diariamente no trabalho, além dos entendimentos aprimorados em salas de aulas do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas desta instituição universitária, foi observado a importância deste tema para os atuais e futuros ingressantes no mercado de trabalho de TI, pois ainda há muitas dúvidas sobre o

papel da SOX e, principalmente, como TI e Governança de TI são essenciais para o atendimento das diretrizes requeridas.

Fundamentado em pesquisa bibliográfico-documental, o repertório teórico-conceitual está assentado em diversas obras, artigos científicos, monografias, dissertações e tese de doutoramento de variados autores e autoras, nacionais e internacionais. Foram utilizados documentos publicados por entidades e organizações nacionais e internacionais relacionadas à Governança Corporativa e a Gestão da Tecnologia da Informação, além de vastos estudos disponibilizados por empresas do ramo de consultorias. Nesta perspectiva, este Trabalho de Graduação, inspirado nas disciplinas de “Gestão e Governança de TI” e “Auditoria de Sistemas”, alocadas no Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas da Fatec Americana – Ministro Ralph Biasi, foi dividido em seis seções, sendo que esta destina-se à Introdução, e a última, às Considerações finais.

A Segunda Seção deste Trabalho de Graduação visa descrever o conceito de Governança Corporativa e a sua respectiva importância para as empresas, além de especificar o processo de implementação de suas diretrizes e pilares. Destaca-se que, antes da assinatura da Lei Sarbanes-Oxley (SOX), as empresas já utilizavam e implementavam as diretrizes da Governança Corporativa. As bases de nossa análise técnica estão alicerçadas nos estudos publicados pelo Instituto Brasileiro de Governança Corporativa (IBGC) e nos artigos de diversos autores e autoras, entre estes, Fernanda Maciel Peixoto.

A Terceira Seção reporta os principais cenários e eventos de fraudes mundiais, que impuseram a necessidade da criação da SOX, como os casos da Enron e da WorldCom. Além disso, foram analisadas as diretrizes da SOX e a sua importância, destacando alguns artigos, como a seção 404. Nesta Seção reflete o impacto da SOX refletiu na estrutura da Governança Corporativa e como esta, hoje, deve ser implementa pelas empresas, especialmente às de capital aberto. O repertório teórico-conceitual assenta-se nas obras de Alexandre Di Miceli, José Mauricio dos Santos Pinheiro e nos estudos do IBGC e da Consultoria Deloitte Touche Tohmatsu, entre outros.

A Quarta Seção especificamente salienta como as empresas devem se adequar às diretrizes da seção 404 da SOX, a fim de que, por meio do *framework* do COSO, possa obter um gerenciamento adequado de riscos e um sistema eficiente de

controles internos. Esta Seção está amparada, entre outros, em Sebastião Bergamini Junior e Maria Cecilia da Silva Brum, além dos estudos publicados pelo IBGC, da IIA (The Institute of Internal Auditors) e das Consultorias Deloitte Touche Tohmatsu e KPMG.

Na Quinta Seção, foco principal deste Trabalho de Graduação, realiza-se uma análise da relação e importância da TI com as operações das áreas de negócios das empresas, compatibilizando as ações deste departamento com a Governança Corporativa, à luz das prescrições da SOX. Neste sentido, a Governança de TI, com a adoção de *frameworks* voltados à TI, como COBIT e ITIL, potencialmente garantirá o gerenciamento e a mitigação dos riscos de TI, bem como a criação e adequação dos controles internos de TI. As bases referenciais estão fundamentadas em variados autores, entre eles, a obra de Aguinaldo Aragon Fernandes e Vladimir Ferraz de Abreu e o artigo de José Mauricio dos Santos Pinheiro. Ademais, foram instrumentalizados estudos publicados pela The IIA, *IT Governance Institute* (ITGI), *Information Systems Audit and Control Association* (ISACA) e AXELOS.

2 GOVERNANÇA CORPORATIVA ANTES DA VIGÊNCIA DA LEI SARBANES-OXLEY (SOX)

Ao longo das últimas décadas, diversos estudos foram publicados debatendo sobre a definição da Governança Corporativa e a importância de sua aplicação nas organizações. Dessa forma, há variações em como definir a Governança Corporativa, fato este que se deve a diversos fatores, como o ano de publicação do estudo, país no qual o estudo foi realizado e o ambiente no qual o estudo foi focado (mercado acionista, imobiliário, etc.).

O Instituto Brasileiro de Governança Corporativa - IBGC (2023) define Governança Corporativa como:

> um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente (IBGC, 2023, p. 17).

Adriano Arrivabene, Renato José Sassi, Pamela Ferreira Alves Andrelo e Maria Luiza Almeida de Oliveira Moura no artigo "Análise do impacto da adequação nos processos operacionais de tecnologia da informação às exigências da lei Sarbanes-Oxley em empresa do ramo financeiro" afirmam que, tendo como parâmetro o pensamento de Andrade e Rossetti (2004),

> a Governança Corporativa busca, essencialmente, a perpetuação das organizações, ou seja, garantir que as organizações continuem ativas no mercado. Trata-se de práticas de gerenciamento que se estendem desde questões legais, como o direito dos investidores, questões financeiras que medem o retorno do investimento e a geração de valor, e avaliando até questões externas à organização, como questões ambientais (Resíduos da produção, efluentes químicos etc.) (Andrade; Rossetti, 2004 *Apud* Arrivabene; Sassi; Andrelo; Moura, 2021, p. 5)

Conforme Edson Labadessa, Alessandro Marco Rosini, Angelo Palmisano e Marcio Megera Conceição (2019), a Governança Corporativa é um instrumento de gestão e segurança para as empresas, pois assegura a segurança dos atos de gestão, do risco jurídico corporativo e da relação com os *stakeholders* (acionistas) (*Cf*. Labadessa; Rosini; Palmisano; Conceição, 2019, p. 5).

Ao pesquisar as definições de Governança Corporativa, conseguimos encontrar fatores em comum entre elas, alguns valores como a Integridade,

Transparência, Equidade, Responsabilização e Sustentabilidade. Esses fatores constituem os pilares da Governança Corporativa que, segundo o IBGC (2023), são definidas de acordo com o Quadro 1:

Quadro 1– Definição dos pilares da Governança Corporativa

Princípio	Definição
Integridade	Praticar e promover o contínuo aprimoramento da cultura ética na organização, evitando decisões sob a influência de conflitos de interesses, mantendo a coerência entre discurso e ação e preservando a lealdade à organização e o cuidado com suas partes interessadas, com a sociedade em geral e com o meio ambiente.
Transparência	Disponibilizar, para as partes interessadas, informações verdadeiras, tempestivas, coerentes, claras e relevantes, sejam elas positivas ou negativas, e não apenas aquelas exigidas por leis ou regulamentos. Essas informações não devem restringir-se ao desempenho econômico-financeiro, contemplando também os fatores ambiental, social e de governança. A promoção da transparência favorece o desenvolvimento dos negócios e estimula um ambiente de confiança para o relacionamento de todas as partes interessadas.
Equidade	Tratar todos os sócios e demais partes interessadas de maneira justa, levando em consideração seus direitos, deveres, necessidades, interesses e expectativas, como indivíduos ou coletivamente. A equidade pressupõe uma abordagem diferenciada conforme as relações e demandas de cada parte interessada com a organização, motivada pelo senso de justiça, respeito, diversidade, inclusão, pluralismo e igualdade de direitos e oportunidades.
Responsabilização	Desempenhar suas funções com diligência, independência e com vistas à geração de valor sustentável no longo prazo, assumindo a responsabilidade pelas consequências de seus atos e omissões. Além disso, prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, cientes de que suas decisões podem não apenas responsabilizá-los individualmente, como impactar a organização, suas partes interessadas e o meio ambiente.
Sustentabilidade	Zelar pela viabilidade econômico-financeira da organização, reduzir as externalidades negativas de seus negócios e operações, e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, natural, reputacional) no curto, médio e longo prazos. Nessa perspectiva, compreender que as organizações atuam em uma relação de interdependência com os ecossistemas social, econômico e ambiental, fortalecendo seu protagonismo e suas responsabilidades perante a sociedade.

Fonte: IBGC, 2023, p. 18-19

Conforme o IBGC, “os princípios aplicam-se a qualquer tipo de organização, independentemente de porte, natureza jurídica ou estrutura de capital, formando o alicerce sobre o qual se desenvolve a boa governança” (IBGC, 2023, p. 18).

Fundamentado na citação supracitada, pode-se considerar tais princípios como

universais para uma boa gestão em uma organização e um bom relacionamento com os seus *stakeholders*. Além disso, a organização não necessariamente precisa ser uma multinacional no ramo financeiro/contábil, pois tais princípios podem ser aplicados em diversos segmentos e categorias, desde empresas de pequeno porte, Microempreendedores individuais (MEI's) até Organizações não-governamentais (ONG's), pois de acordo com Dima Jamali; Asem M. Safieddine; Myriam Rabbath (2008), por meio da Governança Corporativa, as organizações são incentivadas a promover a ética, imparcialidade, prestação de contas, transparência e responsabilidade em todas as suas relações[1].

Nessa mesma linha de pensamento, Cristiane Braida Gelatti e Daniela Meneghetti, no Trabalho de Conclusão de Curso apresentado na Universidade Federal de Santa Maria, no Rio Grande do Sul (UFSM, RS), sob o título "Análise da adequação das empresas brasileiras à Lei Sarbanes-Oxley", apresentado em 2008, fundamentadas no pensamento Fernando Gentil Monteiro (2005), afirmam que

> as organizações que adotam boas práticas de Governança Corporativa tendem a ser mais valorizadas pelo mercado, uma vez que elas são transparentes nas suas relações comerciais, financeiras, societárias, sociais etc., pois prestam contas do que fazem a quem de direito e conferem equidade (igualdade) no tratamento de seus acionistas independentemente da sua classe ou categoria" (Monteiro, 2005 *Apud* Gelatti; Meneghetti, 2008, p. 21).

Kaarst-Brown e Kelly (2005, p. 1) acreditam que, através da Governança Corporativa, políticas de gestão e governabilidade são estabelecidas inclusive na área de Tecnologia da Informação (TI), a qual possui a função de facilitar as atividades desenvolvidas nas organizações, por meio de sua oferta de ferramentas de controle e gestão[2].

---

[1] This is where the concepts of CG and corporate social responsibility (CSR) enter the picture. Under the umbrella of CG, companies are encouraged to promote ethics, fairness, transparency, and accountability in all their dealings (Dima Jamali; Asem M. Safieddine; Myriam Rabbath. Corporate Governance and Corporate Social Responsibility Synergies and Interrelationships. **Journal compilation**, Vol. 16, n. 5, Sep. 2008, p. 444. *Tradução nossa!*)

[2] Recently, we are seeing IT vendors offering new "software tools" to help companies address the concerns of Sarbanes-Oxley. These solutions are being offered, however, before organizations fully understand the nature of the problems with their practices or what role information technology or the IT function may play in either the "problems" or the "solutions" resulting from SOX. Michelle L. Kaarst-Brown; Shirley Kelly. IT Governance and Sarbanes-Oxley: The Latest Sales Pitch or Real Challenges for the IT Function? PROCEEDINGS OF THE 38TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 2005, Vol. 9, p. 1.

Com a definição de Governança Corporativa esclarecida, nota-se o quão ela é importante para as organizações no mercado atualmente. Entretanto, ainda fica algumas dúvidas pendentes, tais como: Quando ela foi estabelecida? Quais motivos que impulsionaram a sua criação? Como a Governança Corporativa é estruturada? Essas dúvidas, entre outras, serão esclarecidas ao longo deste Trabalho de Graduação.

Entretanto, é importante destacar um marco significativo para a Governança Corporativa que se deu com a assinatura da Lei Sarbanes-Oxley (SOX) em 30 de julho de 2002, promulgada pelo congresso dos EUA e sancionada pelo presidente George W. Bush. A Governança Corporativa foi atualizada e teve a sua devida importância reconhecida pelas organizações após a implementação dessa lei.

Segundo Lima, Maciel e Libonati (2008), a Lei SOX representa a mais importante reforma da legislação do mercado de capitais desde a introdução de sua regulamentação, na década de 1930:

> A lei Sarbanes-Oxley, como foi chamada, foi apelidada de Sarbox ou ainda de SOX. Esta lei se configura na mais importante reforma da legislação de mercado de capitais desde a introdução de sua regulamentação na década de 30, após a quebra da bolsa de Nova York em 1929 (Lima; Maciel; Libonati, 2008, p. 6).

Porém, antes de entrarmos em mais detalhes sobre essa lei, uma dúvida emerge de como era tratada a Governança Corporativa antes da implementação da SOX? Esse ponto de reflexão foi promovido por Fernanda Maciel Peixoto (2012):

> O início dos estudos sobre governança corporativa está relacionado à separação entre propriedade e gestão, apresentada, inicialmente, por Adam Smith, em 1776, e discutida por Berle e Means na obra The modern corporation and private property, de 1932 (Peixoto, 2012, p. 25).

Dessa forma, podemos compreender que as ideias e princípios da Governança Corporativa já eram discutidos há muito tempo. Na mesma linha de raciocínio, Fernanda Maciel Peixoto, em sua Tese de Doutoramento, sob o título "Governança corporativa, desempenho, valor e risco: estudo das mudanças em momentos de crise", apresentada na Universidade Federal de Minas Gerais, em 2012, recorre a Adolf Berle e Gardiner Means (1932), pois tratam de questões muito relevantes para o mundo empresarial, como:

> separação entre a propriedade e o controle das grandes corporações; transferência da direção das empresas dos proprietários para os gestores; divergências de interesses entre eles; e a nova configuração

> do controle nas sociedades abertas, por vezes, incompatível com o objetivo de maximização da riqueza dos proprietários (Berle; Means, 1932 *Apud* Peixoto, 2012, p. 25).

De acordo com Peixoto, os pensadores Michael Jensen e William H. Meckling (1976) alertaram para um dos maiores desafios a ser enfrentado pelas empresas, “a separação entre propriedade e gestão, resultando no chamado conflito de agência” (Jensen; Meckling, 1976 *Apud* Peixoto, 2012, p. 25), visto que, esta não separação promoveria uma espécie de oportunismo dos gestores, como a autopromoção com remunerações e benefícios, concentração de poder de voto e controle do fluxo de caixa, para evitar tais práticas o Instituto Brasileiro de Governança Corporativa determina a criação de um conjunto de normas e processos que promovam a transparência, a prestação de contas, a equidade e a responsabilidade corporativa (IBGC, 2023).

Nessa linha de raciocínio, Karla Jeanny Falcão Carioca, Márcia Martins Mendes de Luca e Vera Maria Rodrigues Ponte (2010) acreditam que “o conflito principal ocorre porque as pessoas possuem interesses diferentes e buscam a maximização dos próprios interesses, em detrimento das necessidades dos demais” (Carioca; Luca; Ponte, 2010, p. 52). Para evitar esta situação de oportunismo por parte da equipe gestora, estas autoras recomendam a adoção de boas práticas de governança:

> a fim de solucionar o conflito existente entre o principal e o agente, como forma de proteger os interesses dos acionistas por meio de mecanismos que garantam o comportamento dos gestores alinhado com a necessidade dos acionistas. Apesar de ser um termo de surgimento relativamente recente, a governança corporativa possui forte presença no meio corporativo atual (Carioca; Luca; Ponte, 2010, p. 52).

Após a 2ª Guerra Mundial, Peixoto (2012) informa que a obra “Theory of the firm: managerial behavior, agency costs and capital structure”, de Jensen e Meckling (1976), pode ser considerada um dos mais relevantes estudos precursores da Governança Corporativa (*Cf*. Peixoto, 2012, p. 27). Peixoto complementa, informando que “este estudo aborda a teoria da agência, a teoria dos direitos de propriedade e a teoria de finanças, com o objetivo de estabelecer os alicerces teóricos da estrutura de propriedade das empresas” (Peixoto, 2012, p. 27).

Dessa forma, as primeiras bases para o estabelecimento da Governança Corporativa foram surgindo. Conforme Fiorini, Alonso Junior e Alonso (2016), em 1980

surgiu nos EUA o movimento em torno das melhores práticas de governança corporativa. Devido ao controle acionário descentralizado, os principais executivos das organizações começaram a desfrutar de enorme poder de decisão, gerando grande insatisfação entre os investidores, particularmente nos fundos de pensão (*Cf*. Fiorini; Alonso Junior; Alonso, 2016, p. 11-12).

Segundo retratam no artigo “Governança corporativa: conceitos e aplicações”, de Filipe Antônio Fiorini, Nelson Alonso Junior e Vera Lucia Chaves Alonso, o fundo de pensão Calpers (California Public Employees Retirement System) em conjunto com outros acionistas, fundou o Conselho de Investidores Institucionais (CII – Council of Institutional Investors), no qual buscava cuidar dos interesses dos investidores institucionais, tendo em vista o fatídico episódio ocorrido pelos executivos da Texaco, nos Estados Unidos:

> Segundo Carlsson apud Silveira (2010), “o estopim para o movimento pró-governança foi a tentativa de aquisição do controle da Texaco em 1984 pela Chevron, inviabilizada em função de diversas tentativas defensivas empregadas pelos executivos da Texaco em prejuízo aos acionistas”. Após este acontecimento, o fundo de pensão Calpers (California Public Employees Retirement System), um dos principais acionistas da Texaco, definiu que, como investidores de longo prazo, não aceitariam comportamento similar de outras empresas investidas. Assim, passaram a atuar de forma mais ativa junto aos executivos.
> Em 1985 a Calpers atuou para criação do Conselho de Investidores Institucionais (CII – Council of Institutional Investors), com objetivos bem definidos, mas que basicamente visava cuidar dos interesses dos investidores institucionais. O fundo de pensão também passou a monitorar as práticas de governança corporativa nas empresas e passou a publicar na mídia as que apresentavam algum problema. Em pesquisa realizada em 1994 com mais de 300 empresas dos Estados Unidos, o fundo de pensão Calpers constatou que mais da metade das companhias pesquisadas já possuíam, ou estavam desenvolvendo, suas próprias diretrizes de governança corporativa (Fiorini; Alonso Junior; Alonso, 2016, p. 12).

No Brasil, Álvaro Ricardino e Sofie Tortelboom Aversari Martins (2004) observaram que algumas ideias subjacentes à governança corporativa têm origem bem mais antiga. Os autores relatam a elaboração de um estatuto de uma companhia de comércio, em 1754, no qual o documento relata como se deu a constituição da primeira sociedade por ações brasileira, a qual se iniciou com atividades de transporte e comércio de escravos e, foi assim denominada, pois foi financiada através de recursos de militares, comerciantes e habitantes da região (*Cf*. Ricardino; Martins, 2004, p. 51-53). O estatuto desta companhia contém trechos que se assemelham aos modernos Códigos de Boas Práticas de Governança publicados pelo Instituto

Brasileiro de Governança Corporativa (IBGC), no qual são amplamente utilizados atualmente.

Ainda analisando o mercado brasileiro, Oliveira e Linhares (2007) informam o seguinte fato:

> Mesmo antes do surgimento da Lei Sarbanes-Oxley, o Brasil já dava seus primeiros passos rumo às boas práticas de governança corporativa: (1) em 1995, surgiu o Instituto Brasileiro de Governança Corporativa - IBGC; (2) em dezembro de 2000, foi lançado o Novo Mercado da Bolsa de Valores do Estado de São Paulo - BOVESPA; (3) em 2001, a Lei n.º 10.303 alterou a Lei das Sociedades por Ações - 6.404/76; e (4) em 2002, a Comissão de Valores Mobiliários - CVM criou a sua Cartilha de Governança Corporativa (Oliveira; Linhares, 2007, p. 161).

Entre outros fatores e eventos que enfatizaram a necessidade da Governança Corporativa no mercado global foram destacados pelos pensadores Alexandre Di Miceli da Silveira na obra "Governança corporativa no Brasil e no mundo: Teoria e prática", publicada pela editora Elsevier, em 2010, e por Marco Becht, Patrick Bolton e Alisa Röell na obra “Corporate Governance and Control” (2002). Nas respectivas obras, eles destacam, especialmente, cinco fatores: crescimento e maior ativismo dos investidores institucionais; onda de aquisições hostis nos Estados Unidos nos anos 1980; onda de privatizações nos países europeus e em desenvolvimento; desregulamentação e integração global dos mercados de capitais; crises nos mercados emergentes no final do século XX.

A fim de compreendê-los, no Quadro 2 encontram-se as informações adaptadas:

Quadro 2 – Fenômenos globais relacionados a Governança Corporativa

Fenômenos globais	Impactos
Crescimento e maior ativismo dos investidores institucionais	A partir da década de 1980, os investidores institucionais cresceram significativamente e passaram de uma postura passiva, no qual vendiam ações quando discordavam, para uma atuação ativa na governança das empresas, influenciando decisões por meio de participação em assembleias, eleição de conselheiros e definição de regras de governança.
Onda de aquisições hostis nos Estados Unidos nos anos 1980	A onda de aquisições hostis no mercado norte-americano levou as empresas a adotarem mecanismos defensivos, como as "pílulas envenenadas", para evitar tomadas de controle. Essa reação impulsionou o ativismo dos investidores institucionais e intensificou os debates sobre governança corporativa.
Onda de privatizações nos países europeus e em desenvolvimento	A partir de 1980, a onda de privatizações iniciada no Reino Unido se espalhou por diversos países, especialmente na década de 1990. Esse movimento levantou debates sobre controle e gestão das novas empresas e ampliou a importância dos mercados de capitais.
Desregulamentação e integração global dos mercados de capitais	A partir de 1990, a desregulamentação e a integração global dos mercados de capitais impulsionaram debates sobre governança corporativa. A prática da listagem dupla permitiu que empresas negociassem ações em bolsas estrangeiras, promovendo novas práticas de governança corporativa e expandindo a cultura do mercado de ações para outros países.
Crises nos mercados emergentes no final do século XX	As crises nos mercados emergentes no final do século XX, revelaram falhas na governança empresarial e na proteção aos investidores. Organismos internacionais passaram a priorizar reformas de governança corporativa nesses países como forma de prevenir novas crises.

Fonte: Adaptado de Silveira (*Cf.* 2010, p. 4-5) e Becht; Bolton; Röell (*Cf.* 2002, p. 10-14)

Por fim, Evelyze Cruz Dallagnol, Henrique Adriano de Sousa, Gabriela de Abreu Passos, Joacir Celso Duarte Junior e Mayla Cristina Costa no artigo "Os princípios da Governança Corporativa: o enfoque dado pelas Empresas Listas na B3", publicado no XVI Congresso USP de Iniciação Científica em Contabilidade, em 2019, afirmam, com base em Djalma de Pinho Rebouças de Oliveira, autor da obra “Governança corporativa na prática: integrando acionistas, conselho de administração e diretoria executiva na geração de resultados: conceitos, estruturação, atuação, prática”, publicada pela Editora Atlas, em 2006, que, em 1992, surge o Relatório

Cadbury (1992), coordenado por Adrian Cadbury, no qual se tornaria uma das principais inspirações para os pilares da Lei Sarbanes-Oxley (SOX):

> Foi desenvolvido uma estrutura de administração participativa, registrada em um código que está focado em três princípios básicos: constituição e estruturação do conselho de administração; estruturação e separação das responsabilidades do conselho de administração e da diretoria executiva; e a alocação da administração geral da empresa pelas diretrizes básicas no conselho de administração (Oliveira, 2006 *Apud* Dallagnol; Sousa; Passos; Duarte Junior; Costa, 2019, p. 2).

Para Peixoto (2012), o Relatório Cadbury constitui um "(...) marco da governança corporativa no contexto internacional. Consiste em um código de boas práticas de governança, que surgiu em resposta a escândalos ocorridos nos mercados empresarial e financeiro da Inglaterra ao final da década de 1980" (Peixoto, 2012, p. 28).

Peixoto (2012) declara:

> Esse relatório aborda diversos assuntos, quais sejam: razões para constituir comitês de auditoria e de remuneração, treinamento de diretores, padrões de conduta para conselheiros e diretores, substituição periódica de auditores, controle interno, prestação de contas de conselhos para acionistas, formas eficazes de comunicação com acionistas, dentre outros (Peixoto, 2012, p. 29).

Pode-se observar que mesmo antes da SOX ser criada e das definições de Governança Corporativa serem plenamente estabelecidas, já se pressupunham mecanismos e estudos sobre a temática. Mesmo com as desavenças entre os executivos das organizações e seus acionistas/investidores, a confiança nas organizações e os seus resultados contábeis ainda era muito alta.

Fiorini, Alonso Junior e Alonso ressaltam essa confiança:

"Assim, na década de 1980 o mercado norte-americano foi marcado por um histórico de confiança excessiva dos investidores. Afinal, estavam no mercado mais forte do mundo e que apresentava forte proteção legal" (Fiorini; Alonso Junior; Alonso, 2016, p. 12).

Entretanto, tal confiança foi extremamente abalada em função dos episódios descritos. Na próxima seção, refletir-se-á que, mesmo com a crescente preocupação e importância relacionada a Governança Corporativa, houve ocorrências e escândalos fiscais, que mudaram e impactaram o mercado mundial, assim estabelecendo a necessidade da promulgação da lei Sarbanes-Oxley (SOX).

3 O IMPACTO DA LEI SARBANES-OXLEY (SOX) NA GOVERNANÇA CORPORATIVA: CENÁRIO INTERNACIONAL QUE JUSTIFICOU A CRIAÇÃO DA SOX

Antes de ser apresentado quais foram os principais fatores e eventos que justificaram a criação da Lei Sarbanes-Oxley (SOX), é necessário deixar claro o motivo que leva as organizações e seus executivos a cometerem atos de fraudes e de corrupção.

Conforme Renato Almeida dos Santos, Arnoldo José de Hoyos Guevara, Maria Cristina Sanches Amorim e Ben-Hur Ferraz-Neto (2012):

> (...) a corrupção, em suas várias formas, provoca prejuízos financeiros imediatos, destrói a imagem e a reputação das organizações, estraga o ambiente de trabalho, esgarça a sociedade, aumenta os custos de investimento, e alimenta condutas nocivas para o desenvolvimento econômico e social (Santos; Guevara; Amorim; Ferraz-Neto, 2012, p. 2).

Marcelle Colares Oliveira e Juliana Silva Linhares (2007) no artigo “A implantação de controle interno adequado às exigências da lei Sarbanes-Oxley em empresas brasileiras: um estudo de caso” citam Andrade (1999), que afirmar que a fraude pode ser caracterizada como o resultado de irregularidades e de atos ilegais praticados na organização, que, de forma deliberada, manifesta a intenção do autor em causar tal infração. Andrade citado por Oliveira e Linhares apresenta alguns exemplos de fraudes, dentre eles a “omissão e manipulação de documentos, informações, valores e bens; adulteração de documentos, registros, demonstrações contábeis e informações” (Andrade, 1999, p. 131, *Apud* Oliveira; Linhares, 2007, p.164).

Partindo da mesma ideia, Peter Rodriguez, Donald Siegel, Amy Hillman e Lorraine Eden (2006) insinuam que a corrupção no setor privado é caracterizada pelo abuso de autoridade na obtenção de benefício privado[3].

Nesse mesmo sentido, Norman David Bishara (2010) assegura que a corrupção no setor privado ocorre principalmente em mercados emergentes, em que

[3] “Corruption is most commonly defined as the misuse of public power for private gain” (Peter Rodriguez; Donald S. Siegel; Amy Hillman; Larraine Eden. **Three Lenses on the Multinational Enterprise**: Politics, Corruption and Corporate Social Responsibility. 2006, p. 8. (*Tradução nossa*!)

as organizações com Governança Corporativa menos desenvolvidas são mais suscetíveis à exploração por indivíduos corruptos[4].

Adriano Arrivabene (2012) destaca que o relacionamento entre investidor e organização é mantido em uma linha extremamente tênue:

> O grau de confiança dos investidores é sentido a cada momento do dia, durante as atividades das bolsas de valores, onde são comercializadas as ações das empresas de capitais abertos. Essa dinâmica comercialização reflete, a cada momento, essa situação de instabilidade financeira.
>
> O relacionamento entre investidor e empresa é mantido em uma linha extremamente sensível de situação, momentânea. Os investidores analisam o mercado e confiam nas informações que recebem das empresas onde mantêm seus capitais investidos e, mediante todos os cenários recebidos, analisam e direcionam seus capitais (Arrivabene, 2012, p. 2).

Dessa forma, veremos a seguir alguns dos principais exemplos de casos em que foram identificadas fraudes contábeis, motivadas pela busca do autobenefício dos executivos, seja monetário ou em prol da consolidação de poder, e pelo excesso de confiança em seus atos.

Um dos principais casos de corrupção/fraude contábil da atualidade foi o Caso Enron.

Para Sebastião Bergamini Junior (2005), este caso foi um dos mais emblemáticos da história, pois, até 2001, foi considerado um dos maiores processos de falência do mundo:

> O caso Enron é emblemático por vários motivos: foi, até a quebra da WorldCom ocorrida alguns meses depois, o maior processo de falência do mundo, envolvendo ativos de US$ 63 bilhões e perdas no valor das ações de US$ 32 bilhões; resultou de uma gestão temerária, caracterizada pelos elevados riscos assumidos pela diretoria, num movimento para otimizar o valor de suas opções de ações recebidas em bonificação por desempenho (stock options); evidenciou sérios problemas de conflito de interesses com a Andersen, auditores independentes que também prestavam consultoria à empresa; levantou a questão, sempre presente no meio contábil, sobre o dilema de adotar um sistema de regras contábeis abrangentes baseadas em

[4] "For purposes of this paper the concept of corruption is defined broadly and covers unethical rent-seeking behavior beyond traditional coarse corruption (i.e., bribery), including actions such as fraud, the abuse of majority shareholder power over other shareholders, or the misuse of business assets. Corruption is generally seen as harmful and, accordingly, scholars agree that corruption decreases investment in emerging economies" (Norman David Bishara. Governance and Corruption Constraints: The Business Ethics Glass Ceiling in Middle East Corporate Governance. **Michigan Ross School of Business Paper**, n. 1143, 2010, p. 9.

> princípios ou sistemas de regras claras e inequívocas; e constituiu o primeiro dos grandes processos de falência que resultaram na quebra de confiança dos investidores e em maior rigidez do ordenamento legal (Bergamini Junior, 2005, p. 171).

Diversos autores ao longo da história consentem com o pensamento de Bergamini Junior; entre eles Alexandre Di Miceli Silveira (2010, p. 346) cita que “a Enron é um dos casos mais emblemáticos de fracassos empresariais associados a problemas de governança corporativa”.

Marisa Silva de Oliveira e Denise Gomes Barros Cintra, no artigo “Os impactos da lei Sarbanes Oxley no mercado de capitais e na auditoria externa”, afirmam que “Segundo Schmitt (2002) a falência da Enron abalou o mercado americano expressamente superior à queda das torres gêmeas” (Schimitt, 2002, p. 2, *Apud* Oliveira; Cintra, 2019, p. 6).

Conforme Alexandre Di Micela Silveira (2010, p. 347), a empresa foi fundada em julho de 1985 e ao longo dos anos acumulou muito poder e influência política, chegando a ser a sétima maior empresa norte-americana por receita em 2001, ano em que foi à falência após a divulgação de uma série de fraudes contábeis.

Além disso, Pietro Vinicius Bonotto (2010), endossa que a Enron era uma das maiores companhias do setor de energia mundial e, posteriormente a 1999: “(...) Apresentou crescimento estrondoso desde onde atuou, nos ramos de energia, água, carvão, celulose, papel, plásticos, metais, internet e hedges de transações financeiras de compra e venda” (Bonotto, 2010, p. 11).

Conforme apresentamos, até meados de 2001, a Enron era considerada uma das maiores empresas não só nos Estados Unidos, mas mundialmente. Entretanto, como uma empresa com tanto prestígio e poder decretou a falência alguns meses depois?

A resposta para esta pergunta está fundamentada na obra de Marisa Silva de Oliveira e Denise Gomes Barros Cintra (2019):

> Basicamente a Enron manipulou empresas controladas e coligadas para aumentar seu resultado, uma atividade comum nas organizações. Por meio das Special Purposal Entities (SPE’s), a organização disfarçava as despesas, modificava passivos, alavancava empréstimos, securitizações, leasings e operações arriscadas com derivativos, e também fez uso da legislação para ocultar seu resultado, cometendo manobras contábeis e falta de transparência (Oliveira; Cintra, 2019, p. 5).

Conforme Alexandre Di Miceli Silveira, a queda da Enron não foi repentina. Este autor demonstra que a derrocada se deu a partir de março de 2001, quando a jornalista Bethany McLean publica um artigo para a Revista Fortune, por meio do qual levanta dúvidas sobre a qualidade técnica dos resultados financeiros obtidos pela Enron (*Cf*. Silveira, 2010, p. 348). Alguns meses depois, em 12 de outubro de 2001, David Duncan, um sócio da Arthur Andersen, organiza uma força tarefa de duas semanas para destruição de documentos classificados como “desnecessários” da Enron (*Cf*. Silveira, 2010, p. 348). Estes documentos estavam diretamente relacionados às auditorias empreendidas na companhia ao longo dos anos, o que pode ser caracterizado como uma espécie de queima de arquivos.

Na linha cronológica proposta por Alexandre Di Miceli Silveira, em 16 de outubro de 2001, a “Enron reporta seu primeiro trimestre de prejuízo em mais de cinco anos” (Silveira, 2010, p. 348). Já, em 8 de novembro do mesmo ano, a Enron republica suas demonstrações financeiras dos últimos quatro anos, porém, “com uma baixa contábil de US$ 1,2 bilhão no patrimônio líquido em função de dívidas ocultas em Sociedades de Propósito Específico (SPEs) da companhia” (Silveira, 2010, p. 348). Posteriormente, segundo Silveira, “descobre-se que as dívidas e passivos fora do balanço da organização totalizavam cerca de US$ 25 bilhões” (Silveira, 2010, p. 348). A situação descrita por Silveira fez a Enron perder a confiança dos acionistas e investidores, conduzindo a organização empresarial a declarar falência em 02 de dezembro de 2001: “A Enron perde a confiança do mercado e vai à falência. As ações, que chegaram a US$ 90 no ano anterior, caem para 30 centavos de dólar” (Silveira, 2010, p. 349).

Os prejuízos foram imensos, conforme Alexandre Di Miceli Silveira: o diretor financeiro Andrew Fastow foi condenado a dez anos de prisão e a pagar US$ 24 milhões, o chefe de contabilidade Richard Causey, após a realização de um acordo judicial, foi condenado a 6 anos de prisão em 2005. O CEO da Enron, Jeffrey Skilling recebeu pena de 24 anos de prisão em outubro de 2006 e multa de US$ 45 milhões (*Cf.* Silveira, 2010, p. 357). Enfim, Silveira salienta que houve acordos e julgamentos envolvendo os conselheiros independentes da organização, tais como membros de consultoria e bancos de investimentos, os quais estavam envolvidos com o esquema de corrupção na Enron (*Cf*. Silveira, 2010, p. 358).

Este caso abalou as estruturas do mercado acionário dos Estados Unidos. Entretanto, alguns meses depois emerge o caso envolvendo a organização WorldCom, que superaria o fatídico evento da Enron, e passa a ser classificado como o maior processo de falência até o momento (Bergamini Junior, 2005, p. 171).

Segundo Filipe Antônio Fiorini, Nelson Alonso Junior e Vera Lucia Chaves Alonso,

> a WorldCom era uma gigante do setor de telecomunicações, segunda maior operadora americana de telecomunicações a longa distância e a primeira operadora mundial em serviços de internet, sendo considerada no final dos anos 90 uma empresa símbolo da euforia americana (Fiorini; Alonso Junior; Alonso, 2016, p. 9).

Pietro Vinicius Bonotto ao citar E. S. Browning, autor do artigo “Is the praise for WorldCom too Much?”, publicado no “The Wall Street Journal” (1997), detalha que:

> Em 1997, uma ação da WorldCom iniciou o ano cotada na bolsa de valores de Wall Street a meros centavos de dólar e ao término do mesmo ano acabou chegando ao valor de 60 dólares por ação. Neste momento, os analistas da bolsa notaram a presença da Companhia e do seu visionário CEO, Bernie Ebbers, fazendo com que bancos de investimentos, analistas e corretores fizessem fortes recomendações aos investidores. Com o aumento da cotação das ações da WorldCom, tornara-se fácil a utilização destas nas aquisições de outras companhias (Browning, 1997, *Apud* Bonotto, 2010, p. 6).

Dessa forma, ao longo dos anos a WorldCom foi ganhando relevância no mercado americano e consequentemente as expectativas e a pressão por bons resultados da organização foram aumentando.

Conforme José Carlos de Souza e Jorge Eduardo Scarpin (2006), para conseguir manter bons resultados perante os acionistas, a organização efetuava a ativação indevida de gastos, conforme ilustram no Quadro 4 do artigo “Fraudes contábeis: as respostas da Contabilidade nos Estados Unidos e na Europa”:

> A empresa colocou no balanço 3,8 bilhões de dólares como investimentos, quando na verdade eram despesas. A compra de bens duráveis, que trarão retorno direto, pode ser depreciada no balanço em um período longo. Os gastos do dia a dia, por outro lado, devem ser reconhecidos como despesa imediatamente (Souza; Scarpin, 2006, p. 8).

Vania Maria da Costa Borgerth (2005) cita o seguinte entendimento:

> Durante os cinco anos que antecederam sua falência, a empresa havia crescido intensamente, a partir de fusões e aquisições, usando bilhões

> de dólares de suas próprias ações e dívidas de US$ 25 bilhões como mecanismo de financiamento deste crescimento. Para forjar estas fontes, a Worldcom manipulou suas demonstrações contábeis no período de 1999 a 2002, dando origem ao maior caso se fraude contábil da história americana (Borgerth, 2005, p. 35).

No mesmo estudo, Vania Maria da Costa Borgerth (2005) conclui que:

> O relator do processo contra os executivos da empresa atestou que as práticas adotadas pela WorldCom tinham na simplicidade o seu toque de gênio e poderiam ter sido facilmente descobertas se os agentes que deveriam ter atuado como fiscalizadores : auditores (Arthur Andersen), bancos subscritores (Salomon Brothers, JP Morgan, Bank if América, Deutsche Bank, Chase Securities, etc.), analistas independentes, advogados e executivos da empresa, não tivessem desviado o olhar a fim de preservar a oportunidade de um bom negócio (Borgerth, 2005, p. 35).

Acusada de fraude pela SEC (United States Securities and Exchange Commission) em 27 de junho de 2002:

> A WorldCom perdeu US$ 100 bilhões de valor de mercado entre 25 de junho e 1o de agosto. A constatação de que os executivos da empresa haviam ganhado US$ 140 milhões em salários, bônus e lucros na venda de ações ao mesmo tempo em que cometiam fraudes contábeis para apresentar lucros inexistentes, lesando o público investidor, causou grande indignação pública e contribuiu para a rápida tramitação da Lei Oxley-Sarbanes, promulgada em 30 de julho (Bergamini Junior, 2002, p. 78).

Em 9 de agosto de 2002, foram divulgados novos erros encontrados pelos auditores externos nas “demonstrações contábeis relativas a 1999 e 2000, representados por US$ 3,3 bilhões de provisões e maus empréstimos lançados como lucro operacional, ampliando para US$ 7,2 bilhões o valor dos prejuízos” (Bergamini Junior (2002, p. 78). Sobre este assunto, Adam J. Berger, em artigo intitulado “WorldCom scandal”, publicado no Portal da EBSCO Information Services, em 2022, acrescenta que ao longo dos anos “o valor total dos prejuízos atingiu a marca de aproximadamente US$ 11 bilhões”[5] (*Cf.* Berger, 2022).

Conforme Sebastião Bergamini Junior (2002, p. 78), o diretor financeiro Scott Sullivan e o vice-presidente David Myers entregaram-se às autoridades em 01 de agosto de 2002, sendo liberados após pagarem fianças de US$ 10 milhões e US$ 2 milhões, respectivamente.

---

[5] “The WorldCom scandal is one of the most significant accounting frauds in United States history, involving the misstatement of approximately $11 billion in earnings”. Adam J. Berger. WorldCom scandal. 2022. *In*.: **EBSCO Information Services**, 2025

Vania Maria da Costa Borgerth (2005, p. 38) informa que Bernand Ebbers (CEO) foi condenado a 25 anos de prisão em 14 de julho de 2005, além de ser obrigado a deixar a disposição da justiça a sua fortuna pessoal, para a indenização posterior dos acionistas prejudicados em função da bancarrota da empresa.

O caso WorldCom impactou e surpreendeu o mercado mundial da mesma maneira que o escândalo ocorrido Enron, meses anteriores. Sendo assim, a confiança dos investidores não apenas no mercado em si, mas nas próprias organizações empresariais estava fragilizada.

Conforme Adriano Arrivabene (2012, p. 3), esse abalo no mercado financeiro colocou em xeque a Governança Corporativa e a Governança de Tecnologia da Informação das empresas, em face à clara exposição de vulnerabilidade na segurança das informações destas organizações.

Dessa maneira, em um intervalo de quase 2 anos, os Estados Unidos e o mercado acionário viram dois dos maiores escândalos fiscais/contábeis acontecerem sequencialmente. Em função disso, o governo e mercado americano/mundial se viu diante das seguintes questões: Como podemos recuperar a confiança dos investidores? Como podemos evitar que tais situações ocorram novamente?

3.1. Diretrizes e normatizações estabelecidas pela SOX

No artigo denominado “Análise do impacto da adequação nos processos operacionais de tecnologia da informação às exigências da lei Sarbanes-Oxley em empresa do ramo financeiro”, publicado por Adriano Arrivabene, Renato José Sassi, Pamela Ferreira Alves Andrelo e Maria Luiza Almeida de Oliveira Moura informam que as respostas para as perguntas supracitadas foram dadas em 30 de julho de 2002, com a sanção da Lei Sarbanes-Oxley (SOX), nome advindo da junção dos sobrenomes de seus criadores, os senadores norte-americanos Paul Spyros Sarbanes e Michael Garver Oxley (*Cf*. Arrivabene; Sassi; Andrelo; Moura; 2021, p. 5).

Segundo Vania Maria da Costa Borgerth (2007), citada por Arrivabene, Sassi; Andrelo e Moura,

> a lei busca a eficiência das informações no mercado de capitais, uma vez que os investidores utilizam estas informações para direcionar suas atividades, facilitando assim a análise do risco que estarão assumindo e avaliando qual a sua chance de retorno (Borgerth, 2007, *Apud* Arrivabene; Sassi; Andrelo; Moura; 2021, p. 5).

Nesse sentido, de acordo com os autores citados, a lei é uma espécie de organismo regulador das empresas, a fim de garantir a “integridade das informações e a responsabilidade penal da alta administração sobre elas” (Arrivabene; Sassi; Andrelo; Moura, 2021, p. 5).

De acordo com Alexandre Di Miceli Silveira (2010), a Lei Sarbanes-Oxley “(...) foi a mais importante mudança legal para as companhias norte-americanas desde a promulgação no país das leis básicas sobre valores mobiliários em 1933 e 1934” (Silveira, 2010, p. 93).

Por outro lado, Fiorini, Alonso Junior e Alonso (2016) citam que a SOX foi uma resposta legislativa para a intervenção estatal no mercado, mas que teve por objetivo restaurar a confiança perdida pelos investidores, sob o intuito de evitar que a crise atingisse proporções ainda maiores:

> A introdução desta lei estabeleceu, entre outras coisas, novos padrões de divulgação de informações, novas responsabilidades aos principais executivos da empresa, além da implantação de critérios mais rígidos de fiscalização dos procedimentos contábeis (Fiorini, Alonso Junior e Alonso, 2016, p. 9).

Com o advento da SOX, diz José Maurício dos Santos Pinheiro:

> Com a lei, rígidos parâmetros legais foram impostos às companhias de capital aberto e suas respectivas subsidiárias, cujas ações são negociadas em Bolsas (NYSE e Nasdaq), o que inclui também algumas corporações estrangeiras que negociam ADR’s (American Depositary Receipts – recibos de depósito americano de ações de empresas estrangeiras) não negociáveis no país de origem. No Brasil, essa lei se aplica às empresas com ações negociadas nos mercados de capitais dos Estados Unidos, ou seja, multinacionais de capital americano e empresas brasileiras com ações naquele país. No entanto, as responsabilidades criadas pela lei são de interesse de todas as empresas que queiram se atualizar sobre práticas de gestão de riscos, que estão entrando em vigor nos Estados Unidos e que, em curto prazo, terão ressonância mundial (Pinheiro, 2006, p. 3).

A SOX se tornou uma obrigatoriedade para as organizações/empresas com capital aberto; no entanto, para as empresas com capital privado, tal obrigação não se aplica, mas é recomendável, conforme recomenda uma das maiores consultorias mundiais relacionadas a SOX, a consultoria Deloitte Touche Tohmatsu, de acordo com o documento “Lei Sarbanes-Oxley: guia para melhorar a governa corporativa através de eficazes controles internos” (2003):

> (...) Para uma companhia de capital aberto, a obediência à essa Lei não é negociável. Para os Comitês de Auditoria e para a Alta Administração de companhias de capital aberto, particularmente

> Diretores Executivos e Diretores Financeiros, as definições de administradores financeiros e responsabilidade pessoal tornaram-se mais explícitas e os riscos significativamente mais altos. (...) Companhias de direito privado, embora não obrigadas legalmente a cumprir a nova Lei, também podem optar pela adoção de determinados componentes como parte de um plano geral para o aperfeiçoamento das operações de seu negócio (Consultoria Deloitte Touche Tohmatsu, 2003, p. 6).

José Maurício dos Santos Pinheiro (2006) ao recorrer ao documento na íntegra da Lei Sarbanes-Oxley, publicado no Portal do Governo americano (https://www.dol.gov/agencies/oalj/PUBLIC/WHISTLEBLOWER/REFERENCES/STATUTES/SARBANES_OXLEY_ACT_OF_2002), diz que:

> Em suas 1107 seções, o Ato Sarbanes-Oxley imputa responsabilidades nunca vistas perante os diretores de corporações, que vão desde o pagamento de multas ao cumprimento de penas de reclusão e sanções estendidas aos auditores que atestarem balanços com números fraudulentos. As seções 302 e 404 são as mais comentadas, sendo que a seção 302 trata da responsabilidade pessoal dos diretores executivos e diretores financeiros e a seção 404 determina uma avaliação anual dos controles e procedimentos internos para fins de emissão dos relatórios financeiros. É, portanto, a seção que mais impacta a área de TI (Pinheiro, 2006, p. 3).

Para Alexandre Di Miceli Silveira (2010) as 10 seções extraídas da SOX, indicadas no Quadro 3, são categorizadas como de maior grau de relevância para as empresas brasileiras:

Quadro 3 – Principais seções da SOX para as empresas brasileiras

Seção	Objetivo
201	Define serviços que são proibidos para os auditores dentro das companhias que auditam.
301	Define as funções atribuídas e nível de independência do comitê de auditoria em relação à direção da empresa.
302	Determina a responsabilidade dos diretores das empresas, que devem assinar os relatórios certificando que as demonstrações e outras informações financeiras incluídas no relatório do período, apresentam todos os fatos materiais e que não contém nenhuma declaração falsa ou que fatos materiais tenham sido omitidos.
304	Determina que os CEOs e CFOs são obrigados a restituir os valores recebidos como bônus ou remuneração variável, caso seja necessário corrigir suas demonstrações financeiras por descumprir alguma obrigação relevante da legislação americana.
401	Obriga a divulgação das informações trimestrais e anuais sobre todo fato material não relacionado com o balanço, patrimonial, tais como: transações, acordos, obrigações realizadas com entidades não consolidadas, contingências e outras.
402	Obriga a divulgação das principais transações envolvendo a diretoria e os principais acionistas da companhia. Nenhum diretor ou funcionário graduado de companhia aberta poderá receber, direta ou indiretamente, empréstimos em companhia aberta.
404	Determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Além disso, o auditor independente deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.
406	Define o Código de Ética para os administradores, alta gerência e gerência.
407	Obriga as empresas a informarem anualmente se possuem pelo menos um especialista em finanças no Comitê de Auditoria. Caso não tenham, precisam justificar publicamente a ausência desse profissional.
802	Define as penalidades criminais por alteração / destruição / falsificação de documentos a serem utilizados nas vistorias da SEC.

Fonte: Adaptado de Silveira (2010, p. 94-95) com a ferramenta COPILOT (2025)

Ao longo desta Seção, podemos observar a extensão e complexidade da Lei Sarbanes-Oxley, que estabelece diretrizes desde a estrutura das empresas até as suas diversas obrigações para o atendimento à Lei. Entretanto, para o atendimento ao sistema de controles internos, objeto de estudo que será detalhado ao longo deste Trabalho de Graduação, como deve ser implementado nas empresas, a SOX possui 2 principais seções, a 302 e a 404, conforme já aludido por Pinheiro (2006, p. 3).

Marcelle Colares Oliveira e Juliana Silva Linhares (2007) destacam a importância destas duas seções para a conformidade das empresas à SOX, já que elas tratam das responsabilidades dos diretores executivos e financeiros para com a fidelidade dos números nas demonstrações financeiras, das avaliações dos controles

e procedimentos internos ao longo do tempo e das multas e penalidades aplicáveis as empresas e executivos que cometerem fraudes (*Cf.* Oliveira; Linhares, 2007, p. 164).

Dessa forma, fica evidente a importância destas seções para as organizações. Seguindo essa premissa, neste Trabalho de Graduação iremos focar no atendimento das organizações perante a esses dois artigos, especialmente à seção 404.

Sobre a Seção 302, diz a Consultoria Deloitte Touche Tohmatsu (2003):

> (...) determina que os Diretores Executivos e Diretores Financeiros devem declarar pessoalmente que são responsáveis pelos controles e procedimentos de divulgação. Cada arquivo trimestral deve conter a certificação de que eles executaram a avaliação do desenho e da eficácia desses controles. Os executivos certificados também devem declarar que divulgaram todas e quaisquer deficiências significativas de controles, insuficiências materiais e atos de fraude ao seu Comitê de Auditoria (Consultoria Deloitte Touche Tohmatsu, 2003, p. 4).

Em relação a seção 404, Karla Jeanny Falcão Carioca, Márcia Martins Mendes de Luca e Vera Maria Rodrigues Ponte (2010), dizem que se trata de uma seção destinada à documentação e avaliação dos controles internos:

> (...) compreendendo desde o desenho do controle e como este funciona, até a sua operação, que é analisada por meio de amostras de transações ocorridas dentro dos processos operacionais da empresa. Ambos devem ser testados pela empresa e pela auditoria (Carioca; Luca; Ponte, 2010, p. 57).

Corrobora a exigência técnica a Consultoria Deloitte Touche Tohmatsu (2003) quando enfatiza que o "(...) auditor independente da companhia deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros" (Consultoria Deloitte Touche Tohmatsu, 2003, p. 4).

Os benefícios do atendimento às seções da SOX são vários, dentre eles podemos citar:

> tomar melhores decisões operacionais e obter informações mais pontuais; conquistar (ou reconquistar) a confiança dos investidores; evitar a evasão de recursos; cumprir leis e regulamentos aplicáveis; obter vantagem competitiva através de operações dinâmicas (Consultoria Deloitte Touche Tohmatsu, 2003, p. 7).

Entretanto, as empresas que deixam de instituir os controles exigidos podem se assemelhar a Enron e WorldCom, estando exposta maior à possibilidade de fraude, penalidades impostas pela SEC, se de capital aberto, sofrer publicidade desfavorável, o que impactaria negativamente "sobre o valor do acionista e queixas ou outras ações

judiciais impetradas por acionistas” (Consultoria Deloitte Touche Tohmatsu, 2003, p. 7).

Entretanto, ainda que exaltada a importância da SOX e a necessidade do cumprimento de suas exigências, principalmente para as empresas de capital aberto, ainda há uma certa dificuldade e até resistência no atendimento a lei por parte das empresas e seus respectivos executivos, razões que envolvem diversos fatores, desde monetários até humanos, como a inépcia e a falta de vontade.

Podemos citar, por exemplo, a seção 404 que, segundo Alexandre Di Miceli Silveira (2010), o conceito “controle interno” possui uma definição subjetiva, o que pode ocasionar um investimento demasiadamente desnecessário, no processo de implantação do desenho e na instituição destes controles, visto que, muitas vezes, não compreendem o custo-benefício da inserção destes processos (Silveira, 2010, p. 95). Sendo assim, para que o sistema de controle interno implementado nas organizações se encaixe perfeitamente nas exigências impostas pela SOX, é imprescindível que os executivos possuam o conhecimento de todas as seções da Lei, bem como a sua aplicabilidade.

Outro fator importante seria os custos necessários para o cumprimento das diretrizes legais. Segundo a Consultoria Deloitte Touche Tohmatsu (2023), tais custos seriam:

> (...) Custos diretos podem incluir o tempo dispensado por consultores e funcionários para avaliação, implementação e monitoramento; instrução de funcionários acerca dos controles internos; despesas com a nova tecnologia para suportar o programa de controles internos; e honorários pagos aos auditores independentes para executar os testes dos controles que visam atestar sua asserção quanto à eficácia de seus controles internos. Custos indiretos podem incluir o remanejamento de pessoal e o realinhamento de outros recursos na organização para criar e manter uma melhor estrutura de controles internos (Consultoria Deloitte Touche Tohmatsu, 2023, p. 11).

Conforme salienta a Consultoria, ainda que os custos financeiros para o cumprimento das diretrizes sejam altos, os custos causados pelo descumprimento das diretrizes (não-conformidade) sempre serão maiores (Consultoria Deloitte Touche Tohmatsu, 2023, p. 11). Além disso, espera-se que os benefícios futuros para os proprietários superem os investimentos com adequação e manutenção de uma estrutura de controles internos.

Por fim, o último fator seria um dos mais presentes nas empresas, podendo até ser o principal fator, no qual se trata do fator humano. Lahti e Peterson (2005) citados no artigo “O ato Sarbanes-Oxley e o impacto sobre a governança de TI das corporações”, de José Maurício dos Santos Pinheiro (2006, p. 9), informam que

> você pode ter as melhores políticas, aplicativos, ferramentas e controles, no entanto, nunca conseguirá eliminar completamente o “Fator Humano”. Logo, se não conseguir incorporar a área de gerenciamento de mudança, talvez não consiga se adequar ao Ato Sarbanes-Oxley independente de seus outros esforços (Lahti; Peterson, 2005, *Apud* Pinheiro, 2006, p. 9).

Com efeito, se os executivos e funcionários da empresa não compreenderem e/ou se não estiverem predispostos a cooperar, não será possível o atendimento à SOX, independentemente se os outros requisitos já estejam concluídos/atendidos.

José Maurício dos Santos Pinheiro (2006) cita que a resistência à mudança nas empresas pode ser atribuída a diversos fatores, como o medo do desconhecido, o entendimento de que a situação atual já é satisfatória e não precisa de alterações, o desconhecimento sobre os reais motivos que impulsionam a mudança e a dúvida crucial dos executivos/funcionários sobre os benefícios pessoais envolvidos expressa significativamente nesta indagação: O que eu ganho com isso? (*Cf*. Pinheiro, 2006, p. 9-10).

José Maurício dos Santos Pinheiro (2006, p.10) diz que para que o processo de adequação à SOX seja bem-sucedido, a comunicação entre os membros da organização é essencial, no qual é necessário que a comunicação ocorra com facilidade e de várias formas:

> sejam através de memorandos, e-mails, reuniões presenciais, conversas individuais, etc. O objetivo é produzir um efeito consistente demonstrando a necessidade da conformidade SOX e, principalmente, as consequências da não-conformidade (Pinheiro, 2006, p. 10).

3.2. Governança Corporativa após o advento da Lei Sarbanes-Oxley

Conforme apresentado ao longo deste Trabalho de Graduação, observamos que a Governança Corporativa no período pré-SOX já estava presente nas organizações/empresas, porém, era um conceito visto como “plus”, ou seja, apenas um elemento “adicional”, que não era classificado como fundamental para as organizações. Com a implementação da SOX e as suas diretrizes, as mudanças

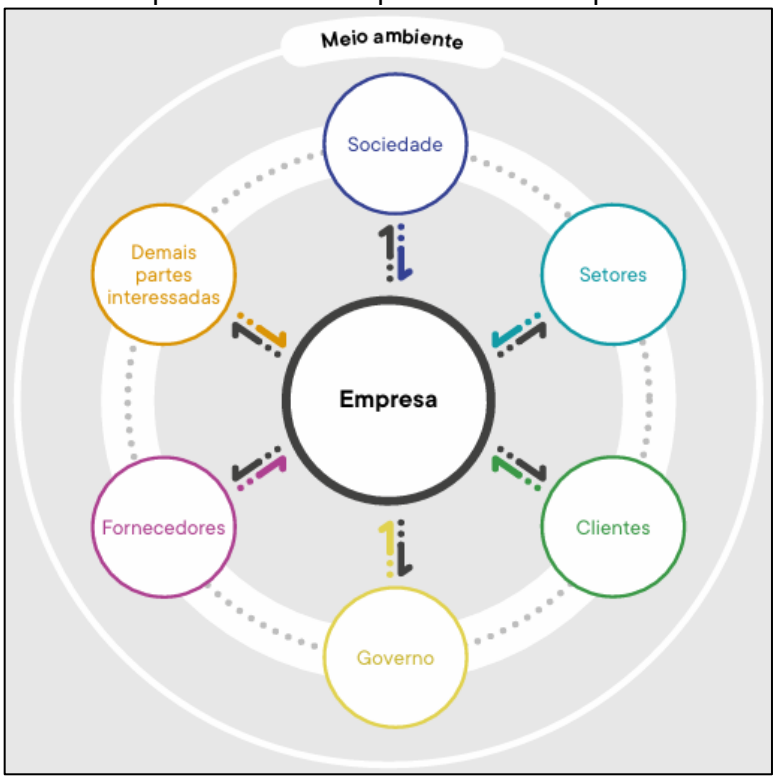
alcançaram um patamar tão relevante, que até a estrutura da Governança Corporativa foi afetada. O material publicado pelo IBGC (2023) confirma tal mudança:

> A governança corporativa evoluiu significativamente nos últimos anos, expandindo seu foco da otimização de valor econômico exclusivamente aos sócios para o objetivo de geração de valor compartilhado entre os sócios e as demais partes interessadas. Essa perspectiva contemporânea reconhece a interdependência entre as organizações e as realidades econômica, social e ambiental em que elas estão inseridas (IBGC, 2023, p. 16).

Dessa forma, a estrutura da Governança Corporativa, que antes era vista como um conceito aplicado apenas para otimização do valor econômico, tais como prevenção de fraudes, conciliações contábeis etc., passou a contemplar outras áreas da empresa, incluindo os departamentos de Tecnologia da Informação (TI) e de Sustentabilidade (ESG).

A Figura 1 confirma tal entendimento:

Figura 1 - Interdependência da empresa com suas partes interessadas



Fonte: Figura 1 do IBGC, 2023, p. 16

De acordo com o IBGC (2023), a estrutura da Governança Corporativa representa:

> (...) O conjunto de agentes, órgãos e relações existentes entre eles, que compõe o sistema de governança corporativa. Nem todas as organizações terão a estrutura completa de governança corporativa, tanto por seu estágio de maturidade, porte, natureza de atuação ou

> arcabouço regulatório, como pelos investimentos necessários para sua implantação. Nesse sentido, flexibilizações e adaptações podem ser caminhos alternativos para incorporar os princípios de governança corporativa a sua realidade, construindo uma jornada de evolução contínua (IBGC, 2023, p. 20).

De acordo com o IBGC (2023, p. 21), “a agenda de governança corporativa engloba diversas questões, sendo algumas delas a prevenção, mitigação e tratamento de conflitos de interesses”. Dessa forma, para atender todos esses pontos, na estrutura da Governança Corporativa é contemplado os envolvidos com esses processos, chamados de “agentes de governança”.

Em outro estudo denominado “Sistema de integridade: fundamentos e boas práticas”, no qual foi publicado pelo IBGC (2025), a definição de agente de governança é definida da seguinte maneira:

> Os agentes de governança devem desempenhar o papel de “guardiões dos princípios da governança corporativa”. Além de estabelecerem políticas, processos e procedimentos claros e eficazes, esses agentes devem garantir a implementação e a ampla divulgação dos componentes do sistema de integridade.
>
> (...) Espera-se que os agentes de governança orientem a tomada de decisão de forma imparcial, justa e transparente, assegurando que os interesses da organização e de suas partes interessadas sejam sempre priorizados (...) (IBGC, 2025, p. 24).

De acordo com o IBGC (2025), sistema de integridade pode ser definido da seguinte maneira:

> Um sistema de integridade pode ser definido como uma estrutura fundamentada em princípios, normas, procedimentos e mecanismos que não se limitam apenas à prevenção, detecção e correção de atos de corrupção, fraudes e outras violações de integridade. Seu foco principal é a disseminação, incorporação e manutenção da cultura organizacional ética e íntegra, gerando confiança interna e externa, reforçando a credibilidade e fortalecendo a sua reputação (IBGC, 2025, p. 11).

Dessa forma, o IBGC (*Cf.* 2025, p. 24) estabelece que os agentes de governança conectem a estrutura de governança ao sistema de integridade e que a sua efetividade não seja responsabilidade exclusiva de um gestor ou departamento específico, mas sim um compromisso compartilhado por todos os sócios, administradores, colaboradores, parceiros e terceiros da organização. No entanto, os membros da estrutura de governança têm responsabilidades diferenciadas nesse sistema, conforme descrito no Quadro 4:

Quadro 4 - Agentes de governança e suas responsabilidades

Agente	Responsabilidade
Sócios	Deve promover a criação e manutenção de uma cultura ética, definir estratégias alinhadas ao sistema de integridade e aprovar diretrizes organizacionais, além de garantir que suas ações estejam em conformidade com os valores da organização.
Conselho de administração	Deve assegurar que a ética e o propósito organizacional sustentem o sistema de integridade, promovendo sua cultura e supervisão. É responsável por aprovar políticas, recursos, estruturas e instrumentos de gestão, além de acompanhar riscos, denúncias, investigações e indicadores. Também deve avaliar a efetividade do sistema e garantir sua coerência com os valores da organização.
Diretor-presidente	Deve assegurar que a ética, a governança e o propósito organizacional fundamentem o sistema de integridade, promovendo sua cultura e a liderando. É responsável também por garantir recursos, autonomia e estrutura para a função de integridade, além de apoiar políticas, canais de denúncia e treinamentos internos.
Diretorias	Devem implementar e fortalecer o sistema de integridade conforme as diretrizes do conselho, promovendo a cultura ética na organização. Além disso, devem incentivar treinamentos, garantir conformidade com normas e leis, gerir riscos à integridade em suas áreas e aplicar medidas disciplinares quando necessário.
Governance officer e o departamento de Governança Corporativa	Devem apoiar os agentes de governança em seus processos, assegurando a inclusão de temas de integridade nas pautas. Também são responsáveis por conduzir programas de integração e educação continuada, alinhando essas iniciativas aos componentes do sistema de integridade.
Jurídico	Deve prover assessoria jurídica as áreas, verificando se há riscos de violações de leis, normas e regulamentos internos e externos nos processos da organização.
Gestão de pessoas	Deve assegurar que os processos de gestão de pessoas (contratação, demissão etc) estejam alinhados com os princípios de ética e integridade das organizações.
Demais unidades e áreas	Devem cumprir normas e legislações aplicáveis, gerenciar riscos à integridade em suas atividades e implementar controles internos eficazes. Devem comunicar irregularidades aos canais apropriados e contribuir com propostas de melhoria contínua para o sistema de integridade.

Fonte: Adaptado de IBGC (2025, p. 25-30) com a ferramenta COPILOT (2025)

Conforme o IBGC (2025),

> sócios, conselho de administração e diretoria podem contar com órgãos de governança para apoiar suas funções, especialmente nas áreas de fiscalização e controle. Dependendo da legislação, estrutura societária, porte e complexidade da organização, algumas estruturas são obrigatórias ou apenas recomendáveis (IBGC, 2025, p. 31).

No Quadro 5, podemos observar as responsabilidades destes Órgãos de fiscalização e de controle:

Quadro 5 - Órgãos de fiscalização e controle e suas responsabilidades

Órgão	Responsabilidade
Conselho fiscal	Deve fiscalizar os atos dos executivos, assegurando conformidade com os deveres institucionais e denunciando irregularidades conforme os processos definidos. Também é responsável por encaminhar os resultados das verificações às instâncias competentes, promovendo ações corretivas alinhadas às diretrizes éticas e regulatórias.
Comitê de auditoria	Deve monitorar o cumprimento de diretrizes, leis e regulamentos, acompanhar órgãos reguladores e participar de comitês para tratar irregularidades. Também é responsável por recomendar auditorias especializadas, comunicar suspeitas às autoridades, acompanhar investigações e medidas adotadas, além de avaliar periodicamente a eficácia do sistema de integridade e reportar resultados à alta administração.
Comitê de integridade	Deve assegurar que princípios e valores sejam traduzidos em normas de conduta e devidamente disseminados, supervisionar investigações e conflitos de interesse, e gerir canais de denúncia e consequências. Também é responsável por propor melhorias nos processos de integridade e apoiar a criação ou atualização de políticas e procedimentos, submetendo-os à aprovação do conselho de administração.
Chief integrity officer (CIO)	Deve promover e fortalecer a cultura de integridade, garantindo políticas, estrutura e metodologias para gestão de riscos, alinhadas aos princípios éticos e normas da organização. É responsável por implementar e monitorar o código de conduta, canais de denúncia e políticas, coordenar investigações e propor sanções, além de supervisionar indicadores e processos de integridade, inclusive com terceiros.
Controles internos	Devem prevenir desvios às diretrizes éticas, testar a efetividade dos indicadores e avaliar a eficácia dos controles do sistema de integridade, além de monitorar deficiências identificadas ao longo dos testes.
Gestão de riscos	Deve implementar práticas de gestão à integridade, desde a definição do apetite e tolerância até o mapeamento, avaliação, resposta, monitoramento e reporte dos riscos. Deve garantir que as áreas proponham medidas preventivas e corretivas, manter as práticas atualizadas e alinhadas às diretrizes éticas e identificar vulnerabilidades e exposições a práticas antiéticas ou violações regulatórias para tratamento adequado.
Auditoria interna	Deve assegurar a eficiência e efetividade da governança, gestão de riscos e controles internos, verificando a conformidade de processos e políticas. Também é responsável por avaliar indicadores e controles de integridade, identificar e reportar irregularidades, e contribuir para a melhoria contínua das políticas e procedimentos, garantindo sua eficácia na prevenção e detecção de desvios e fraudes.
Auditoria Independente/Externa	Deve assegurar que as demonstrações contábeis estejam livres de distorções relevantes, garantindo conformidade com as normas aplicáveis. Também deve avaliar riscos, manter ceticismo profissional e minimizar a possibilidade de emitir opinião inadequada durante todo o processo de auditoria.

Fonte: Adaptado de IBGC (2025, p. 31-37) com a ferramenta COPILOT (2025)

Ao longo desta Seção monográfica, podemos observar a complexidade para o estabelecimento de uma estrutura de Governança Corporativa visando o atendimento às exigências técnicas e jurídicas derivadas da SOX. Através de seus inúmeros capítulos e seções, a SOX se tornou essencial para a integridade das operações das empresas e para o bom relacionamento com os investidores, especialmente por meio da seção 404, as empresas estabelecem controles internos para garantir a veracidade e a autenticidade de seus resultados financeiros.

Na próxima Seção serão esclarecidas as diretrizes para o estabelecimento dos controles internos nas empresas, mediante a metodologia proposta pelo COSO (Committee of Sponsoring Organizations of the Treadway Commission), visando responder uma das questões centrais deste Trabalho de Graduação acerca da relação da Tecnologia da Informação (TI) com a SOX, a fim de garantir a integridade dos resultados financeiros obtidos pelas empresas.

4 COSO (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION)

Com o aumento da demanda da integridade e na transparência nas operações nas últimas décadas, o mercado corporativo necessitava de um método para atestar os seus resultados financeiros. Diante de tal situação, surgiu o COSO, no qual se tornou uma das mais influentes e amplamente aceitas estruturas para a gestão de controles internos e riscos corporativos.

De acordo com Maria Cecilia da Silva Brum (2014) na Dissertação de Mestrado em Ciências Contábeis sob o título “Controles Internos e de Tecnologia da Informação na mitigação dos riscos de conformidade das informações contábeis”, é informado que para o COSO (2012, p. 111), “a capacidade de gerar informação de qualidade começa com a qualidade dos dados de origem”. Brum conclui que “dados imprecisos ou incompletos, e as informações obtidas sobre esses dados, podem resultar em julgamentos potencialmente errôneos, estimativas ou outras decisões de gestão” (COSO, 2012, p. 111 *Apud* Brum, 2014, p. 20).

Para a garantia de integridade desses dados seria necessária uma estrutura/modelo. Tal necessidade seria atendida através do estabelecimento do COSO e os seus *frameworks*. Segundo Marcelle Colares Oliveira e Juliana Silva Linhares (2007), a origem do COSO data a partir de 1992:

> Em 1985, foi criada, nos Estados Unidos, a National Commission on Fraudulent Financial Reporting (Comissão Nacional sobre Fraudes em Relatórios Financeiros), uma iniciativa independente, para estudar as causas da ocorrência de fraudes em relatórios financeiros/contábeis. (...) Em 1992, publicaram o trabalho Internal Control Integrated Framework (Controles Internos: Um Modelo Integrado). Esta publicação tornou-se referência mundial para o estudo e aplicação dos controles internos (...) (Oliveira; Linhares, 2007, p. 166).

Após a publicação do *framework*, no qual alguns autores o denominam como COSO Report, a *National Comission on Fraudulent Financial Reporting* passou a ser denominada como COSO, conforme asseguram Marcelle Colares Oliveira e Juliana Silva Linhares (2007, p. 166) “(...) posteriormente a Comissão transformou-se em Comitê, que passou a ser conhecido como The Committee of Sponsoring Organizations – COSO (Comitê das Organizações Patrocinadoras)”.

Conforme José Maximo Daronco, o COSO possui como objetivo “(...) melhorar

o desempenho das organizações e os padrões de governança corporativa, por meio do desenvolvimento de metodologias e orientações sobre gerenciamento de riscos corporativos e controles internos" (Daronco, 2013, p. 36).

Sebastião Bergamini Junior (2005) destaca o envolvimento do COSO Report com a SOX:

> A SOX não faz menção ao protocolo Coso, no entanto, era necessário utilizar um protocolo aceitável para avaliar a efetividade dos controles internos contábeis. (...) Esse protocolo constitui um modelo de controle que deve ser adaptado às peculiaridades de cada empresa, de modo a resultar em uma metodologia de avaliação dos controles internos. Esse modelo fornece o critério de avaliação dos componentes de controle com a finalidade de obter um elevado grau de transparência das demonstrações contábeis. Sua característica principal é conceder visão de integração dos controles internos contábeis (Bergamini Junior, 2005, p. 168).

Para José Maximo Daronco (2013) na Dissertação de Mestrado em Ciências Contábeis sob o título "Análise de processos de controles internos e de TI no requisito de conformidade da governança corporativa", informa que através da publicação do COSO Report (1992), também conhecido como COSO 1, o controle interno é definido como um:

> (...) processo, desenvolvido pelo conselho de administração, executivos e pessoas de uma organização, para garantir, com razoável certeza, que sejam atingidos os objetivos da organização, nas seguintes categorias: eficácia e eficiência das operações, confiabilidade das informações financeiras e conformidade com as leis e regulamentações (COSO, 1992 *Apud* Daronco, 2013, p. 36).

Da mesma maneira, a definição para o termo "risco" será esclarecida de acordo com um estudo realizado pela SCCE (Society of Corporate Compliance and Ethics) e HCCA (Health Care Compliance Association) (2020), em associação com a COSO (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION), risco é definido como:

> (...) a possibilidade de que eventos ocorram e afetem a realização da estratégia e dos objetivos de negócios. Os riscos considerados nesta definição incluem aqueles relacionados a todos os objetivos de negócios, incluindo conformidade. Riscos de conformidade são aqueles relacionados a possíveis violações de leis, regulamentos, termos contratuais, normas ou políticas internas aplicáveis, onde tal violação possa resultar em responsabilidade financeira direta ou indireta, penalidades civis ou criminais, sanções regulatórias ou outros

> efeitos negativos para a organização ou seus colaboradores[6] (COSO; SCCE; HCCA, 2020, p. 1).

É importante ressaltar que ambos os “controles internos” e “risco” serão descritos detalhadamente ao longo desta Seção. Estes termos são peças fundamentais para a compreensão do “Cubo do COSO”.

Conforme Sebastião Bergamini Junior (2005), o COSO Report estabeleceu uma estrutura tridimensional denominada de Cubo do COSO, por meio da qual estabelece uma base do sistema de controle interno:

> A integração dos controles se baseia no uso de uma estrutura tridimensional (o chamado cubo do Coso), cujas dimensões compreendem os objetos de avaliação, as categorias de atividades de controle e os componentes de controle, da seguinte forma: (a) na primeira face estão os objetos de avaliação, ou seja, as unidades administrativas que deverão ser avaliadas; (b) na segunda face estão as três categorias de atividades de controle: processo, registro e conformidade; e (c) os cinco componentes de controle estão na terceira face: ambiente de controle, avaliação de risco, controle das atividades, processo de comunicação e a monitoração (Bergamini Junior, 2005, p. 168).

Segundo este mesmo autor (2005), “as vantagens do uso do Coso Report em fortalecer o sistema de controles internos contábeis despertaram os executivos para as possibilidades de promover o fortalecimento de todos os controles internos administrativos” (Bergamini Junior, 2005, p. 176).

De acordo com Romulo Paiva Farias, Marcia Martins Mendes de Luca e Marcos Vinicius Veras Machado (2009), em função do sucesso da primeira versão do Coso Report, foi necessária uma atualização no *framework* criado pelo COSO:

> O Coso Report passou a ser referência mundial na gestão de controle interno. Todavia, em 2004, o Coso publicou nova versão para o seu trabalho e criou uma metodologia chamada Enterprise Risk Management (ERM), ou Gestão de Riscos Empresariais. A visão do ERM é mais estratégica e leva em conta oportunidades associadas ao risco (Farias; Luca; Machado, 2009, p. 64).

---

[6] “Risk is defined by COSO as “the possibility that events will occur and affect the achievement of strategy and business objectives.” Risks considered in this definition include those relating to all business objectives, including compliance. Compliance risks are those risks relating to possible violations of applicable laws, regulations, contractual terms, standards, or internal policies where such violation could result in direct or indirect financial liability, civil or criminal penalties, regulatory sanctions, or other negative effects for the organization or its personnel”. SOCIETY OF CORPORATE COMPLIANCE AND ETHICS; HEALTH CARE COMPLIANCE ASSOCIATION. **COSO** (Committee of Sponsoring Organizations of the Treadway Commission): Enterprise Risk Management: Compliance Risk Management: Applying the COSO ERM framework. Nov. 2020, p. 1. (*Tradução nossa!)*

Segundo Sebastião Bergamini Junior (2005), os objetivos do COSO ERM podem ser descritos da seguinte maneira:

> O ERM compreende, entre outras atividades: o alinhamento da estratégia implementada com base numa propensão predeterminada ao risco; o aumento das decisões com base no instrumental de risco; a redução de perdas decorrentes de imprevistos operacionais; a identificação e o gerenciamento, de forma integrada, dos diversos riscos do negócio; a mensuração das oportunidades; e a melhoria no processo de alocação de capital (Bergamini Junior, 2005, p. 177).

Com o estabelecimento do COSO ERM, o Cubo do COSO consequentemente foi atualizado também. Segundo Sebastião Bergamini Junior (2005), a estrutura do Cubo do COSO teve as seguintes mudanças:

> A abordagem tridimensional do cubo do Coso Report se repete no ERM, que utiliza um cubo semelhante, acrescentando outros ingredientes: (a) a primeira face, relativa ao objetos do gerenciamento, permaneceu inalterada; (b) na segunda face, relativa aos objetivos do gerenciamento, foi adicionada uma categoria às três existentes – as atividades estratégicas de controle; e (c) na terceira face, relativa aos componentes de controle, foram acrescentados três aos cinco anteriormente existentes: definição dos objetivos, identificação dos eventos e resposta ao risco (Bergamini Junior, 2005, p. 177).

Em função desta reestruturação, o Cubo do COSO ERM pode ser representado, conforme Figura 2, elaborada pela ENAP (Escola Nacional de Administração Pública) e adaptada por este autor:

Figura 2 - Cubo do COSO ERM

Fonte: Adaptado da Figura 1 da ENAP, 2018, p. 6

O COSO ERM evoluiu o gerenciamento dos riscos e a sua relação com os controles internos, conforme declara Sebastião Bergamini Junior (2005):

> A técnica de avaliação de risco evoluiu de forma significativa, originando novos paradigmas: o cenário anterior previa uma postura de inspecionar, detectar e reagir aos riscos do negócio; considerava-se que o pessoal ineficiente era a fonte primária de riscos; e os controles eram direcionados para os riscos de origem financeira ou vinculados aos resultados escriturais. O cenário atual contempla uma série de novos desafios: a postura esperada é de prever e prevenir os riscos inerentes a um conjunto de processos; os processos ineficientes são, de fato, as fontes primárias de riscos; e os controles devem ser as ferramentas de gestão e de monitoração de riscos (Bergamini Junior, 2005, p. 176).

Pode-se observar ao longo desta Seção que para o atendimento ao artigo/seção 404 da SOX, o gerenciamento de riscos e os controles internos devem estar conectados e em plena sincronia. Portanto, no próximo item desta Seção será explicada a importância do gerenciamento de riscos e o seu envolvimento com os controles internos.

4.1. Gerenciamento de riscos

Para Nor Azimah Abdul Aziz (2012)[7]:

> No curso da condução de um negócio, as empresas enfrentam riscos variados diariamente, incluindo falhas nos mecanismos de controle interno, desastres financeiros, catástrofes ou desastres ambientais, não conformidade e violações regulatórias. Esses riscos são exacerbados pelo avanço da tecnologia, pela alta aceleração no ritmo dos negócios, pela sofisticação financeira multifacetada e pela globalização, que contribuíram para ampliar a complexidade dos riscos que as empresas precisam suportar (Aziz, 2012, p. 25).

Para Marcelle Colares Oliveira e Juliana Silva Linhares (2007), há diferentes categorias de riscos. Neste sentido, tanto a mitigação quanto o seu impacto acabam sendo distintos:

> Entende-se como risco a existência de situações que possam impedir o alcance de objetivos corporativos ou operacionais. Os riscos podem decorrer de processos errados ou de falta de controles internos. A

[7] "In the course of running a business, companies face wide ranging risks on daily basis which include the failures of internal control mechanism, financial fiasco, catastrophe or environmental disasters, non-compliance and regulatory violations. These risks are exacerbated by the advancement of technology, high acceleration in the pace of business, multi-faceted financial sophistication and globalisation which have all contributed to amplify the complexity of risks for companies to endure". Nor Azimah Abdul Aziz. Managing corporate risk and achieving internal control through statutory compliance. *In*.: **Journal of Financial Crime**, Vol. 20, 2012, p. 25. *Tradução nossa!*

> maioria dos riscos está relacionada com procedimentos operacionais e de conformidade com a legislação. Todos os tipos de risco prejudicam o sucesso da área estratégica e comprometem a reputação da empresa (Oliveira; Linhares, 2007, p. 161).

Como exemplo, foi utilizado o ambiente de gerenciamento de riscos disponibilizados no Portal do Serviço Federal de Processamento de Dados (SERPRO, 2025), no qual os riscos são categorizados como: Riscos Estratégicos; Riscos ao Negócio; Risco Operacionais; e Riscos de Projetos Estratégicos.

As descrições para cada um destes riscos, obtidas por meio da pesquisa do documento do Portal SERPRO, sob o título “Gestão de Riscos e Controles” (2025), podem ser visualizadas no Quadro 6:

Quadro 6 – Riscos nas operações da SERPRO

Agente	Responsabilidade
Riscos Estratégicos	Referem-se aos riscos definidos no momento do planejamento estratégico, associados à estratégia da empresa. O foco é o acompanhamento de fatores que podem tornar vulnerável o alcance dos objetivos estratégicos. Estes riscos, são identificados anualmente considerando cenários externos e informações estratégicas como os cenários regulatório do setor público, econômico e de tecnologia da SERPRO.
Riscos de Negócio	São riscos que prejudicam o atingimento da missão, visão ou valores do Serpro, atualizados anualmente, em processo semelhante ao dos riscos estratégicos. São riscos relacionados à estratégia de longo prazo.
Riscos Operacionais	Os riscos operacionais são causados por falhas na infraestrutura e dependência de poucos fornecedores, mitigados com investimentos em tecnologias críticas e negociações estratégicas. Os riscos financeiros decorrem de restrições orçamentárias e inadimplência, enfrentados com diversificação de clientes e novos produtos. Já os riscos de não conformidade envolvem mudanças legais sem tratamento adequado.
Riscos de Projetos Estratégicos	Inclui os riscos associados aos projetos estratégicos da Empresa, no qual são mapeados e os riscos críticos e controles relativos a estes projetos são monitorados, tal como priorizado pela Diretoria Executiva por meio das diretrizes do Plano Anual de Gestão de Riscos e Controles da SERPRO.

Fonte: Adaptado de SERPRO (2025) com a ferramenta COPILOT (2025)

Para a mitigação dos riscos ser eficiente, são necessários métodos para gerenciá-los. Oliveira e Linhares (2007) ressaltam a importância do gerenciamento dos riscos:

> O gerenciamento de riscos é necessário para antecipar possíveis erros, fraudes ou processos que possam gerar impactos negativos para a organização. A identificação adequada dos riscos tanto minimiza perdas como pode oferecer à corporação vantagens competitivas.
>
> Para o exercício de uma boa governança corporativa dentro de uma empresa, é necessária a implantação de técnicas para identificação, avaliação e controle de riscos. O gerenciamento de riscos compreende estas técnicas e implica a existência de um apropriado controle

> interno. Para que o gerenciamento de riscos seja um sucesso, é preciso que os líderes das organizações possam enxergá-lo como uma forma de gerar valor aos acionistas (Oliveira; Linhares, 2007, p. 161).

Para o IBGC (2023), a definição e os responsáveis pelo gerenciamento de riscos nas empresas são definidos da seguinte maneira:

> O gerenciamento de riscos se dá por meio de processos estruturados que auxiliem a identificação, o controle e a mitigação dos fatores de risco relacionados ao negócio. A gestão de riscos contribui para a continuidade e geração de valor da organização. Essa atividade é responsabilidade de todos os agentes de governança e deve ter como base a conformidade com princípios, políticas, normas, regulamentos e leis aplicáveis.
>
> A gestão de riscos está suportada por três linhas de atuação. A primeira corresponde aos gestores de cada linha de negócio; a segunda, às funções de gestão de riscos, controles internos e compliance; e a terceira, à auditoria interna (IBGC, 2023, p. 63).

Em relação as três linhas de defesa, conforme estudo intitulado “Declaração de posicionamento do IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles”, publicado pela IIA Brasil (Instituto dos Auditores Internos do Brasil) (2013), conforme a figura 3:

Figura 3 - Modelo de três linhas de defesa

Fonte: IIA Brasil, 2013, p. 2

Originalmente, esta estrutura fundamenta-se no modelo disponibilizado no Artigo 41 da “Guidance on the 8th EU Company Law Directive”, publicado pela EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING (ECIIA); FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS (FERMA) (2010, p. 9):

Figura 4 - Estrutura original do Modelo de três linhas de defesa
(Three lines of defence model)

Fonte: ECIIA; FERMA (2010, p. 9)

No estudo denominado “Auditoria interna aspectos essenciais para o conselho de administração”, realizado pelo IBGC em conjunto com o IIA Brasil (2018), são informadas, em detalhes, as responsabilidades de cada linha de defesa.

Tal estudo informa que “na 1ª linha de defesa, está a gestão operacional, no qual é responsável por manter os controles internos eficazes” (IBGC; IIA Brasil, 2018, p. 20).

Em outro estudo publicado pela IIA Brasil, sob o título “Declaração de posicionamento do IIA: As três linhas de defesa no gerenciamento eficaz de riscos e controles” (2013), dentre suas funções a gestão operacional “identifica, avalia, controla e mitiga os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos (...)” (IIA Brasil, 2013, p. 3).

Para a 2ª linha de defesa, o IBGC e o IIA Brasil (2018) informam que ela é composta por “(...) gestores de gerenciamento de riscos, conformidade, controles internos e outras áreas de controle” (IBGC; IIA Brasil, 2018, p. 20). As suas responsabilidades podem ser descritas da seguinte maneira:

> (...) Ela monitora as práticas de controles efetuadas pela primeira linha, sugere melhorias e contribui para que os responsáveis pelos processos, que estão na primeira linha, possam identificar os ris cos de suas áreas. Também está na segunda linha a função de conformidade (compliance), que monitora os riscos de não aderência a leis, normas, procedimentos etc.
>
> A segunda linha dispõe de conhecimento e amplitude para atuar em toda a organização, mas não conta com isenção plena para avaliar,

> uma vez que está envolvida com a gestão (IBGC; IIA Brasil, 2018, p. 20).

Por fim, conforme o IBGC e o IIA Brasil (2018), a isenção e a independência são elementos da 3ª linha de defesa para a garantia da auditoria interna:

> Como está fora da gestão, ela tem condições para avaliar tanto as funções quanto os processos relacionados a controles internos, conformidade e gestão de riscos feitas pelas duas linhas anteriores, assim como avaliar a organização como um todo.
>
> Nas organizações com as três linhas delimitadas, a auditoria interna pode auditar as funções da segunda linha de defesa, assim como as funções operacionais da primeira linha (...) (IBGC; IIA Brasil, 2018, p. 20).

Ao longo desta Seção foi relatado as melhores práticas para que as empresas consigam avaliar os riscos envolvidos não apenas em suas operações, mas também em seus regulamentos, normas internas e tomadas de decisões. Pode-se observar que a principal ferramenta para a mitigação dos riscos se dá com a criação e a manutenção dos controles internos. Sobre este assunto Romulo Paiva Farias, Marcia Martins Mendes de Luca e Marcos Vinicius Veras Machado (2009) asseguram que:

"O controle interno não pode ser dissociado do risco. Ambos seguem um caminho conjunto que auxilia a instituição a atingir seus objetivos quando aplicado e gerenciado da forma mais adequada" (Farias; Luca; Machado, 2009, p. 57).

A fim de complementar as informações refletidas nesta seção, é importante sublinhar que há uma norma específica para o gerenciamento de riscos, a ISO 31000:2018, que é uma referência internacional para a gestão dos riscos. Nesta mesma linha de pensamento, vale a pena ressaltar que, além dos riscos envolvidos nas operações das empresas, há os denominados "riscos ocupacionais", os quais são adequadamente descritos na NR (Norma Regulamentadora) 01, que traz disposições gerais e trata especificamente do gerenciamento de riscos ocupacionais, cujos dados estão voltados, sobretudo, para a área de segurança do trabalho[8].

Conforme aludido o gerenciamento e acompanhamento dos riscos apresentados durante essa seção são de extrema importância para uma empresa. A falha, a ignorância ou a demora na intervenção para mitigar um risco, pode transformá-

[8] Sobre a NR 01 (Portaria MTE nº 1.419, de 27 de agosto de 2024) entrará em vigor em 26 de maio de 2026 (Portaria MTE nº 765, de 15 de maio de 2025): https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/nr-01-atualizada-2025-i-1.pdf

lo de “simples risco” a um potencial “risco irreversível”, o que sujeitaria a empresa a prejuízos financeiros, além de outras retaliações de ordem jurídica, que podem conduzi-la a uma possível falência.

Sendo assim, o próximo item desta Seção descreverá as diretrizes e maneiras no qual os controles internos atestam e validam a integridade e conformidade das operações das empresas.

4.2. Controles Internos

De acordo com o IBGC (2023), “os controles internos são processos estabelecidos pelos agentes de governança com o objetivo de assegurar o alcance dos objetivos da organização em conformidade com requerimentos legais e regulatórios” (IBGC, 2023, p. 64).

Sergio Arnor Vieira (2007) afirma:

> Os controles internos dizem respeito às regras estabelecidas para proteção dos ativos da organização e englobam todos os recursos financeiros e não financeiros que precisam ser protegidos contra perdas, desperdícios ou desvios, daí a necessidade de um eficiente mecanismo de controle.
>
> O controle interno é um processo destinado a garantir, com razoável certeza e precisão, o atendimento dos objetivos da empresa, seja na eficiência e efetividade operacional, seja na confiança nos registros apresentados pelos relatórios contábeis e financeiros, seja na conformidade com as observâncias às leis e aos normativos aplicáveis à entidade e à sua área de atuação, por meio do desenvolvimento de um eficiente mecanismo de complience [sic!] (Vieira, 2007, p. 179-180).

No estudo “Sistema de integridade: fundamentos e boas práticas” publicado pelo IBGC (2025), compreende os controles internos como portadores de diversas funções, tais como a criação de mecanismos preventivos para lidar com desvios éticos, a realização de testes de efetividade dos indicadores de integridade, a análise da eficácia dos controles por meio de revisões e testes operacionais, o monitoramento de deficiências nos controles e o acompanhamento da implementação de melhorias na estrutura/sistema de controles internos (*Cf*. IBGC, 2025, p. 36).

Marcelo de Aguiar Coimbra e Vanessa Alessi Manzi (2010) citados no artigo de Maria Cecilia da Silva Brum (2014), denominado “Controles internos e de tecnologia

da informação na mitigação dos riscos de conformidade das informações contábeis" explicitam que os controles internos possuem os seguintes objetivos:

> auxiliar a organização a alcançar seus objetivos mediante a mitigação de riscos, reduzir a possibilidade de danos à sua reputação, assegurar que a empresa esteja cumprindo as leis e regulamentações, garantir a salvaguarda dos ativos, exatidão e fidedignidade dos registros e manter a exposição aos riscos de modo aceitável pela organização são resultados esperados de um sistema de controle interno (Coimbra; Manzi, 2010 *Apud* Brum, 2014, p. 23).

Por fim, para Ricardo Vinícius Dias Jordão, Antônio Artur de Souza e Anna Carolina Teddo (2012), os controles internos podem ser analisados como uma maneira de otimizar o processo de gestão e, consequentemente, melhorar o nível de governança corporativa e o controle das atividades empresariais nas empresas (*Cf*. Jordão; Souza; Teddo, 2012, p. 88). Tal entendimento pode ser confirmado por Marcelle Colares Oliveira e Juliana Silva Linhares (2007):

> Mediante a confiança nos controles internos é que se torna possível colher relatórios e demonstrações contábeis com informações condizentes com a realidade da organização, para desta forma tomar as melhores decisões e transparecer confiabilidade para o mercado financeiro em geral (...) (Oliveira; Linhares, 2007, p. 162).

Neste sentido, pode-se entender que uma das principais funções do controle interno é justamente a mitigação dos riscos nas operações das empresas. José Maximo Daronco (2013) diz que

> apesar de serem vários os conceitos apresentados por diversos autores, existe uma unidade de pensamento sobre o que se compreende por controle interno: são mecanismos adotados pelas empresas no sentido de minimizar o impacto de riscos de processo e de negócio (Daronco, 2013, p. 34).

Exposto o conceito de controles internos, a partir de agora serão refletidos os princípios e as diretrizes que garantem a eficácia e a integridade dos testes dos controles internos, visando o atendimento da seção 404 da SOX.

Fundamentando-se no livro "Manual de auditoria governamental", de Maria da Glória Arrais Peter e Marcus Vinícius Veras Machado (2003), Marcelle Colares Oliveira e Juliana Silva Linhares (2007) descrevem os princípios dos controles internos, os quais foram organizados por este autor, conforme Quadro 7:

Quadro 7 – Princípios dos controles internos

Princípio	Definição
Relação custo/benefício	Consiste na minimização da probabilidade de falhas/desvios quanto ao atendimento dos objetivos e metas. Este conceito reconhece que o custo de um controle não deve exceder aos benefícios que possa proporcionar.
Qualificação adequada, treinamento e rodízio de funcionários	A eficácia dos controles internos está diretamente relacionada com a competência e integridade do pessoal. Assim, é imprescindível que haja uma política de pessoal que contemple esses aspectos.
Delegação de poderes e determinação de responsabilidades	Visam a assegurar maior rapidez e objetividade às decisões, fazendo-se necessário um regimento/estatuto e organograma adequado, onde a definição de autoridade e consequentes responsabilidades sejam claras e satisfaçam plenamente às necessidades da organização; e manuais de rotinas/procedimentos claramente determinados, que considerem as funções de todos os setores do órgão/entidade.
Segregação de funções	A estrutura de um controle interno deve prever a separação entre as funções de autorização ou aprovação de operações e a execução, controle e contabilização das mesmas, de tal forma que nenhuma pessoa detenha competências e atribuições em desacordo com este princípio.
Instruções devidamente formalizadas	Para atingir um grau de segurança adequado, é indispensável que as ações, procedimentos e instruções sejam disciplinados e formalizados através de instrumentos eficazes, ou seja, claros e objetivos e emitidos por autoridade competente.
Controles sobre as transações	É imprescindível estabelecer o acompanhamento dos fatos contábeis, financeiros e operacionais, objetivando que sejam efetuados mediante atos legítimos, relacionados com a finalidade do órgão/entidade e autorizados por quem de direito.
Aderência às diretrizes e normas legais	É necessária a existência, no órgão/entidade, de sistemas estabelecidos para determinar e assegurar a observância das diretrizes, planos, normas, leis, regulamentos e procedimentos administrativos internos.

Fonte: Adaptado de Peter; Machado (2003) *Apud* Oliveira; Linhares (2007, p. 162)

Com tais bases, as empresas possuem as diretrizes necessárias para implementarem a estrutura/sistema dos controles internos. Entretanto, é importante ressaltar que esta implementação estrutural deve ser bem avaliada pela gestão executiva da empresa.

Conforme já foi refletido nas Seções anteriores deste Trabalho de Graduação, o atendimento à SOX é obrigatório para as empresas que possuem ações nas bolsas americanas; porém, caso uma empresa possua interesse voluntário por implementar um sistema de controle interno em seus processos, não há nada que as impeça, tendo em vista que as boas práticas apenas reforçam o nível de solvência e integridade destas instituições empresariais.

Não obstante, antes da implementação do sistema de controles internos, as empresas devem consideram algumas questões como a efetividade do sistema de controles internos e o seu esforço/custo para a sua respectiva implementação.

Em relação à efetividade, José Alves Dantas, Fernanda Fernandes Rodrigues, Gileno Fernandes Marcelino e Paulo Roberto Barbosa Lustosa (2010), garantem que o sistema de controle interno oferece uma garantia razoável, mas não absoluta:

> Em resumo, o controle interno oferece uma garantia razoável, não absoluta. Embora o controle interno possa ajudar a entidade a alcançar seus objetivos, não é uma panaceia. Nesse sentido, é preciso evitar que se crie o pressuposto de que instrumentos como governança corporativa e controles internos tenham 'poderes mágicos' (Dantas; Rodrigues; Marcelino; Lustosa, 2010, p. 6).

Em relação ao esforço/custo da implementação, as empresas devem avaliar a quantidade de controles internos que serão criados e quais áreas e/ou processos serão contemplados e/ou afetados, caso contrário, além do custo elevado para manter os controles internos, as empresas poderão experienciar dificuldades nas atividades do dia a dia. Nesta linha de argumentação, José Alves Dantas, Fernanda Fernandes Rodrigues, Gileno Fernandes Marcelino e Paulo Roberto Barbosa Lustosa (2010) asseguram:

> (...) O custo dos controles internos não deve ser superior aos benefícios que deles se esperam; as organizações têm recursos limitados e devem priorizar sua utilização nas atividades (incluindo os controles) que agregam mais valor; no caso dos controles, os recursos devem ser investidos para mitigar os riscos mais relevantes; e o excesso de controles pode onerar demasiadamente o processo, tornando-o dispendioso e contraproducente (pronto para a reengenharia) (Dantas; Rodrigues; Marcelino; Lustosa, 2010, p. 7).

Entretanto, apesar destas considerações, a implementação de um sistema de controle interno é fundamental para o atendimento às exigências da SOX, conforme estudo da Consultoria Deloitte Touche Tohmatsu (2003):

> Para muitas companhias, o cumprimento das medidas da Lei Sarbanes-Oxley relativas aos controles internos exigirá um esforço significativo. Na verdade, o trabalho inicial – desenvolver um programa de controles internos e a infraestrutura-suporte relacionada – pode ser intensivo. Entretanto, uma vez que o programa esteja bem estabelecido, a carga será amenizada e a estrutura e os processos tornar-se-ão parte dos procedimentos operacionais padrão de sua companhia (Consultoria Deloitte Touche Tohmatsu, 2003, p. 17).

Neste mesmo estudo, a Consultoria Deloitte Touche Tohmatsu (2003) apresenta as etapas para a implantação do programa/sistema de controles internos, conforme Quadro 8:

Quadro 8 – Etapas para a implantação de um sistema de controles internos, segundo a Consultoria Deloitte Touche Tohmatsu

Etapas	Definição
Planejar o programa	Recomenda-se formar uma equipe de gerenciamento para desenvolver o sistema de controle. O planejamento deve garantir o entendimento sobre os objetivos, escopo, custos e abordagem do projeto. É essencial garantir os recursos necessários, definir o papel de recursos externos e estabelecer uma base para monitorar o progresso. Além disso, os processos e metodologias de gestão devem estar alinhados para garantir a eficácia do sistema.
Avaliar o ambiente de controle	A eficácia dos controles internos vai além de regras formais, envolvendo também fatores subjetivos como cultura organizacional e postura ética. Esse conjunto forma o “Ambiente de Controle”, que deve ser fortalecido por ações como a valorização dos controles, reforço ao código de ética, liderança exemplar, treinamentos contínuos e canais seguros de comunicação, inclusive para denúncias anônimas.
Definir o escopo	O objetivo é mapear os riscos ligados à emissão de relatórios financeiros, para que a equipe de gerenciamento possa desenvolver controles eficazes de mitigação. O processo começa com a identificação das unidades operacionais, localidades e subsidiárias relevantes. Em seguida, são feitas entrevistas com gestores para detectar riscos que afetem a precisão e integridade das informações divulgadas, sejam elas financeiras ou não financeiras.
Construir um repositório de controles	Servirá como um repositório central de informações sobre os controles internos da organização, incluindo seus objetivos, desenho, implementação e formas de avaliação. Essa base será usada como referência nas revisões periódicas da administração. Para construí-la, é necessário definir os objetivos de controle, mapear as atividades atuais, compará-las com esses objetivos e corrigir possíveis falhas nos controles existentes.
Executar testes iniciais e contínuos	Após criar o repositório de controles, é fundamental avaliar se os controles estão funcionando de forma eficaz. Tal análise pode ser feita pela administração ou pela equipe de gerenciamento. O objetivo é identificar falhas, orientar correções em casos de deficiências e garantir que os controles operacionais estejam operando adequadamente. Também é necessário implementar um programa de testes contínuo para apoiar as revisões periódicas da administração.
Monitorar	A auditoria interna é essencial para supervisionar e relatar a eficácia dos controles internos. Quando não há essa função, a equipe de gerenciamento assume essa responsabilidade. O monitoramento inclui avaliar a qualidade dos dados, verificar a integridade e pontualidade dos testes, garantir que os avaliadores entendam os impactos de suas análises e assegurar que toda a documentação esteja completa e precisa.

Fonte: Adaptado de Consultoria Deloitte Touche Tohmatsu (2003, p. 17-22) com a ferramenta COPILOT (2025)

Com o sistema de controles internos estabelecido, é necessário testar o desenho e a efetividade perante a mitigação de riscos, tendo em vista as diretrizes definidas pela SOX.

De acordo com o Quadro 8, a garantia da efetividade dos controles é validada pelo departamento de Auditoria Interna. Para o IBGC (2023), “a auditoria interna tem a função de fortalecer a governança das organizações a partir da aplicação de uma abordagem sistemática e disciplinada à avaliação e melhoria dos processos de gerenciamento de riscos e controle” (IBGC, 2023, p. 62).

Em relação a auditoria interna, o IBGC (2023) reforça dois pontos para a execução destas práticas:

> As avaliações feitas pela auditoria interna devem estar alinhadas ao direcionamento estratégico da organização e se destinam a aperfeiçoar controles internos, normas e procedimentos, além de identificar riscos e recomendar controles para mitigá-los.
>
> A auditoria interna deve atuar em cooperação com a auditoria independente com o objetivo de fortalecer o ambiente de controle e mitigar os riscos da organização (IBGC, 2023, p. 63).

Em um estudo publicado pela IIA Brasil (2013), é destacado a importância da auditoria interna nas empresas:

> Estabelecer uma atividade profissional de auditoria interna deveria ser um requisito de governança para todas as organizações. Não é importante apenas para empresas de grande e médio porte, mas também pode ser igualmente importante para negócios menores, já que eles podem enfrentar ambientes igualmente complexos com uma estrutura organizacional menos formal e robusta para garantir a eficácia de seus processos de governança e gerenciamento de riscos (IIA Brasil, 2013, p. 5).

Em conjunto com a auditoria interna, as empresas possuem como um dos agentes de governança a auditoria independente, ou seja, a auditoria externa. Segundo o IBGC (2023), a auditoria independente possui a seguinte atribuição:

“(...) Emitir opinião se as demonstrações financeiras e os relatórios corporativos integrados preparados pela administração representam adequadamente, em todos os seus aspectos relevantes, a posição patrimonial e financeira da organização” (IBGC, 2023, p. 61).

Tal objetivo é alcançado através dos seguintes passos:

> Os auditores devem avaliar se os controles internos utilizados pela administração são adequados e suficientes para permitir a elaboração

> de demonstrações financeiras e relatórios corporativos integrados que não apresentem distorções relevantes, independentemente se causadas por erro ou fraude.
>
> O auditor independente deve emitir relatório com recomendações decorrentes de sua avaliação dos controles internos realizada durante o processo de auditoria (IBGC, 2023, p. 61).

A importância da auditoria independente para o sistema de controle interno das empresas é destacada pela IIA Brasil (2013):

> (...) Quando coordenados com sucesso, os auditores externos, reguladores e outros grupos externos à organização podem ser considerados linhas adicionais de defesa, que fornecem avaliações às partes interessadas da organização, incluindo o órgão de governança e a alta administração (...) (IIA Brasil, 2013, p. 6).

Com os papéis dos agentes de governança definidos, os controles internos passam a atender potencialmente as exigências delimitadas pela SOX. Mediante os testes dos controles, as empresas conseguem atestar o nível de eficácia de suas operações e a integridade dos seus relatórios financeiros.

O próximo item deste Trabalho de Graduação será apresentado um modelo, uma espécie de “passo a passo”, para a execução do teste dos controles, visando responder a seguinte pergunta: Caso os controles internos não estejam adequados, qual será a consequência para a empresa?

4.3. Não conformidades (deficiências) e suas consequências

Para a confirmação de que os controles internos estejam adequados, as empresas necessitam realizar dois testes/validações: os testes de desenho (test of design) e o teste de eficácia (test of effectiveness).

A Consultoria KPMG (2006) propõe:

> A documentação e avaliação do ICOFR[9] é parte essencial do processo de avaliação da administração. Fornece evidência de que os controles, que fazem parte do processo de avaliação da administração, foram identificados e devidamente comunicados aos que respondem pela sua execução e de que podem ser monitorados. Adicionalmente, os resultados da avaliação da administração quanto ao desenho e à eficácia operacional dos controles devem ser documentados (...) (Portal da Consultoria KPMG, 2006, p.10).

Conforme a Consultoria KPMG (2006), o teste de desenho possui como objetivo verificar se os controles internos, quando corretamente operados, são capazes de prevenir ou detectar erros nos registros contábeis. Esse teste é realizado

[9] *Internal Control Over Financial Reporting*

por meio de indagação, observação, inspeção de documentos e, de forma mais eficaz, mas não obrigatoriamente, pelo processo de *walk-through,* no qual seria o "passo a passo" do teste/verificação realizado. Tal processo ajuda a administração a compreender o fluxo das transações, avaliar se o desenho/mapeamento dos processos foi bem realizado, identificar pontos críticos de erro nas demonstrações financeiras, avaliar a efetividade dos controles e confirmar sua operação (*Cf*. Portal da Consultoria KPMG, 2006, p. 11).

Na realização dos testes, segundo a Consultoria KPMG (2006), o escopo de avaliação teria alguns aspectos, tais como o tipo do controle, a natureza (manual ou automatizado, preventivo ou detectivo), a sua frequência/periodicidade (diária, semanal, mensal, por ocorrência etc.), a competência dos responsáveis (departamento contábil ou TI, por exemplo) por executar o controle no dia a dia e, por último, os procedimentos para a correção de falhas, caso sejam identificadas (*Cf*. Portal da Consultoria KPMG, 2006, p.11).

Com o desenho dos controles internos bem estruturado, é necessário testar a sua eficiência, através de uma quantidade específica de amostras. De acordo com o Portal da Consultoria KPMG (2006), "a quantidade de teste depende de vários fatores. Todavia, ela deve ser suficiente para suportar a avaliação pela administração quanto à eficácia dos controles internos (...)" (Portal da Consultoria KPMG, 2006, p. 12).

A Consultoria KPMG (2006) indica exemplos de tamanhos mínimos de amostragem para a execução do teste de eficiência, conforme Quadro 9:

Quadro 9 – Exemplo de tamanhos mínimos de amostra para teste

Frequência de operação do controle	Tamanho mínimo da amostra
Anual	1
Trimestral	2-3
Mensal	2-4
Semanal	5-0 [sic!]
Diário	15-30
Controle manual recorrente (várias vezes por dia)	30-60

Fonte: Adaptado do Portal da Consultoria KPMG (2006, p. 12)

Após a realização dos testes, a administração ou o auditor interno pode eventualmente se deparar com alguns fatores que podem ocasionar um risco de falha no controle. De acordo com o Portal da Consultoria KPMG (2006), algumas destas falhas seriam as alterações nos processos/atividades mapeados, que podem ocasionar divergências ao testar o controle na fase de eficiência; a modificação dos

responsáveis pela execução ou pelo monitoramento dos controles; e a forma de execução do controle, automatizada ou manual, que pode afetar diretamente nos resultados dos testes (*Cf*. Portal da Consultoria KPMG, 2006, p. 12).

No tocante à pergunta: O que acontece quando um controle interno falha em sua execução? Tal situação pode originar uma não conformidade/deficiência do controle interno. Nessa linha de argumentação, a Consultoria Deloitte Touche Tohmatsu (2003), define deficiência como:

> (...) Uma falha no desenho, na implementação e/ou na eficácia operacional de uma atividade de controle. Essas falhas podem afetar adversamente a capacidade da companhia para iniciar, registrar, processar, resumir e reportar dados financeiros e não financeiros precisos (Consultoria Deloitte Touche Tohmatsu, 2003, p. 10).

Segundo publicação realizada pelo Portal Wolters Kluwer, em 2025, sob o título “Pontos fracos do controle interno: Identificação e soluções para auditores internos”, a descrição de deficiência e suas consequências são definidas como:

> Uma deficiência de controle interno é uma falha ou lacuna no sistema de controle interno de uma organização que a torna vulnerável a erros, fraudes, ineficiências ou violações de conformidade. As deficiências nos controles internos geralmente resultam de controles projetados de forma inadequada. Essas vulnerabilidades podem prejudicar a confiabilidade dos relatórios financeiros, dificultar a eficiência operacional e prejudicar a reputação da empresa.
>
> Quando um ponto fraco em um controle interno leva a um problema real, temos uma deficiência de controle interno. Uma deficiência representa falhas específicas em um sistema de controle interno que não consegue evitar, detectar ou corrigir erros e irregularidades prontamente (Portal Wolters Kluwer, 2025).

Ainda de acordo com o Portal Wolters Kluwer (2025), as deficiências são classificadas em três tipos, 1) no projeto de controle; 2) operacionais; e 3) de conformidade:

> Deficiências no projeto do controle: Ocorrem quando os controles são projetados de forma inadequada e não atingem os objetivos pretendidos. Por exemplo, a falta de segregação de funções pode levar a fraudes.
> Deficiências operacionais: Os controles projetados corretamente, mas executados de forma inadequada ou inconsistente, se enquadram nessa categoria. Um exemplo comum inclui documentação insuficiente ou aprovações não obtidas conforme necessário.
> Deficiências de conformidade: Surgem quando as organizações deixam de aderir às leis, aos regulamentos ou às políticas internas aplicáveis, arriscando multas, penalidades e danos à reputação (Portal Wolters Kluwer, 2025).

Segundo a Consultoria Deloitte Touche Tohmatsu (2003), há uma outra classificação para a deficiência de controle interno, que é a mais grave, denominada de “deficiência significativa”:

> A descrição apresentada pela SEC para uma deficiência significativa torna-a análoga a uma “condição reportável”, conforme descrito nos padrões de auditoria. Condições reportáveis são deficiências nos controles que chegam ao conhecimento dos auditores e que, segundo seu julgamento, devem ser comunicadas ao Comitê de Auditoria porque representam deficiências significativas no desenho ou na operação de controles internos (...) (Consultoria Deloitte Touche Tohmatsu, 2003, p. 10).

Para o Portal da Consultoria KPMG, no documento intitulado “Controles internos e as deficiências reportadas pelas empresas abertas brasileiras” (2024), as deficiências significativas:

> (...) São entendidas como aquelas que, no julgamento do auditor independente, têm impacto suficiente para merecer a atenção dos órgãos de governança. As deficiências nos controles internos ficam evidentes quando não há controles internos implementados ou quando os controles são implementados, mas de maneira não efetiva, sendo incapazes de prevenir, detectar ou corrigir distorções nas informações publicadas pelas organizações (Portal da Consultoria KPMG, 2024, p. 4).

É importante frisar que a recomendação aludida pelo Portal da Consultoria KPMG está diretamente vinculada a Resolução do Conselho Federal de Contabilidade (CFC) n.º 1.210/2009, que aprova a NBC TA (Normas Técnicas de Auditoria Independente), em conformidade às Normas Brasileiras de Contabilidade (NBC), especialmente a NBC TA 265, que trata especificamente da “Comunicação de Deficiências de Controle Interno”.

Ainda neste estudo proposto no Portal da Consultoria KPMG (2024) há uma pesquisa com 282 empresas, das quais 99 reportaram a existência de deficiências nos controles internos (Portal da Consultoria KPMG, 2024, p. 3). Das deficiências indicadas, a Consultoria KPMG as separou em três temas: processo contábil e as demonstrações financeiras; atividade operacional e gestão; e inclusive a tecnologia da informação (TI) (*Cf*. Portal da Consultoria KPMG, 2024, p. 5).

Nas deficiências constatadas pela pesquisa elaborada pela Consultoria KPMG (2024), alguns dos erros reportados no que diz respeito ao processo contábil e as demonstrações financeiras, podem ser exemplificados como “a falta de controle dos saldos bancários”, “erros contábeis” e “erros na elaboração das demonstrações

financeiras e notas explicativas”; quanto à atividade operacional e gestão, o documento cita “falta de processos e políticas corporativas”, “ineficiência da auditoria interna e/ou compliance” e “a estrutura de gerenciamento de riscos inadequada”; e quanto aos processos envolvendo a Tecnologia de Informação, podem ser mencionados a “inexistência de políticas de TI”, “acesso indevido a transações/banco de dados” e a “falta de integração entre sistemas” (*Cf*. Portal da Consultoria KPMG, 2024, p. 5).

Neste Trabalho de Graduação destaca-se a importância da Lei Sarbanes-Oxley para a integridade dos controles internos nas empresas. Conforme refletido, a SOX possui como um dos objetivos principais a garantia e a veracidade dos resultados financeiros, que devem ser divulgados pelas empresas, os quais são indicadores para os acionistas e, por conseguinte, aos órgãos governamentais, para as futuras tomadas de decisões. Conforme apresentado até agora, para as empresas conseguirem almejar este resultado, além de uma boa estrutura de governança corporativa e da implementação de controles internos, é fundamental o envolvimento do departamento de Tecnologia da Informação (TI), a fim de constituir a Governança de TI.

Dessa forma, com o referencial teórico estabelecido, a próxima Seção descreverá a relação da SOX com o departamento de TI. Serão refletidos quais são os principais riscos envolvidos nos processos das empresas, o papel da governança de TI, diretamente vinculada à governança corporativa, além da adoção das melhores práticas e *frameworks* por parte deste departamento para a garantia do atendimento à SOX.

5 LEI SARBANES-OXLEY E O DEPARTAMENTO DE TI

Ao longo desta Seção do Trabalho de Graduação será realizada a análise da relação entre a SOX e o departamento de TI, utilizando as definições de Governança Corporativa, SOX, Gerenciamento de Riscos e Controles Internos. Além disso, serão utilizadas outras fontes que complementam estas definições, tendo em vista a pesquisa aplicada à Tecnologia da Informação.

Atualmente, a TI desempenha um papel fundamental na sociedade. Seja para fins acadêmicos, para entretenimento ou para a execução/automação de atividades, a TI está presente, auxiliando na tomada de decisões. A mesma utilidade também se aplica ao mercado corporativo, pois, independente do ramo/segmento e tamanho de uma empresa, a TI estará presente nas operações desenvolvidas, ou seja, diariamente haverá a troca de informações/dados entre departamentos e sistemas.

O conceito de dados é considerado bem ambíguo; entretanto, para fundamentar a relação da TI com a SOX, será instrumentalizado o conceito publicado no Portal da IBM, em 2025, por Annie Badman e Matthew Kosinski, sob o título “O que são dados?”. Segundo Badman e Kosinski, dados são:

> uma coleção de fatos, números, palavras, observações ou outras informações úteis. Por meio do processamento de dados e da análise de dados, as organizações transformam dados brutos em insights valiosos que melhoram a tomada de decisões e geram resultados de negócios melhores (Badman; Kosinski, 2025).

Nesse sentido, pode-se perceber a importância dos dados e das informações para as empresas. Nas Seções anteriores deste Trabalho de Graduação foi destacada a necessidade da garantia da integridade das informações e no processo de documentação dos relatórios contábeis, pois tais dados revelam o planejamento das empresas, além de garantir o bom relacionamento com acionistas/investidores. Dessa forma, além do uso do gerenciamento de riscos e da adoção dos controles internos, as empresas utilizam o departamento de TI para a garantia destes dados.

A importância da TI nas empresas é destacada por Cleyton Takashi Kawaguti (2008), na monografia denominada “Governança corporativa em tecnologia da informação: um diferencial na obtenção de vantagem competitiva entre instituições financeiras”. Neste documento, Kawaguti recorre a Peter Weill e Jeanne Wenzel Ross (2006), a fim de especificar que:

> Na era da informação, os ativos tradicionais, como pessoas, instalações, dinheiro e relacionamento com clientes passaram a exercer valor secundário. A tecnologia da informação (TI) é o ativo de maior importância nessa era. No entanto, implementações de TI envolvem investimentos elevados, complexos e contínuos, e que, ainda por cima, não são garantia de obtenção dos resultados esperados. Esse cenário de incerteza faz com que muitos administradores renunciem à utilização plena da tecnologia da informação (Weill; Ross, 2006 *Apud* Kawaguti, 2008, p. 17).

O ITGI (IT Governance Institute), órgão hoje incorporado à ISACA (Information Systems Audit and Control Association), destaca na publicação “COBIT 4.1”, de 2007, a importância da TI para as empresas, não apenas na execução de atividades, mas também para a própria Governança Corporativa:

> Para muitas organizações a informação e a tecnologia que a suporta representam o seu bem mais valioso, mas muitas vezes é o menos compreendido. Organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação e a utiliza para direcionar os valores das partes interessadas no negócio. Essas organizações também entendem e gerenciam os riscos associados, tais como as crescentes demandas regulatórias e a dependência crítica de muitos processos de negócios da TI.
>
> A necessidade da avaliação do valor de TI, o gerenciamento dos riscos relacionados à TI e as crescentes necessidades de controle sobre as informações são agora entendidos como elementos-chave da governança corporativa (ITGI, 2007, p. 7).

Dessa forma, pode-se entender que o departamento de TI possui uma função de destaque nas empresas, através do atendimento contínuo as áreas de negócios. Para Aguinaldo Aragon Fernandes e Vladimir Ferraz de Abreu (2014), como exemplo de necessidades de aplicações de TI, categorizam que elas “(...) são necessárias para atender à continuidade e às estratégias do negócio. Determinam também quais aplicações deverão ser mantidas, melhoradas, substituídas e implantadas” (Fernandes; Abreu, 2014, p. 18). Dos exemplos informados pelos autores, podem-se citar os sistemas transacionais, sistemas de gestão, aplicações de *business intelligence* e de reconhecimento biométrico (*Cf*. Fernandes; Abreu, 2014, p. 18).

Tal suporte às aplicações é classificado como uma operação de serviço de TI, que, para Fernandes e Abreu (2014), pode ser entendida como “(...) operações onde acontece o atendimento da TI no fornecimento de serviços aos usuários, gestores e, possivelmente, clientes da organização, fornecedores, parceiros etc” (Fernandes; Abreu, 2014, p. 22). Os autores ainda citam alguns exemplos que podem ser enquadrados como operações de serviço de TI, conforme são explicitados no Quadro

10:

Quadro 10 – Principais operações de serviços de TI

Operações	Definição
Operações de sistemas	Contemplam desenvolvimento e manutenção de sistemas.
Operações de suporte técnico	Contemplam atendimento a usuários no uso dos softwares e infraestrutura da instalação.
Operações de infraestrutura	Contemplam serviços de infraestrutura de TI, suporte de TI, gestão de ativos de software, entrega de serviços e suporte a serviços.
Operações de segurança da informação	Contemplam serviços de planejamento da segurança da informação e o monitoramento diário de riscos ao ambiente computacional da organização e a seus dados, bem como atividades de conscientização, treinamento e educação para a segurança.
Operações de suporte ao CIO	Contemplam atividades de planejamento da TI, orçamento da TI, gerenciamento de contratos, gerenciamento de fornecedores, escritório de projetos e inovação tecnológica para negócios etc.
Operações de Governança de TI	Contemplam atividades para a promoção da implantação das melhores práticas na execução dos serviços de TI, seu planejamento, monitoramento, gestão e melhoria contínua.
Operações de processos	Consiste em projetos de elaboração, melhoria e implantação de processos de negócio e também o desenho de inovações nos processos de negócio.
Operações de arquitetura de TI	Consiste em atividades de planejamento e definição de arquiteturas de TI, notadamente de software, infraestrutura tecnológica e de aplicações e de serviços.
Outras operações	Serviços de garantia da qualidade, grupo de engenharia de software, grupo de gerenciamento da configuração, grupo de novas tecnologias e outras que dependem do tipo da operação requerida pela organização, comuns em empresas que trabalham com vários produtos do tipo “informação intensiva”, como é o caso das instituições financeiras.

Fonte: Adaptado de Fernandes; Abreu, 2014, p. 22-23

Pode-se observar a grande gama de operações de serviços que o departamento de TI realiza, operando desde o desenvolvimento de sistemas e aplicativos, até à realização de melhorias de processos e treinamentos. Ao analisar as operações destes serviços, é possível relacionar que a maioria destas operações às exigências prescritas pela Lei Sarbanes-Oxley. Dizem Fernandes e Abreu (2014): “A TI, como sabemos, é um elemento crítico como fonte de risco para a continuidade do negócio e para o atendimento ao SOX” (Fernandes; Abreu, 2014, p. 33).

O entendimento de que a SOX e a Governança Corporativa possuem uma estreita ligação com a TI também é compartilhado por José Maurício dos Santos Pinheiro (2006): “a SOX acabou apresentando um impacto significativo sobre a área de Tecnologia da Informação das organizações ao nível mundial uma vez que se insere no âmbito da governança corporativa e apresenta artigos diretamente voltados para a área de TI (...)” (Pinheiro, 2006, p. 3).

Acerca do vínculo das áreas de negócios e as atividades com TI destaca Pinheiro:

> Como não é possível separar processos de negócios e tecnologia no panorama corporativo atual, uma avaliação da infraestrutura operacional e pessoal de TI das empresas é igualmente requerida. (...) É importante salientar que o Ato Sarbanes-Oxley requer mais do que a documentação citada ou o estabelecimento de controles financeiros. Ao regular a atividade de contabilidade e auditoria das empresas de capital aberto, a SOX reflete diretamente seus dispositivos nos sistemas de tecnologia da informação (Pinheiro, 2006, p. 3-4).

Em relação aos sistemas contábeis e financeiros, Aguinaldo Aragon Fernandes e Vladimir Ferraz de Abreu (2014) destacam que do ponto de vista do departamento de TI, tais sistemas devem:

> Ter disponibilidade para acesso e emissão de relatórios de resulta dos financeiros e contábeis;
>
> armazenar os dados e as informações de forma adequada e com segurança;
>
> ter a possibilidade de implementar trilhas de auditoria e verificação de processos;
>
> ter os seus riscos (assim como os pertinentes à infraestrutura) conhecidos e gerenciados (Fernandes; Abreu, 2014, p. 11-12).

Nesse sentido, pode-se afirmar que o departamento de TI é fundamental para o sucesso e para a integridade das informações disponibilizadas nos relatórios financeiros, emitidos pelas áreas de negócios, pois ao passar dos anos com a crescente demanda e utilização de sistemas de automatização, sistemas de gestão, uso de Inteligência Artificial etc., a tendência é que os processos que, atualmente são realizados manualmente ou com pouco uso da tecnologia, sejam totalmente migrados para o meio virtual/sistemático. Dessa forma, a adequação do departamento de TI das empresas com a SOX é fundamental.

Afirma José Maurício dos Santos Pinheiro:

> (...) a implementação de novos processos, procedimentos ou aplicativos para a conformidade SOX deve beneficiar a empresa como um todo e a Tecnologia da Informação se torna crítica para o sucesso da conformidade SOX, assim como o suporte dos diversos ambientes empresariais será crítico para o sucesso da TI (Pinheiro, 2006, p. 5).

Entretanto, é importante ressaltar que a SOX não deixa explícito quais diretrizes e obrigações o departamento de TI e suas respectivas operações devem seguir e adotar. Nesta linha argumentativa, corrobora José Maurício dos Santos Pinheiro que a SOX:

> (...) apresenta um impacto significativo sobre a estrutura de TI da maioria das empresas. No entanto, um grande problema se apresenta: não existem especificações sobre que controles têm de ser estabelecidos dentro da estrutura de TI para a conformidade com a nova legislação (Pinheiro, 2006, p. 5).

Mesmo com as diretrizes não sendo informadas claramente, as operações e atividades do departamento de TI possuem um forte vínculo com as Seções 302 e 404 da SOX (*Cf.* Fernandes; Abreu, 2014, p. 32-33).

Para Pinheiro (2006, p. 6) este vínculo está diretamente relacionado com a Seção 404 da SOX:

> Considerando que os aplicativos de TI frequentemente suportam o início, a autorização, o registro, o processamento e a divulgação de transações financeiras, os controles de TI devem representar uma parte integrante do controle interno sobre os relatórios financeiros (ICOFR – Internal Control Over Financial Reporting).

Ainda que este embate seja realizado indiretamente, Fernandes e Abreu, por meio do Quadro 11, demonstram como a SOX impacta nas operações de TI:

Quadro 11 – Implicações da SOX nas operações de TI

Implicações da SOX	Operações de TI
O conteúdo da informação deve ser apropriado	Desenvolvimento/gerenciamento de requisitos de software, verificação (testes), validação pelos usuários, gestão de mudança e configuração.
A informação deve estar disponível no momento em que for necessária	Disponibilidade de aplicativos/infraestrutura, gerenciamento de incidentes no ambiente de produção, suporte ao usuário e gerenciamento de desempenho.
A informação é atual ou pelo menos é a última disponível	Gerenciamento de dados, planejamento e gerenciamento de desastres e segurança da informação na infraestrutura.
Os dados e as informações estão corretos	Segurança da informação em aplicativos, segurança da infraestrutura de TI, teste de softwares e gerenciamento de dados.
A informação é acessível aos usuários interessados	Segurança da informação referente a controle de acessos/privilégios e controle de autorizações.
Há um sistema de controle interno sobre relatórios financeiros	Avaliação de riscos de TI, gestão da qualidade e planos de desastres e recuperação

Fonte: Adaptado da Tabela 2.1 de Fernandes; Abreu, 2014, p. 34

Para a execução das atividades supracitadas no Quadro 11, visando o atendimento à SOX, a Governança de TI torna-se um poderoso recurso para o gerenciamento dos *frameworks* tanto para a gestão de suas atividades, quanto para o gerenciamento dos riscos envolvendo as suas operações e, principalmente, para a criação de controles internos.

5.1. Papel da Governança de TI

A Governança de TI está diretamente relacionada ao gerenciamento de riscos e na criação de controles internos. O seu papel é tão relevante que o seu bom funcionamento impacta positivamente em todos os departamentos de uma empresa, conforme destacam Renato José Sassi, Adriano Arrivabene, Cleber William Vicente e Rogério Lopes Passos (2023):

> Trata-se de um processo que não só abrange o ambiente tecnológico, mas também o ambiente técnico, os recursos humanos e toda a estrutura da empresa, para tal, é fundamentada em um tripé formado por profissionais de TI e usuários, ambos envolvidos conjuntamente nas atividades de manipular, controlar e monitorar as informações das empresas (Sassi; Arrivabene; Vicente; Passos, 2023, p. 696).

Neste sentido, pode-se categorizar que a Governança de TI possui um importante vínculo tanto com a Lei Sarbanes-Oxley quanto com a Governança Corporativa.

Entretanto, antes de ser descrito tal ligação, é necessário esclarecer a definição da Governança de TI e a sua estrutura, no qual será realizado ao longo deste item do Trabalho de Graduação.

José Maurício dos Santos Pinheiro (2006) descreve a Governança de TI como:

> (...) Uma derivação de Governança Corporativa, termo que tem hoje grandes aplicações no mundo empresarial. A Governança em TI inclui estruturas de relacionamentos e processos que tem como objetivos dirigir e controlar a organização para que esta alcance seus objetivos, mas que, simultaneamente, devem equilibrar os riscos em relação ao retorno da tecnologia de informação e a seus processos. São estruturas e processos que permitem controlar a execução e a qualidade dos serviços, viabilizando o acompanhamento de contratos internos e externos, ou seja, a Governança em TI define as condições para o exercício eficaz da gestão com base em conceitos consolidados de qualidade (Pinheiro, 2006, p. 1).

O ITGI (2007) a define como “(...) aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização” (ITGI, 2007, p. 7).

Além de estabelecer parâmetros e boas práticas para a realização das operações de serviços de TI, conforme aludido no Quadro 9; através da Governança de TI é possível melhorar o uso e o tratamento dos dados de uma empresa: “(...) a governança de TI habilita a organização a obter todas as vantagens de sua informação, maximizando os benefícios, capitalizando as oportunidades e ganhando

em poder competitivo" (ITGI, 2007, p. 7).

Fernandes e Abreu destacam que "o principal objetivo da Governança de TI é alinhar a TI aos requisitos do negócio, considerando soluções de apoio ao negócio, assim como a garantia da continuidade dos serviços e a minimização da exposição do negócio aos riscos de TI" (Fernandes; Abreu, 2014, p. 15). Além disso, acrescentam os autores que a Governança de TI deve

> (...) Prover a TI da estrutura de processos que possibilite a gestão do seu risco e compliance para a continuidade operacional da empresa; (...) Promover o emprego de regras claras para as responsabilidades sobre decisões e ações relativas à TI no âmbito da empresa (Fernandes; Abreu, 2014, p. 15-16).

Estes objetivos, de acordo com o documento do ITGI, estão contemplados nos pilares da Governança de TI, denominados como "áreas de foco", sendo classificados como alinhamento estratégico, entrega de valor, gestão de recursos, gestão de riscos e mensuração de desempenho (*Cf*. ITGI, 2007 p. 8).

Sendo assim, as áreas de foco "(...) descrevem os tópicos que os executivos precisam atentar para direcionar a área de TI dentro de suas organizações" (ITGI, 2007, p. 9).

No Quadro 12 apresenta-se a descrição de cada área de foco:

Quadro 12 – Áreas de Foco/Princípios da Governança de TI

Área	Operações de TI
Alinhamento estratégico	Foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização.
Entrega de valor	É a execução da proposta de valor de TI através do ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização, concentrando-se em otimizar custos e provendo o valor intrínseco de TI
Gestão de recursos	Refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem se à otimização do conhecimento e infraestrutura.
Gestão de risco	Requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia.
Mensuração de desempenho	Acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de performance e entrega dos serviços, usando, por exemplo, "balanced scorecards" que traduzem as estratégias em ações para atingir os objetivos, medidos através de processos contábeis convencionais.

Fonte: Adaptado da Figura 2 de ITGI, 2007, p. 8

Pode-se observar que os objetivos e áreas de foco/princípios da Governança de TI possuem uma relação e até uma certa semelhança com as diretrizes da Governança Corporativa e da SOX. Embora possuam descrições e algumas características diferentes, Governança de TI, Governança Corporativa e SOX buscam a qualidade e a integridade no uso das informações, tanto as contábeis quanto as tecnológicas.

Entretanto, é importante ressaltar que o escopo de uso e atuação da Governança de TI não está limitado apenas à Governança Corporativa e a SOX. Há outras certificações e regulamentos/leis que gerenciam a atuação da Governança de TI, tais como a ABNT NBR ISO/IEC 38500, o Acordo de Basileia II, o BSC (Balanced ScoreCard), CMM etc.

É importante sublinhar que o objetivo deste Trabalho de Graduação, prioritariamente, é explicar a relação da TI, seus elementos/ferramentas, com a Governança Corporativa e com a SOX.

Em relação a Governança Corporativa, é fundamental que os seus princípios e os seus agentes estejam em sincronia com a Governança de TI.

Para Peter Weill, no artigo denominado “Don’t just lead, govern: How top-performing firms govern IT”, através do estabelecimento de uma boa estrutura de Governança de TI, é desenhado e estabelecido boas práticas e princípios para a Governança Corporativa, em relação ao uso e ao gerenciamento da TI a fim de que os objetivos da empresa sejam alcançados. Weill ainda destaca que a Governança de TI incentiva e aproveita a engenhosidade de todos os colaboradores da empresa no uso da TI, enquanto garante a conformidade com a visão e os princípios gerais da empresa[10] (*Cf*. Weill, 2004, p. 3).

A relação entre a Governança de TI e a Governança Corporativa é ressaltada pela ABNT – Associação Brasileira de Normas Técnicas, na NBR ISO/IEC 38500 (2018), quando preconiza que a Governança da TI “(...) auxilia as estruturas da Governança Corporativa a assegurarem a conformidade com as obrigações

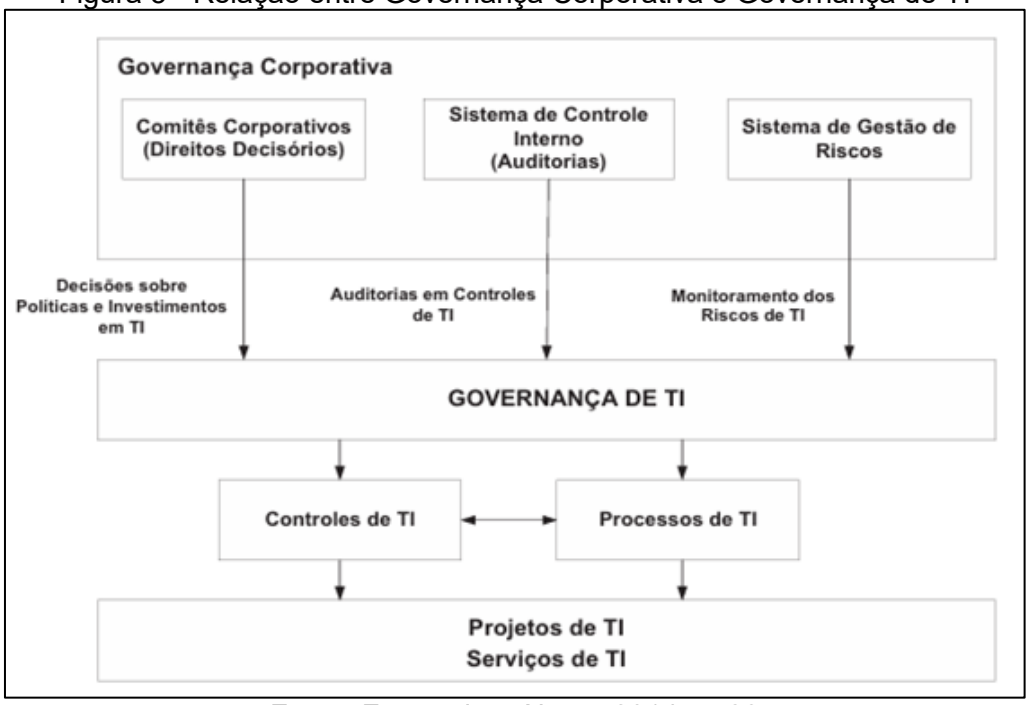
[10] “(…) Good IT governance draws on corporate governance principles to manage and use IT to achieve corporate perform ance goals. Effective IT governance encourages and leverages the ingenuity of all enterprise personnel in using IT, while ensuring compliance with the enterprise’s overall vision and principles (…)” (Peter Weill. Don’t just lead, govern: How top-performing firms govern IT. **MIS Quarterly Executive** vol. 3, n. 1, 2004, p. 3.

(regulamentares, legislativas, contratuais) em relação ao uso aceitável da TI" (ABNT, 2018, p. 5). Tal auxílio é realizado através da "(...) gestão de riscos eficaz e no incentivo à exploração de oportunidades decorrentes do uso da TI" (ABNT, 2018, p. 5).

Por fim, a relação entre Governança de TI e Governança Corporativa é retratada por Fernandes e Abreu ao declararem que os "(...) sistemas de controle e risco e de direitos decisórios da Governança Corporativa criam as restrições de operação dos serviços e projetos de TI" (Fernandes; Abreu, 2014, p. 27-28).

Neste mesmo contexto argumentativo, Fernandes e Abreu disponibilizam a representação visual dessa relação, ilustrada na Figura 5:

Figura 5 - Relação entre Governança Corporativa e Governança de TI



Fonte: Fernandes; Abreu, 2014, p. 28

Acerca da relação entre Governança de TI e SOX, Michelle L. Kaarst-Brown e Shirley Kelly (2005, p. 2) no artigo "IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function?" consideram que a SOX

> visa tanto a responsabilidade da gestão quanto a eficiência operacional, duas áreas que estão intimamente ligadas à função de TI. (...) Esse vínculo não se limita apenas ao nível da tecnologia ou dos sistemas, mas atinge o coração da governança de TI e do valor

> agregado. Tem o potencial de mudar as relações entre TI e o negócio[11] (Kaarst-Brown; Kelly 2005, p. 2).

Para Erastus Karanja e Jigish Zaveri, "nas diretrizes de conformidade da Lei SOX, o papel do ITG [Information Technology Governance] é implícito, embora na maioria das empresas as informações contábeis e os sistemas de relatório financeiro estejam incorporados em sistemas sofisticados baseados em TI"[12] (Karanja; Zaveri, 2012, p. 1). Sobre a relação entre SOX e Governança de TI ainda dizem:

> Nas empresas modernas, a infraestrutura de TI na forma de computadores, e-mails, intranets, Internet, ferramentas Web 2.0 e outras tecnologias é a espinha dorsal do ambiente diário, e a ITG deve desempenhar um papel de liderança auxiliando a equipe de TI e não-TI, bem como a gestão, a compreender seu escopo e as disposições de aplicação relacionadas à Lei SOX[13] (Karanja; Zaveri, 2012, p. 5).

Nesta linha argumentativa, Karanja e Zaveri, fundamentados nas seções 302, 401, 404 e 802, estabelecem a relação entre SOX e Governança de TI e sugerem algumas recomendações para a aplicação da legislação americana na Governança de TI, conforme ilustra o Quadro 13. Não obstante, para fins de esclarecimentos acadêmicos, este Trabalho de Graduação tem por objetivo apenas explorar a Seção 404, no tocante ao gerenciamento de riscos e controles internos.

---

[11] "SOX targets both management accountability and operating efficiencies – two areas that the IT function is tightly coupled with. (...) This coupling is not just at the level of the technology or the systems, but strikes to the heart of IT governance and value-added. It has the potential to change relationships between IT and the business" (Michelle L. Kaarst-brown; Shirley Kelly. IT Governance and Sarbanes-Oxley: The Latest Sales Pitch or Real Challenges for the IT Function? PROCEEDINGS OF THE 38TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 2005, Vol. 9, p. 2 (*Tradução nossa*!).

[12] "In the SOX Act compliance guidelines, the role of the ITG is implicit although in most firms, accounting information and financial reporting systems are embedded under sophisticated IT based systems". Erastus Karanja; Jigish Zaveri. Effect of the SOX Act on IT Governance. *In*.: **AIS Electronic Library**, 2012, p. 1. *Tradução nossa!*

[13] "In the modern firms, IT infrastructure in the form of computers, emails, intranets, Internet, Web 2.0 tools and other technologies are the backbone of the day-to-day environment and the ITG should play a leading role in aiding the IT and non-IT staff and management to comprehend their scope and the enforcement provisions as it pertains to the SOX Act. Erastus Karanja; Jigish Zaveri. Effect of the SOX Act on IT Governance. *In*.: **AIS Electronic Library**, 2012, p. 5. *Tradução nossa!*

Quadro 13 – Possíveis recomendações da SOX para Governança de TI

Seção da SOX	Papel da Governança de TI
Seção 302	Garantir que os sistemas que dão suporte aos processos de relatório financeiro sejam auditáveis, completos, forneçam dados precisos e informações sobre quando, onde e por quem os dados contábeis e financeiros foram coletados, manipulados, compartilhados ou armazenados.
Seção 401	Implementar sistemas financeiros capazes de fornecer dados precisos, consistentes e em tempo hábil, tanto internos quanto externos à empresa. Ter sistemas de informação organizacionais eficientes que permitam o compartilhamento de dados e a gestão de riscos com todas as partes interessadas ao longo da cadeia de valor.
Seção 404	Documentar e auditar regularmente os processos realizados pela unidade de TI. Incorporar mecanismos de controle de segurança de dados e informações. O CIO colabora constantemente com o CEO e o CFO para garantir o alinhamento da TI com a estratégia da empresa e quaisquer alterações/modificações no TI.
Seção 802	Garantir a autenticidade, consistência e precisão dos registros financeiros estabelecendo e aplicando políticas adequadas de controle de acesso. Educar a equipe de TI e funcionários relacionados sobre a importância de seguir as melhores práticas ao manusear dados e informações. Informar sobre quaisquer violações de dados envolvendo você ou parceiros e assegure que sistemas de backup fora do local estejam em funcionamento.

Fonte: Adaptado da Tabela 2 de Karanja e Zaveri, 2012, p. 4

Karanja e Zaveri informam que a Governança de TI deve possuir um responsável por estabelecer a relação com as áreas de negócios, com a Governança Corporativa e, principalmente, com a SOX, no qual seria o CIO (Chief Information Officer) (*Cf.* Karanja; Zaveri, 2012, p. 5)[14]. Para eles, o CIO possui a função de "garantir que as demonstrações financeiras sejam precisas e que os controles internos da empresa estejam em conformidade, porque quaisquer consequências negativas da não conformidade com a Lei SOX os afetarão indiretamente" (Karanja; Zaveri, 2012, p. 5)[15].

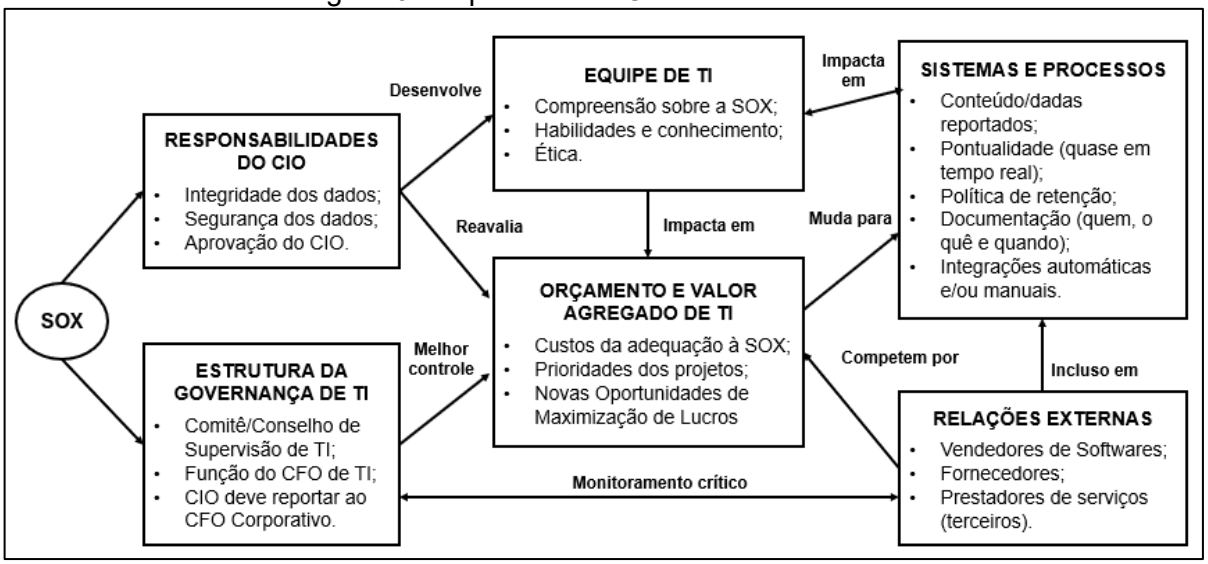
Conforme visto, a SOX impactou em diversos fatores relacionados a TI, inclusive em sua estrutura. Com os papéis da Governança de TI e de seus representantes estabelecidos, em decorrência das diretrizes expedidas pela SOX pode-se, enfim, visualizar a complexidade e a magnitude dos impactos gerados na

[14] "(…) As earlier acknowledged, SOX Act does not stipulate guidelines for the IT unit although we argue here that the role of CIO, who is in charge of ITG, is paramount in meeting the compliance requirements". Erastus Karanja; Jigish Zaveri. Effect of the SOX Act on IT Governance. *In*.: **AIS Electronic Library**, 2012, p. 5.

[15] "(...) Ensuring that the financial statements are accurate and the firm's internal control are in compliance because any negative consequences of non-SOX Act compliance will indirectly affect them". Erastus Karanja; Jigish Zaveri. Effect of the SOX Act on IT Governance. *In*.: **AIS Electronic Library**, 2012, p. 5. *Tradução nossa!*

estrutura de TI, conforme Figura 6:

Figura 6 - Impactos da SOX na estrutura de TI



Fonte: Adaptado da Figura 1 de Kaarst-Brown; Kelly, 2005, p. 2

Para Fernandes e Abreu (2014), os impactos que a implementação da SOX causa diretamente à Governança de TI são vários; podem ser citados a necessidade de implantar novos controles e funcionalidades em aplicações legadas, de implementar novas aplicações, além de ajustar e aprimorar os processos de TI existentes para mitigar os riscos identificados. Também é necessário projetar e implantar novos processos de TI, consequentemente, podendo acarretar mudanças no organograma do TI. Fernandes e Abreu (2014) concluem informando que devem ser definidos e implantados novos indicadores de desempenho e que, por sua vez, os riscos relacionados à TI precisam ser monitorados constantemente (*Cf*. Fernandes; Abreu, 2014, p. 35).

Ainda que a SOX não prescreva diretrizes específicas ao Departamento de TI, conforme já explicado, a Seção 404 da SOX exige que as empresas estabeleçam métodos para garantir o gerenciamento de riscos nas suas operações e na integridade de seus relatórios e resultados financeiros, papel fundamental a ser exercido pela Governança de TI, conforme destacado no documento intitulado “Global Technology Audit Guide 1: Riscos e Controles de Tecnologia da Informação – 2ª Edição”, publicado pelo The Institute of Internal Auditors (IIA), de 2012:

> O gerenciamento de riscos é um componente essencial de uma estrutura eficaz de governança de TI dentro de uma organização. A identificação e o gerenciamento de riscos de TI permitirão que a atividade de TI gerencie os negócios de TI com maior eficiência, além de identificar possíveis oportunidades para melhorar suas práticas (IIA, 2012, p. 6)

Dessa forma, para desempenhar esta função, a Governança de TI possui vários *frameworks* (métodos) para a criação e monitoramentos dos riscos e dos controles internos de TI, dentre eles o COBIT (Control Objectives for Information and Related Technologies) e a ITIL (Information Technology Infrastructure Library), itens que serão explorados nesta subseção.

5.2. COBIT e ITIL

De acordo com a Seção 4 deste Trabalho de Graduação, para o gerenciamento dos riscos e o estabelecimento dos controles internos, as empresas geralmente seguem o modelo e as práticas estabelecidas pelo COSO Report e COSO ERM. Entretanto, tais modelos abrangem práticas que contemplam ambientes, departamentos e atividades de uma empresa no geral, ou seja, não focam completamente em um único departamento; sendo assim, não atendem exclusivamente o departamento de TI e de Governança de TI.

Dessa forma, houve-se a necessidade de criar ferramentas que pudessem direcionar os executivos, a Governança de TI e os auditores internos/externos na mitigação dos riscos de TI e, consequentemente, na proposição, manutenção e avaliação dos controles internos de TI, comumente chamados de *frameworks*. Conforme aludido, a SOX não dita quais *frameworks* relacionados ao TI que as empresas devem adotar. No entanto, diversos autores e empresas concordam, conforme será demonstrado, que os melhores modelos indicados são COBIT e a ITIL.

De acordo com publicação “Qual a diferença de aplicação entre ITIL e Cobit?”, realizada pelo Portal Qualitor, em 2022, destaca a importância do COBIT e ITIL para Governança de TI:

> Tanto a ITIL quanto o Cobit são frameworks de processos. Ou seja, são duas grandes fontes de referência que reúnem as práticas mais indicadas e eficientes do mercado. É como se fossem duas enciclopédias de governança e gestão de serviços de TI, descrevendo que tipo de postura funciona ou não em diversos cenários diferentes.
>
> Os dois são essenciais para empresas que querem alcançar excelência técnica e de segurança em seu setor de TI. E eles se complementam, ou seja, o ideal é que ambos sejam utilizados como referência para nortear as atividades de Tecnologia da Informação de forma coordenada. Unidos, seu potencial de aprimorar a governança dessa área é amplificado (Portal Qualitor, 2022).

Pode-se notar algumas semelhanças entre os dois *frameworks,* entretanto

possuem diretrizes e objetivos distintos, ao tratar do gerenciamento dos processos e de operações de TI. O artigo denominado “ITIL e Cobit: entenda as principais diferenças e suas aplicações”, publicado no Portal Blog Impacta, em 2017, distingue os dois *frameworks*:

> Enquanto Cobit se preocupa principalmente em orientar as organizações na implementação, operação e melhoria dos processos de governança e gestão de TI, ITIL oferece orientações de boas práticas para gestão e execução de serviços de TI, sob a perspectiva da geração de valor ao negócio.
>
> De forma mais simples, o Cobit diz ‘o que’ é a ITIL explica ‘como’ (Portal Blog Impacta, 2017).

Em seguida, neste Trabalho de Graduação, serão descritas as diretrizes e estruturas destes *frameworks*, além dos respectivos atendimentos e alinhamentos à SOX e à Governança de TI.

5.2.1. COBIT

Ao longo desta Seção foi destacado que a Governança de TI propõe boas práticas e métodos para que o departamento de TI, no geral, consiga suportar as operações e objetivos das empresas, mediante gerenciamento das operações e dos riscos de TI, bem como a implementação de controles internos de TI. Entretanto, para que tais objetivos sejam alcançados, é necessário um modelo/*framework* que se adeque e dê suporte as diretrizes implementadas pelo COSO, das quais o COBIT é uma das principais ferramentas preferidas pelas empresas.

No documento publicado pela ITGI, denominado “COBIT 4.1: Modelo, Objetivos de Controle, Diretrizes de Gerenciamento e Modelos de Maturidade”, de 2007, pode-se definir o COBIT como um “modelo e uma ferramenta de suporte que permite aos gerentes suprirem as deficiências com respeito aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas (...)” (ITGI, 2007, p. 10).

Neste documento ainda destaca que o COBIT:

> (...) fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas práticas do CobiT representam o consenso de especialistas. Elas são fortemente focadas mais nos controles e menos na execução. Essas práticas irão ajudar a otimizar os investi mentos em TI, assegurar a entrega dos serviços e prover métricas para julgar quando as coisas saem erradas (ITGI, 2007, p. 7).

Segundo Fernandes e Abreu (2014), a primeira versão do COBIT foi lançada em 1994 e ao longo dos anos sofreu várias atualizações, especialmente em 1998, 2000, 2005, 2007 e em 2012, como COBIT 5 (*Cf*. Fernandes; Abreu, 2014, p. 203-204). É importante ressaltar que devido ao ano de publicação do livro destes autores citados, não foi considerada a versão atual do COBIT, lançada em 2018, conforme declara o Portal da ISACA (https://www.isaca.org/resources/cobit).

Há várias definições para o objetivo principal do COBIT. De acordo com o ITGI, o COBIT tem como missão “pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia a dia por gerentes de negócios, profissionais de TI e profissionais de avaliação” (ITGI, 2007, p. 11).

Para o ITGI (2007), os objetivos do COBIT estão intrinsecamente ligados com as diretrizes estabelecidas pelo COSO. Diz o documento: “o COSO (e outras metodologias similares) é geralmente aceito como uma metodologia de controle interno para corporações. O CobiT é um modelo de controles internos geralmente aceitos para a área de TI” (ITGI, 2007, p. 9).

Nesta mesma linha argumentativa, o COBIT e a Governança de TI possuem uma significativa ligação:

> Para atingir uma governança efetiva, os executivos requerem que os controles sejam implementados pelos gerentes operacionais com uma metodologia de controles definida para todos os processos de TI. Os objetivos de controle de TI do CobiT são organizados em processos de TI; portanto o modelo proporciona uma clara ligação entre os requerimentos de governança de TI, processos de TI e controles de TI (ITGI, 2007, p. 9).

De posse dos dados pesquisados, pode-se entender que, de maneira semelhante ao COSO, o uso do COBIT não é obrigatório; entretanto, para o atendimento dos objetivos das áreas de negócios e das diretrizes da SOX, é altamente recomendável a sua implementação por parte das empresas, independentemente de seu ramo de atuação ou tamanho. Dizem Fernandes e Abreu (2014):

> O modelo do CobiT é genérico o bastante para representar todos os processos normalmente encontrados nas funções da TI e compreensível tanto para a operação como para os gerentes de negócios, pois cria uma ponte entre o que o pessoal operacional precisa executar e a visão que os executivos desejam ter para “governar” (Fernandes; Abreu, 2014, p. 205).

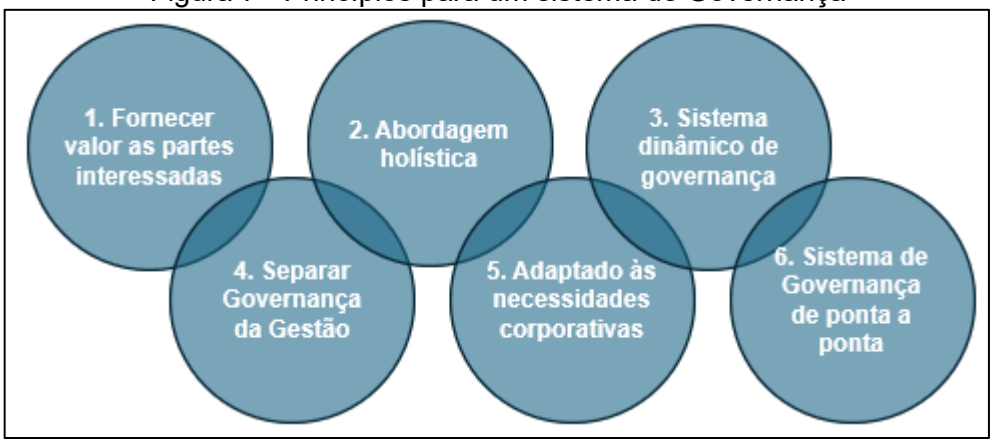
Em relação à estrutura do COBIT, serão utilizados os princípios e domínios de processos do COBIT 2019, disponibilizados em “Cobit® 2019 Framework: Introduction & Methodology”, publicado pela ISACA, além da “Cartilha COBIT 2019”, organizada por João Souza Neto e Leandro Pfeifer Macedo (2021) e da obra “Implantando a Governança de TI: da estratégia à gestão dos processos e serviços”, de Aguinaldo Aragon Fernandes e Vladimir Ferraz de Abreu (2014).

No que se diz sobre a estrutura dos princípios do COBIT 2019, João Souza Neto e Leandro Pfeifer Macedo (2021) informam que:

> O COBIT® ® 2019 foi desenvolvido com base em dois conjuntos de princípios:
>
> Princípios que descrevem os principais requisitos de um Sistema de Governança para informações e tecnologia; e
>
> Princípios para uma estrutura de Governança que pode ser utilizada para construir um Sistema de Governança para a toda a organização (Souza Neto; Macedo, 2021, p. 9).

A primeira estrutura do COBIT possui seis princípios, conforme Figura 7:

Figura 7 - Princípios para um sistema de Governança



Fonte: Adaptado da Figura 3.1 de ISACA, 2018, p. 17

Segundo Fernandes e Abreu (2014, p. 206) e Souza Neto e Macedo (2021, p. 9), para fornecer valor as partes interessadas, as empresas precisam de um sistema de governança, que gerem valor a partir do uso da TI. Isto pode ser mensurado quando há equilíbrio por meio da entrega de benefícios, otimização dos riscos e os custos dos recursos.

Em relação a uma abordagem holística, Souza Neto e Macedo (2021) informam que “um sistema de Governança Corporativa de TI é construído a partir de uma série de componentes que podem ser de diferentes tipos e que trabalham juntos de uma forma holística” (Souza Neto; Macedo, 2021, p. 9). Em outras palavras, os

componentes podem ser entendidos como processos, arquiteturas, informações etc., e que para atender este princípio, todos devem funcionar em conjunto e em harmonia.

Em relação a um sistema dinâmico de governança, Souza Neto e Macedo informam que:

> Isso significa que cada vez que um ou mais dos fatores de desenho são alterados (por exemplo, uma mudança de estratégia ou tecnologia), o impacto dessas mudanças no Sistema de Governança Corporativa de TI deve ser considerado. Uma visão dinâmica da governança Corporativa de TI levará a um Sistema de Governança Corporativa de TI viável e com prontidão estratégica (Souza Neto; Macedo, 2021, p. 9).

Souza Neto e Macedo informam que “um Sistema de Governança deve distinguir claramente entre as atividades e estruturas de Governança e Gestão” (Souza Neto; Macedo, 2021, p. 9). A expressão Gestão foi tratada anteriormente, em 2014, por Fernandes e Abreu como “Gerenciamento” (Fernandes; Abreu, 2014, p. 212).

Nesta mesma linha argumentativa, Fernandes e Abreu corroboram este pensamento quanto explicitam que o COBIT deve distinguir as atividades e as estruturas organizacionais, de modo que a Governança assegure:

> (...) que as necessidades, condições e opções das partes interessadas sejam avaliadas para determinar objetivos corporativos balanceados e acordados a serem atingidos, estabelecendo prioridades, tomando decisões e monitorando o desempenho e a conformidade em relação à direção e aos objetivos acordados (Fernandes; Abreu, 2014, p. 211).

Em contrapartida, os autores informam que o Gerenciamento “planeja, constrói, executa e monitora atividades de forma alinhada com a direção estabelecida pelo grupo de governança, visando o atingimento dos objetivos corporativos. Em geral, é uma responsabilidade da gerência executiva, sob a liderança do CEO da empresa” (Fernandes; Abreu, 2014, p. 212).

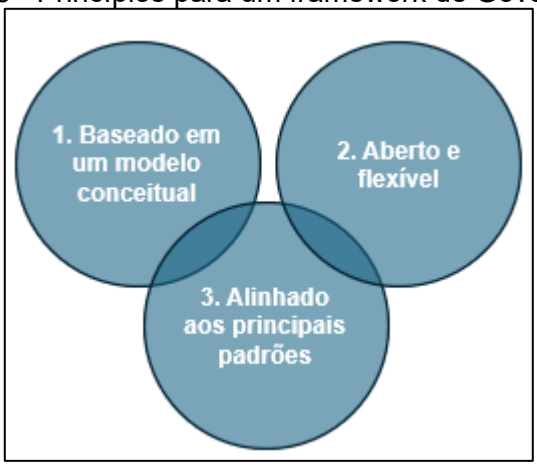
Quanto ao quinto princípio de um sistema de governança, Souza Neto e Macedo informam que “deve ser adaptado às necessidades da organização, com a utilização de um conjunto de fatores de desenho como parâmetros para personalizar e priorizar os componentes do Sistema de Governança” (Souza Neto; Macedo, 2021, p. 9).

Quanto ao último princípio, Souza Neto e Macedo especificam que um sistema de governança deve

> cobrir a organização de ponta a ponta, focando não apenas na função de TI, mas em toda a tecnologia e processamento de informações que a organização colocar em prática para alcançar seus objetivos, independentemente de onde o processamento está localizado na organização" (Souza Neto; Macedo, 2021, p. 9).

A segunda estrutura do COBIT 2019 está relacionada aos princípios para um *framework* de Governança, conforme Figura 8:

Figura 8 - Princípios para um framework de Governança



Fonte: Adaptado da Figura 3.2 de ISACA, 2018, p. 18

Quanto ao primeiro dos três princípios, da Figura 8, a ISACA (2018) descreve como "um *framework* de governança deve ser baseado em um modelo conceitual, identificando os principais componentes e os relacionamentos entre os componentes, para maximizar a consistência e permitir a automação"[16] (ISACA, 2018, p. 18).

Para o segundo princípio, assegura que "um framework de governança deve ser aberto e flexível. Deve permitir a adição de novos conteúdos e a capacidade de abordar novas questões da forma mais flexível possível, mantendo a integridade e a consistência"[17] (ISACA, 2018, p. 18).

Por fim, para o último princípio, a ISACA (2018) define que "um framework de governança deve estar alinhado com os principais padrões, estruturas e

[16] "A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation". ISACA (Information Systems Audit and Control Association). COBIT 2019 Framework: Introduction and Methodology. 2018, p. 18. (*Tradução nossa!)*

[17] A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency". ISACA (Information Systems Audit and Control Association). COBIT 2019 Framework: Introduction and Methodology. 2018, p. 18. (*Tradução nossa!)*

regulamentações relevantes”[18] (ISACA, 2018, p. 18).

Além dos princípios e diretrizes supracitados, o COBIT, de acordo com Fernandes e Abreu, “sugere um modelo de referência que define e descreve processos, agrupando-os nas áreas-chave de governança e gerenciamento” (Fernandes; Abreu, 2014, p. 212).

Na versão do COBIT 5, de 2012, e do COBIT 2019, há cinco domínios de processos, sendo dividido em 37 processos de TI na versão do COBIT 5, os quais foram atualizados para 40 na atual versão de 2019.

No Quadro 14 serão apresentadas as definições dos domínios:

Quadro 14 – Domínios de processos do COBIT

Domínio	Descrição
Governança - Avaliar, Dirigir e Monitorar (EDM)	Este domínio contém cinco processos de governança, dentro dos quais são definidas práticas de avaliação, direção e monitoração.
Alinhar, Planejar e Organizar (APO)	Este domínio tem abrangência estratégica e tática e identifica as formas através das quais a TI pode contribuir melhor para o atendimento dos objetivos de negócio, envolvendo planejamento, comunicação e gerenciamento em diversas perspectivas.
Construir, Adquirir e Implementar (BAI)	Este domínio cobre identificação, desenvolvimento e/ou aquisição de soluções de TI para executar a estratégia de TI estabelecida, assim como a sua implementação e integração junto aos processos de negócio. Mudanças e manutenções em sistemas existentes também estão cobertas por este domínio, para assegurar a continuidade dos respectivos ciclos de vida.
Entregar, Reparar e Suportar (DSS)	Este domínio cobre a entrega propriamente dita dos serviços requeridos, incluindo gerenciamento de segurança e continuidade, reparo de equipamentos e demais itens relacionados, suporte aos serviços para os usuários, gestão dos dados e da infraestrutura operacional.
Monitorar, Avaliar e Medir (MEA)	Este domínio visa assegurar a qualidade dos processos de TI, assim como a sua governança e conformidade com os objetivos de controle, através de mecanismos regulares de acompanhamento, monitoração de controles internos e de avaliações internas e externas.

Fonte: Adaptado da Figura 6.5 de Fernandes; Abreu, 2014, p. 213 (Uso das descrições); Souza Neto; Macedo, 2021, p. 12-13 (Uso das nomenclaturas dos domínios)

Ao analisar o Quadro 14, reforça-se a ideia de que, além de auxiliar e orientar os colaboradores e executivos do departamento de TI e da Governança de TI no planejamento e gerenciamento de suas operações, por meio do COBIT pode-se estabelecer as bases para o gerenciamento de riscos e criação dos controles internos

[18] “A governance framework should align to relevant major related standards, frameworks and regulations”. ISACA (Information Systems Audit and Control Association). COBIT 2019 Framework: Introduction and Methodology. 2018, p. 18. (*Tradução nossa!)*

de TI (*Cf*. ITGI, 2007, p. 10).

Neste sentido, o COBIT, como ferramenta de TI, auxilia nos controles internos e, por consequência, ajuda a atender as prescrições da SOX, conforme atestam Fernandes e Abreu (2014):

> Como modelo de Governança de TI, o CobiT pode ser aplicado tanto em pequenas organizações como em grandes empresas de TI, desde que esteja consistente com os objetivos de negócio e com as suas estratégias relacionadas à TI.
>
> (...) O CobiT é aplicável a todas as funções envolvidas na governança e no gerenciamento da informação e da tecnologia relacionada, nas quais a informação pode ser processada. Isso inclui a gestão executiva da corporação, os gestores de negócio, os gestores de TI e também os profissionais que atuam em verificações (como por exemplo auditores e áreas de garantia de qualidade) (Fernandes; Abreu, 2014, p. 220-221).

De acordo com o apresentado neste Trabalho de Graduação, o COBIT e a ITIL são os principais *frameworks* para a Governança de TI. Apesar das diferenças, ambos se complementam e buscam estabelecer as melhores práticas para o gerenciamento (“o que”) e execução (“como”) das operações de TI. Dessa forma, neste próximo subitem, será descrito a importância da ITIL para a Governança de TI.

5.2.2. ITIL

A importância da ITIL como *framework* é destacado por várias fontes de informação pesquisadas, seja em artigos, seja em livros. Em sua grande maioria, é possível observar um fator em comum de que o uso da ITIL nas empresas vem crescendo exponencialmente, desde a época de seu lançamento, em meados de 1980, até os dias atuais, a ITIL ainda se consagra como uma das melhores e mais importantes *frameworks* para o gerenciamento dos serviços de TI.

Segundo Aguinaldo Aragon Fernandes e Vladimir Ferraz de Abreu (2014), a ITIL pode ser descrita como:

> (...) um agrupamento das melhores práticas utilizadas para o gerenciamento de serviços de tecnologia de informação de alta qualidade, obtidas em consenso após décadas de observação prática, pesquisa e trabalho de profissionais de TI e processamento de dados em todo o mundo. Devido à sua abrangência e profundidade, a ITIL tem se firmado continuamente como um padrão mundial de fato para as melhores práticas para o gerenciamento de serviços de TI (Fernandes; Abreu, 2014, p. 227).

No documento denominado “Developing the IT Audit Plan”(2008), de autoria de

Kirk Rehage, Steve Hunt e Fernando Nikitin, dentre as melhores práticas que uma empresa pode ter, a padronização de suas operações e serviços é essencial, com uso da ITIL, tais objetivos podem ser alcançados. No estudo, a definição do *framework* é dada como "(...) um conjunto de conceitos e técnicas para o gerenciamento de infraestruturas de TI, bem como o desenvolvimento e a instalação de novos sistemas computacionais e operações de TI"[19] (Rehage; Hunt; Nikitin, 2008, p. 7). Dentre os benefícios de seu uso destaca-se que estabelece um "(...) vocabulário comum de termos definidos e amplamente utilizados. Organizações que implementam os conceitos da ITIL têm reivindicado um maior grau de confiabilidade e menores custos de entrega"[20] (Rehage; Hunt; Nikitin, 2008, p. 8).

Em relação objetivo da ITIL, Fernandes e Abreu informam que:

> Como um *framework*, o principal objetivo da ITIL é prover um conjunto de práticas de gerenciamento de serviços de TI testadas e comprovadas no mercado (organizadas segundo uma lógica de ciclo de vida de serviços), que podem servir como balizadoras, tanto para organizações que já possuem operações de TI em andamento e pretendem empreender melhorias, quanto para a criação de novas operações (...) (Fernandes; Abreu, 2014, p. 227).

Conforme destacam Fernandes e Abreu (2014), a sua origem data do "(...) final dos anos 80, a partir de uma encomenda do governo britânico, que não estava satisfeito com o nível de qualidade dos serviços de TI a ele prestado" (Fernandes; Abreu, 2014, p. 225-226). Segundo estes autores, ao longo dos anos, este *framework* foi recebendo atualizações, por exemplo, em 2007 foi lançado a terceira versão, denominada de ITIL V3 e, em julho de 2011, esta versão foi atualizada, surgindo a ITIL 2011 (*Cf*. Fernandes; Abreu, 2014, p. 226).

De maneira semelhante ao COBIT, em função do ano de publicação do livro de Fernandes e Abreu, versão atual da ITIL, denominada ITIL 4, lançada em 2019 pela *joint venture* AXELOS (2019), não foi considerada. Esta versão disponibiliza as práticas mais atuais para o gerenciamento das operações/serviços de TI:

---

[19] "(…) set of concepts and techniques for managing IT infrastructures, as well as the development and installation of new computer systems and IT operations". Kirk Rehage; Steve Hunt; Fernando Nikitin. Developing the IT Audit Plan. *In*.: **The Institute of Internal Auditors**, 2008, p. 7. (*Tradução nossa!)*

[20] "(…) it establishes a common vocabulary of defined and widely used terms. Organizations that implement ITIL concepts have claimed a higher degree of reliability and lower delivery costs". Kirk Rehage; Steve Hunt; Fernando Nikitin. Developing the IT Audit Plan. *In*.: **The Institute of Internal Auditors**, 2008, p. 8. (*Tradução nossa!)*

> ITIL 4 fornece a orientação necessária para que as organizações enfrentem novos desafios de gestão de serviços e utilizem o potencial da tecnologia moderna. Ele foi projetado para garantir um sistema flexível, coordenado e integrado para a governança e gestão eficazes de serviços de TI[21] (AXELOS, 2019, p. 14).

Em relação a estrutura da ITIL, serão utilizados os modelos e estruturas da versão da ITIL 4, disponibilizados no documento denominado "ITIL® Foundation: ITIL 4 Edition", publicado pela AXELOS (2019). Nesse item do Trabalho de Graduação será demonstrado a principal estrutura da ITIL 4, denominado como sistema de valor de serviços (SVS).

Para o AXELOS (2019), o SVS da ITIL 4 pode ser definido como um "(...) modelo operacional para a criação, entrega e melhoria contínua de serviços. É um modelo flexível que define seis atividades principais que podem ser combinadas de diversas maneiras, formando múltiplos fluxos de valor"[22] (AXELOS, 2019, p. 14).

De acordo com Hernan Aranda, em artigo publicado no Portal Invgate, em 17 de outubro de 2025, intitulado "O que é o Sistema de Valor de Serviço (SVS) na ITIL 4?", destaca-se que o SVS da ITIL 4:

> (...) conecta todas as partes do Gerenciamento de Serviços (pessoas, processos, ferramentas, governança e esforços de melhoria) em um sistema que suporta a criação de valor por meio de serviços de TI. (...) O SVS mostra como uma organização transforma a demanda (como necessidades ou solicitações do usuário) em resultados (como serviços de TI confiáveis, suporte ou produtos digitais) (Aranda, 2025).

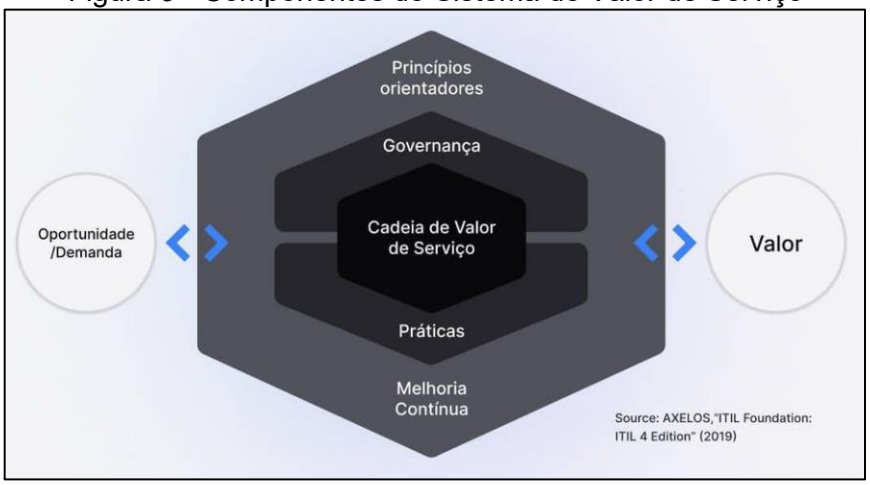
Aranda disponibiliza o modelo dos componentes do SVS, conforme a Figura 9:

---

[21] "ITIL 4 provides the guidance organizations need to address new service management challenges and utilize the potential of modern technology. It is designed to ensure a flexible, coordinated and integrated system for the effective governance and management of IT-enabled services". AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 14 (*Tradução nossa!)*

[22] "(...) operating model for the creation, delivery, and continual improvement of services. It is a flexible model that defines six key activities that can be combined in many ways, forming multiple value streams". AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 14 (*Tradução nossa!)*

Figura 9 - Componentes do Sistema de Valor de Serviço



Fonte: AXELOS, 2019, p. 55 *Apud* Aranda, 2025

Em relação aos princípios orientadores, Aranda (2025) informa que eles "(...) são recomendações práticas que influenciam o comportamento das equipes e funções, mesmo fora da TI. Eles ajudam as pessoas a tomarem decisões consistentes sem a necessidade de instruções detalhadas" (Aranda, 2025).

AXELOS (2019) lista 7 princípios orientadores[23], os quais incorporam as mensagens centrais da ITIL e do gerenciamento de serviços em geral, apoiando ações bem-sucedidas e boas decisões de todos os tipos e em todos os níveis"[24] (AXELOS, 2019, p. 59).

Outro ponto crucial é a sua conexão com os outros *frameworks*, dentre eles o "(…) Lean, Agile, DevOps e COBIT. Isso permite que as organizações integrem efetivamente o uso de múltiplos métodos em uma abordagem geral de gerenciamento de serviços"[25] (AXELOS, 2019, p. 59).

Em relação a Governança, tal componente está explicitamente vinculada à Governança de TI:

> (...) O corpo diretivo pode adotar os princípios orientadores da ITIL e adaptá-los, ou definir seu próprio conjunto específico de princípios e

[23] Focus on value; Start where you are; Progress iteratively with feedback; Collaborate and promote visibility; Think and work holistically; Keep it simple and practical; Optimize and automate. AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 58-59

[24] "(...) embody the core messages of ITIL and of service management in general, supporting successful actions and good decisions of all types and at all levels". AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 59 (*Tradução nossa!)*

[25]"(…) Lean, Agile, DevOps, and COBIT. This allows organizations to effectively integrate the use of multiple methods into an overall approach to service management". AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 59 (*Tradução nossa!)*

> comunicá-los a toda a organização. O corpo diretivo também deve ter visibilidade dos resultados das atividades de melhoria contínua e da mensuração do valor para a organização e seus stakeholders[26] (AXELOS, 2019, p. 81).

No tocante a algumas atividades exercidas pela Governança de TI no SVS, Aranda (2025) cita, alguns exemplos, tais como: “aprovação de orçamentos de TI com base no desempenho do serviço; definir políticas de acesso para serviços em nuvem; e verificar se um novo fornecedor atende aos padrões de segurança” (Aranda, 2025).

Para AXELOS (2019), a Cadeia de Valor de Serviço é o componente principal do SVS, no qual compõe um “(...) um modelo operacional que descreve as principais atividades necessárias para responder à demanda e facilitar a realização de valor por meio da criação e gestão de produtos e serviços”[27] (AXELOS, 2019, p. 82). Neste sentido, Aranda complementa esta lista de ações e descreve seis tipos de atividades que as organizações realizam para fornecer serviços: Planejar; Melhorar; Envolver-se; Projetar e fazer a transição; Obter/construir; e Fornecer e dar suporte (*Cf*. Aranda, 2025).

É importante ressaltar que a Cadeia de Valor de Serviços substituiu o antigo - porém, muito conhecido -, modelo de Ciclo de Vida do Serviço, que é um dos pontos principais da ITIL V3. Tal modelo ainda pode ser utilizado atualmente nas empresas, pois as diretrizes inclusas neste modelo ainda são válidas; entretanto, segundo Vawns Murphy, no artigo intitulado “A Cadeia de valor de Serviço da ITIL”, publicado no Portal ManageEngine (2025), informa que, apesar de seus benefícios, a estrutura imposta pela ITIL V3 possuía algumas limitações: “(...) a maioria das pessoas via o ciclo de vida dos serviços da ITIL v3 como muito linear (...)” (Murphy, 2025). Assim, com o advento das novas tecnologias que vêm sendo implementadas ao longo dos anos, as empresas devem se adaptar a tal fenômeno, conforme argumenta Murphy:

> (...) a cadeia de valor de serviços é uma maneira de se adaptar a isso e, ao apoiar a agilidade e a estrutura, essa cadeia permite que os departamentos de TI entendam melhor, planejem e gerenciem as

---

[26] (…) the governing body can adopt the ITIL guiding principles and adapt them, or define its own specific set of principles and communicate them across the organization. The governing body should also have visibility of the outcomes of continual improvement activities and the measurement of value for the organization and its stakeholders”. AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 81 (*Tradução nossa!)*

[27] “(…) an operating model which outlines the key activities required to respond to demand and facilitate value realization through the creation and management of products and services. AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 82 (*Tradução nossa!)*

> atividades necessárias para criar valor por meio dos seus serviços, levando a uma prestação de serviços melhor, mais rápida e segura e a uma experiência aprimorada do cliente (Murphy, 2025).

Sobre a categoria “Práticas”, a Empresa AXELOS (2019) as define como “(...) um conjunto de recursos organizacionais projetados para executar trabalho ou atingir um objetivo”[28] (AXELOS, 2019, p. 105). Elas são categorizadas e segregadas em três grupos, por meio dos quais há “(...) 14 práticas de gerenciamento geral, 17 práticas de gerenciamentos de serviços e 3 práticas de gerenciamento teórico”[29] (AXELOS, 2019, p. 105).

Pode-se entender que tais práticas propõem as melhores maneiras para que colaboradores e o departamento de TI possa realizar as suas atividades, como o tratamento de incidentes e o desenvolvimento de softwares, por exemplo. Phyllis Drucker, no artigo “Entendendo as práticas de gerenciamento da ITIL 4”, publicado no Portal EngineManage (2025), diz que a adoção de tais práticas “(...) permitem que as organizações construam um modelo operacional que atravessa silos departamentais, incentivando as unidades de negócio, incluindo a TI, a trabalhar em conjunto para agregar valor” (Drucker, 2025).

No que se refere à categoria “Melhoria Contínua”, a Empresa AXELOS (2019) informa que:

> (...) ocorre em todas as áreas da organização e em todos os níveis, do estratégico ao operacional. Para maximizar a eficácia dos serviços, cada pessoa que contribui para a prestação de um serviço deve ter em mente a melhoria contínua e estar sempre em busca de oportunidades de aprimoramento[30] (AXELOS, 2019, p. 92).

Aranda cita alguns exemplos para a melhoria contínua, dentre eles:

> Revisar as categorias de tickets a cada trimestre para reduzir as solicitações mal encaminhadas;
> Ajustar os SLAs após o feedback dos usuários;
> Usar dados de desempenho para propor um novo recurso de

---

[28] “(…) a set of organizational resources designed for performing work or accomplishing an objective (…)”. AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 105 (*Tradução nossa!)*

[29] “(...)14 general management practices, 17 service management practices, and three technical management practices (…)”. AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 105 (*Tradução nossa!)*

[30] “(…) takes place in all areas of the organization and at all levels, from strategic to operational. To maximize the effectiveness of services, each person who contributes to the provision of a service should keep continual improvement in mind, and should always be looking for opportunities to improve”. AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 92 (*Tradução nossa!)*

autoatendimento (Aranda, 2025).

Por fim, para os três últimos componentes do SVS, AXELOS define a categoria "Oportunidade" como "(...) opções ou possibilidades de agregar valor às partes interessadas ou melhorar a organização"[31] (AXELOS, 2019, p. 57). A categoria "Demanda" é representado como "(...) a necessidade ou desejo por produtos e serviços de clientes internos e externos"[32] (AXELOS, 2019, p. 57-58). Quanto à categoria "Valores" define-se como "(...) o entendimento de que o valor está sujeito à percepção das partes interessadas, sejam elas clientes ou consumidores de um serviço, ou parte da(s) organização(ões) prestadora(s) de serviços"[33] (AXELOS, 2019, p. 20).

Com a estrutura da ITIL 4 definida, pode-se observar a sua complexidade, bem como a alta quantidade de diretrizes e boas práticas que o *framework* disponibiliza. Através de sua aplicação, as empresas podem esperar diversos benefícios; Fernandes e Abreu (2014) dizem que "a adoção das práticas da ITIL pretende levar uma organização a um grau de maturidade e qualidade que permita o uso eficaz e eficiente dos seus ativos estratégicos de TI (...)" (Fernandes; Abreu, 2014, p. 227).

De acordo com o Portal Blog Impacta (2017), em publicação de 2017 intitulada "ITIL e Cobit: entenda as principais diferenças e suas aplicações", afirma que os benefícios da implantação da ITIL impactam diretamente na Governança de TI, no qual é informado que:

> Se implantado corretamente, após um estudo de viabilidade, a ITIL beneficia diretamente a governança de TI e a forma como a área se relaciona com o restante da organização. E ainda proporciona, entre outras coisas:
> redução do tempo de execução de tarefas e de solução de problemas;
> aumento da satisfação de usuários e clientes;
> maior controle da gestão;
> diminuição de custos operacionais (Portal Blog Impacta, 2017).

Pode-se notar que as diretrizes e componentes da ITIL não citam diretamente os controles internos, nem a SOX. Entretanto, tal fato não diminui a importância da

---

[31] "(...) options or possibilities to add value for stakeholders or otherwise improve the organization". AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 57 (*Tradução nossa!)*

[32] "(…) the need or desire for products and services from internal and external customers". AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 57-58 (*Tradução nossa!)*

[33] "(…) is the understanding that value is subject to the perception of the stakeholders, whether they be the customers or consumers of a service, or part of the service provider organization(s)" AXELOS. **ITIL® Foundation**: ITIL 4 Edition, 2019, p. 20 (*Tradução nossa!)*

ITIL para o gerenciamento dos riscos e para os controles internos de TI. Através do gerenciamento adequado das operações de TI é possibilitado às empresas a garantia de que as suas atividades serão executadas corretamente, atestando, assim, a eficácia dos controles internos de TI e beneficiando a empresa em sua totalidade. Assim, conforme apresentado neste item, o uso contínuo do COBIT e ITIL é altamente recomendável.

É importante sublinhar que os modelos e estruturas apresentados ao longo deste Trabalho de Graduação representam os principais conceitos destes *frameworks*. Entretanto, devido a sua extensão e ampla gama de informações que o COBIT e a ITIL possuem, para que a sua aplicação seja realizada de maneira adequada, o autor deste Trabalho de Graduação recomenda a leitura dos guias/manuais dos dois *frameworks*, a fim de implementar adequadamente um modelo de gerenciamento de riscos e de controles internos de TI.

Outro ponto importante é que a aplicação e a manutenção destes *frameworks* devem ser acompanhadas e incentivadas pelos colaboradores e gestores, não apenas do departamento de TI, mas para toda a empresa. Os *frameworks*, em si, não irão resolver imediatamente os problemas e incidentes relacionados ao gerenciamento das operações/serviços. Entretanto, irão estabelecer bases e fundamentos para que tais operações sejam realizadas adequadamente, de modo que o departamento de TI e a Governança de TI consigam apoiar e suportar as operações das áreas de negócios.

Ao longo desta Seção foram apresentadas a relação, a importância do departamento de TI com as áreas de negócios e com a SOX. Através de seus colaboradores, executivos (CIO, por exemplo), *frameworks* e práticas indicadas, pode-se entender que o departamento de TI é responsável direta e indiretamente pela integridade das informações constantes nos relatórios financeiros das empresas. Além disso, foi realçado que, mediante a Governança de TI e o uso dos frameworks destacados, cooperam no gerenciamento e nas operações de TI e, consequentemente, minimiza os riscos envolvidos nessas operações.

No entanto, há dois fatores cruciais que ainda devem ser esclarecidos: Como que um risco de TI é categorizado?” Quais são os controles internos para mitigá-los? Dessa forma, nos próximos itens desta Seção, serão apresentados os principais riscos e controles internos de TI.

5.3. Riscos e Controles Internos de TI

Conforme explicitado, a Tecnologia da Informação é considerada um dos pilares para o bom funcionamento de uma empresa, pois, além de estabelecer a infraestrutura para que as áreas de negócios executem as suas operações/atividades (através dos sistemas, banco de dados etc.), ela também garante a integridades e a autenticidade das informações emitidas pela empresa. Contudo, apesar dos diversos benefícios que o uso da TI oferece, em contrapartida, também pode incidir em riscos, os quais as empresas devem monitorar e gerenciar.

Em documento publicado pela IIA, em 2012, denominado “Global Technology Audit Guide 1: Riscos e Controles de Tecnologia da Informação – 2ª Edição”, indica os riscos que podem ser causados à empresa pelo uso da TI:

> Embora a tecnologia proporcione oportunidades de crescimento e desenvolvimento, ela também representa ameaças, como disrupção, roubo e fraude. Pesquisas mostram que agressores externos ameaçam organizações, mas pessoas de confiança são uma ameaça muito maior. Felizmente, a tecnologia também pode fornecer proteção contra ameaças (...) (IIA, 2012, p. 3).

Dessa forma, é possível realizar a análise de que diante das novas tecnologias implementadas ao longo dos anos, tais como o uso da IA (Inteligência Artificial) para a automatização das tarefas e a substituição do uso de servidores locais para os servidores online (*On-Cloud*), acabam proporcionando novos riscos para as empresas, os quais devem ser propostos mecanismos para reduzir e/ou eliminar completamente os seus impactos.

Fernandes e Abreu (2014) ressaltam que, com o advento da internet, houve impactos na gestão e na infraestrutura de TI, exemplificando que a operação da empresa “(...) sofre riscos diários de intrusão visando o “roubo” de dados e a disseminação de códigos maliciosos e vírus (...)” (Fernandes; Abreu, 2014, p. 9).

No documento publicado pela IIA, em 2013, denominado “Global Technology Audit Guide 4: Management of IT Auditing: 2nd Edition” afirma que “os riscos de TI continuam a mudar à medida que a tecnologia evolui. Alguns desses riscos estão relacionados à própria tecnologia e outros à maneira como a empresa utiliza a TI”[34] (IIA, 2013, p. 2)

---

[34] “IT risks continue to change as technology evolves. Some of these risks are related to the technology itself and some to the manner in which the business uses IT”. The Institute of

Na Seção anterior, especificamente no item 4.1 deste Trabalho de Graduação, foi definido risco e como gerenciá-lo. Entretanto, a definição utilizada levou em consideração a empresa em sua totalidade, em que as áreas de negócios e a de Governança Corporativa estavam inclusas. A fim de responder como os riscos de TI são categorizados, sob o fundamento teórico-conceitual do documento publicado pela ISACA (Information Systems Audit and Control Association), em 2020, "Risk IT Framework: 2nd Edition", pode-se definir risco de TI como:

> o conceito de risco, quando considerado no contexto da tecnologia da informação e cibersegurança, refere-se a um vocabulário extenso, incluindo ameaças e vulnerabilidades, apetite e tolerância ao risco, impacto, priorização e resposta, entre muitos outros termos que são fundamentais para as disciplinas de governança, gestão e avaliação de riscos em tecnologia da informação[35] (ISACA, 2020, p. 9)

De acordo com documento publicado pela IBGC, em 2007, sob o título "Guia de Orientação para Gerenciamento de Riscos Corporativos", os riscos de TI podem ser representados por alguns exemplos:

> (...) falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais). Pode estar também associado a erros ou fraudes, internas ou externas, nos sistemas informatizados ao capturar, registrar, monitorar e reportar corretamente transações ou posições (IBGC, 2007, p. 19).

Conforme se constante, há uma grande quantidade de exemplos em que um risco de TI pode se categorizar. Não obstante, esta tarefa pode-se provar bem complexa, pois vários fatores devem ser considerados, entre eles a área de atuação da empresa, o tamanho da empresa, o grau de comprometimento dos executivos com o gerenciamento dos riscos, a estrutura e área/ambiente do departamento de Governança de TI.

Segundo a ISACA (2020), o risco de TI não estará sempre "exposto" para a

---

Internal Auditors. **Global Technology Audit Guide 4**: Management of IT Auditing: 2nd Edition, 2013, p. 2 (*Tradução nossa!)*

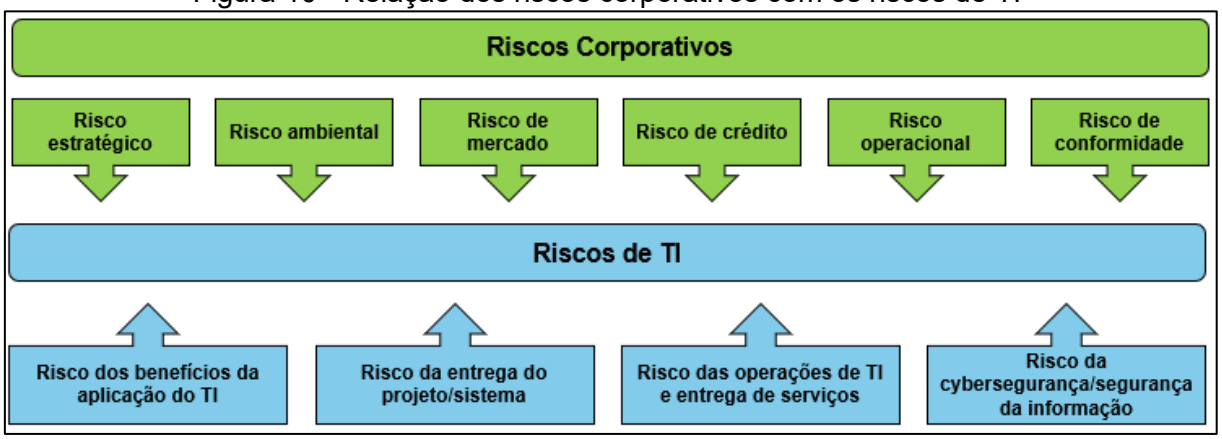
[35] "The concept of risk—when considered in the context of information technology and cybersecurity—references an extensive vocabulary, including threats and vulnerabilities, risk appetite, tolerance, impact, prioritization and response, among many other terms that are critical to the disciplines of risk governance, management and assessment of information technology". ISACA. **Risk IT Framework**: 2nd Edition, 2020, p. 9 (*Tradução nossa!)*

empresa, ou seja, visto que pode este surgir ao longo das execuções das atividades diárias:

> Em uma empresa típica em um dia típico, atividades relacionadas a TI, organizadas em processos de TI, são realizadas. Eventos ocorrem de forma contínua: decisões importantes sobre tecnologia precisam ser tomadas, reparos para incidentes operacionais devem ser aplicados, problemas de software precisam ser resolvidos e aplicativos devem ser desenvolvidos. Cada um desses eventos envolve tanto risco quanto oportunidade[36] (ISACA, 2020, p. 20).

Dessa forma, partindo deste pressuposto, pode-se chegar ao entendimento que os riscos de TI, embora distintos e diferentes dos riscos corporativos, possuem uma importante conexão, cujas vulnerabilidades podem impactar a empresa em sua totalidade. A ISACA (2020) fornece um modelo em que combina estes dois tipos diferentes de riscos, conforme ilustra a Figura 10:

Figura 10 - Relação dos riscos corporativos com os riscos de TI



Fonte: Adaptado da Figura 1.1 de ISACA, 2020, p. 14

Dentre os riscos de TI informados na Figura 10, a ISACA (2020) destaca a dificuldade de classificar os riscos envolvendo as operações de TI e a Cybersegurança/Segurança da Informação, bem como o seu devido monitoramento, pois eles contemplam uma alta gama de "(...) características específicas e únicas. Eles podem envolver qualquer número de tecnologias especializadas, agentes de ameaça, erros humanos, vetores de ataque, falhas de controle e vulnerabilidades de

[36] "In a typical enterprise on a typical day, I&T-related activities, organized in I&T processes, are deployed. Events occur on a nonstop basis: Important technology choices must be made, repairs for operational incidents must be applied, software problems need to be addressed and applications must be built. Each of these events carries both risk and opportunity". ISACA. **Risk IT Framework**: 2nd Edition, 2020, p. 20 (*Tradução nossa!)*

softwares”[37] (ISACA, 2020, p. 15).

Além disso, a ISACA (2020) destaca que o entendimento da “causa raiz” dos riscos de TI envolvendo a Cybersegurança/Segurança da Informação não podem estar limitados somente a tecnologia em si (sistemas, por exemplo), mas que o fator humano se prepondera, visto que “(...) muitos eventos de risco que chamam atenção começam com erros humanos cometidos por pessoas reais”[38] (ISACA, 2020, p. 15).

Com a definição dos riscos de TI e as suas respectivas categorizações, pode-se notar a complexidade e o alto de grau de importância/dedicação que a empresa deve dar ao tema. O IIA (2012) ressalta tal ponto, informando que os riscos de TI “(...) são apenas uma parte da complexa interconectividade geral que existe entre pessoas, processos, infraestrutura e o ambiente de riscos corporativos, e que deve ser gerida como um todo pela organização” (IIA, 2012, p. 5).

Conforme foi ressaltado neste Trabalho de Graduação, a Governança de TI dispõe de vários *frameworks* para a execução do gerenciamento dos riscos de TI e que o uso do COBIT combinado com a ITIL fornece as melhores diretrizes e práticas para realização desta atividade. Por fim, foi salientado que, através do uso do COSO ERM, as empresas conseguem estabelecer mecanismos para a mitigação dos riscos identificados, no qual foi sublinhado o uso dos controles internos. Entretanto, antes de ser feito o entendimento sobre os controles internos de TI, é necessário entender quais fatores levam à sua implementação.

O IIA (2012) fornece um passo a passo na identificação e na análise dos riscos de TI:

> (...) Normalmente, começa com a identificação de eventos ou circunstâncias particulares relevantes para os objetivos da organização (ex., os riscos de violações de dados), avaliando-os em termos de probabilidade e magnitude do impacto (ex., o risco inerente a uma violação de dados é classificado como alto e o impacto também é classificado como alto), determinando uma resposta (ex., novas políticas para proteger melhor os dados da organização) e monitorando o progresso da implementação de respostas (ex., a implementação de novas medidas de segurança pela atividade de TI para evitar violações de dados) (...)” (IIA, 2012, p. 11).

---

[37] “(...) specific, unique characteristics. They can involve any number of specialized technologies, threat actors, human errors, attack vectors, control failures and software vulnerabilities”. ISACA. **Risk IT Framework**: 2nd Edition, 2020, p. 15 (*Tradução nossa!)*

[38] “(...) many headline-grabbing risk events begin with human errors by real people”. ISACA. **Risk IT Framework**: 2nd Edition, 2020, p. 15 (*Tradução nossa!)*

Dessa forma, com os riscos de TI identificados e analisados, é necessário meios para mitigá-los, daí a importância de recorrer ao funcionamento dos controles internos de TI. Foi declarado na Seção 4 deste Trabalho de Graduação que as empresas devem possuir cautela ao estabelecer os controles internos, e que deve ser realizado uma avaliação de seu custo/benefício, além do esforço para implementá-lo e mantê-lo em funcionamento; porém, ainda que estes aspectos chamem a atenção, os controles internos são considerados as melhores opções para controlar/mitigar os riscos de TI identificados. Neste momento, o foco será concentrado nos controles internos de TI, como são estruturados e como podem garantir a integridade das operações das empresas.

Segundo o IIA (2012), o escopo dos controles internos de TI contempla "(...) os processos que prestam avaliação das informações e serviços de informação e ajudam a controlar ou mitigar os riscos associados ao uso da tecnologia por uma organização" (IIA, 2012, p. 16). Pode-se associar a importância dos controles internos de TI com a Governança Corporativa e com a SOX. Neste sentido, IIA (2012) afirma que eles "(...) são essenciais para proteger ativos, clientes, parceiros e informações confidenciais; demonstrar um com portamento seguro, eficiente e ético; e preservar a marca, a reputação e a confiança" (IIA, 2012, p. 3).

Em relação a aplicabilidade dos controles internos de TI, o IIA (2012) destaca a sua importância, pois:

> (...) prestam avaliação quanto à confiabilidade das informações e dos serviços de informação. Os controles de TI ajudam a reduzir os riscos associados ao uso da tecnologia por uma organização. Eles variam de políticas corporativas à sua implementação física dentro de instruções codificadas; da proteção do acesso físico até a capacidade de rastrear ações e transações aos indivíduos responsáveis; e de edições automáticas até análises de razoabilidade para grandes conjuntos de dados (IIA, 2012, p. 4).

Assim, pode-se compreender que a aplicação dos controles de TI abrange várias áreas e departamentos, desde as operações das áreas de negócios, do próprio departamento de TI e na garantia da segurança da informação, no qual se enquadra desde dados sigilosos da empresa até informações privativas de clientes e fornecedores. O IIA (2012) corrobora que o departamento de TI "(...) inclui componentes de tecnologia, processos, pessoas, organização e arquitetura, bem como a própria informação. Muitos controles de TI são de natureza técnica e a TI

fornece as ferramentas para muitos controles de negócios” (IIA, 2012, p. 3).

Para o atendimento destes departamentos e operações, os controles internos de TI, segundo IIA, tem oito classificações (2012, p. 16), que serão descritas neste item do Trabalho de Graduação.

Quanto aos controles internos de TI, o IIA (2012) informa que:

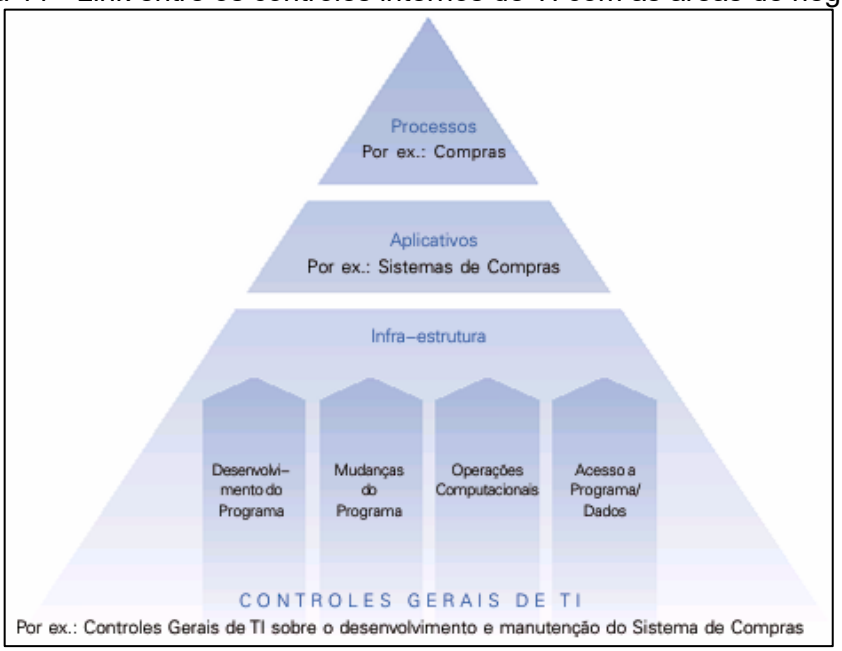
> (...) devem fazer parte dos principais processos de TI relacionados ao planejamento, organização, aquisições, mudanças, entrega de serviços de TI e suporte e monitoramento de TI. Os controles de TI que apoiam uma ampla gama desses processos de TI normalmente seriam os controles de infraestrutura de TI, que cobrem áreas como controles de rede, controles de banco de dados, controles do sistema operacional e controles de hardware, por exemplo. Os controles de TI que cobrem aplicativos e, em muitos casos, áreas de negócios importantes podem incluir controles de edição de entradas, controles de conclusão ou conciliação de processos e controles de reporte de exceções (...) (IIA, 2012, p. 13).

Conforme visto, as operações e serviços executados e mantidos pelo departamento de TI impactam diretamente na integridade nas operações realizadas pelas áreas de negócios, as quais devem ser levadas em consideração no processo de desenvolvimento dos controles internos, segundo recomenda a Consultoria KPMG (2006), em “Seção 404 da Lei Sarbanes-Oxley: Certificação dos Controles internos pela Administração”:

> Considerando que os aplicativos de TI frequentemente suportam o início, a autorização, o registro, o processamento e a divulgação de transações financeiras, os controles de TI podem representar uma parte integrante do ICOFR. Os aplicativos relacionados aos relatórios financeiros e contábeis constantemente, são sustentados por sistemas legados ou auxiliares que fornecem dados financeiros críticos, e muitas das empresas precisam ter um alto nível de confiança em um grande número de aplicativos para alcançar os seus objetivos (Portal da Consultoria KPMG, 2006, p. 6)

A relação entre os controles internos de TI e as operações das áreas de negócios pode ser vislumbrada na Figura 11:

Figura 11 - Link entre os controles internos de TI com as áreas de negócios



Fonte: Portal da Consultoria KPMG, 2006, p. 7

Na Figura 11 pode-se observar o termo “Controles Gerais de TI”, que se trata de uma classificação dos controles internos de TI, que, em breve, será esmiuçado.

Por fim, em relação à segurança da informação, a IIA (2012) a descreve como “(...) parte integrante dos controles de TI. A segurança das informações aplica-se à infraestrutura e aos dados e é a base para a confiabilidade da maioria dos outros controles de TI” (IIA, 2012, p. 21).

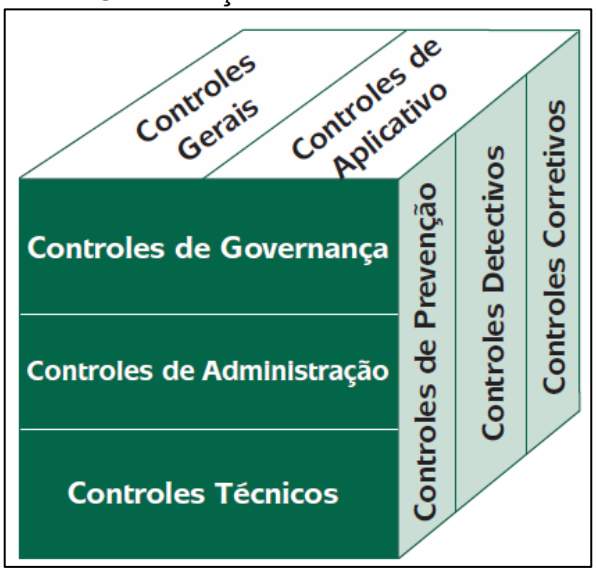
A Cibersegurança/Segurança da Informação contempla riscos preocupantes em relação não só ao TI, mas para a empresa na sua totalidade, pois com o advento e avanço das novas tecnologias, caso as empresas não implementem meio para controlar/mitigar tais riscos, elas podem ficar suscetíveis a possíveis fraudes e ataques cibernéticos de hackers, inclusive colocando em risco dados pessoais e sensíveis de colaboradores, fornecedores, clientes, conforme nos alerta a Lei 13.709/2018, a LGPD (Lei Geral de Proteção de Dados), que estabelece diretrizes para o tratamento e armazenamento destes dados e cria punições, como multas, se tais diretrizes não forem cumpridas, o que corrobora a importância do departamento de TI e da Segurança da Informação[39], pois têm um vínculo direto com os controles internos de TI.

[39] Reforça-se que os pilares da Segurança da Informação estão assentados na Confidencialidade, Integridade e Disponibilidade, conforme testifica documento produzido pelo IIA (Cf. 2012, p. 21-22).

Diante das relações apresentadas, pode-se notar que os controles internos de TI atendem e mitigam vários riscos nas operações das empresas. Dessa forma, tal classificação pode “(...) ajudar a entender seus propósitos e onde eles se encaixam no sistema geral de controles internos (...) (IIA, 2012, p. 16). Neste mesmo documento produzido pelo IIA informa que “compreendendo essas classificações, o analista de controle e o auditor são mais capazes de estabelecer suas posições no *framework* de controle (...)” (IIA, 2012, p. 16).

A Figura 12 reporta a classificação dos controles internos de TI:

Figura 12 - Classificações dos controles internos de TI



Fonte: Figura 2 do IIA, 2012, p. 16

No Quadro 15, serão explicitados os tipos de controles internos de TI, com informações parcialmente transcritas das seções “6.1 Controles Gerais e de Aplicativos de TI” e “6.2 Governança de TI, Administração e Controles Técnicos” do documento produzido pela “The Institute of Internal Auditors (IIA)”:

Quadro 15 – Classificação dos controles internos de TI

Classificação	Descrição
Controles Gerais	Aplicam-se a todos os componentes, processos e dados de sistemas de uma determinada organização ou ambiente de sistemas. Os controles gerais incluem, mas não estão limitados à governança de TI, gerenciamento de riscos, gestão de recursos, operações de TI, desenvolvimento e manutenção de aplicativos, gestão de usuários, segurança lógica, segurança física, gerenciamento de alterações, backup e recuperação, e continuidade de negócios.
Controles de Aplicativos	Pertencem ao escopo de processos de negócios individuais ou sistemas de aplicativos, e incluem controles dentro de um aplicativo que gira em torno de entrada, processamento e saída. Os controles de aplicativo também podem incluir edições de dados, segregação de funções de negócios (ex., início de transação *versus* autorização), balanceamento dos totais de processamento, registro de transações e reporte de erros.
Controles Preventivos	Impedem que erros, omissões ou incidentes de segurança ocorram. Exemplos incluem edições de entradas de dados simples, que bloqueiam a inserção de caracteres alfabéticos em campos numéricos; controles de acesso, que protegem dados confidenciais ou recursos do sistema contra pessoas não autorizadas; e controles técnicos complexos e dinâmicos, como software antivírus, firewalls e sistemas de prevenção contra intrusões.
Controles Detectivos	Detectam erros ou incidentes que ultrapassam os controles preventivos. Por exemplo, um controle detectivo pode identificar números de conta de contas inativas ou que tenham sido sinalizadas para monitoramento de atividades suspeitas. Os controles detectivos também podem incluir monitoramento e análise, para descobrir atividades ou eventos que excedam os limites autorizados ou que violem os padrões de dados conhecidos, que possam indicar manipulação inadequada.
Controles Corretivos	Corrigem erros, omissões ou incidentes assim que são detectados. Eles variam desde a simples correção de erros na entrada de dados, até a identificação e remoção de usuários não autorizados ou software de sistemas ou redes para recuperação de incidentes, interrupções ou desastres.
Controles de Governança de TI	Envolve supervisionar o gerenciamento, princípios, políticas e processos eficazes da informação e garantir que estejam implementados e funcionando corretamente. Esses controles estão ligados aos conceitos de governança, que são orientados tanto por metas e estratégias organizacionais quanto por órgãos externos, como os reguladores.
Controles de Administração	A administração deve garantir que os controles de TI necessários para atingir os objetivos estabelecidos pela organização sejam aplicados e deve garantir um processamento confiável e contínuo. Esses controles são implantados como resultado de ações deliberadas da administração, em resposta a riscos para a organização, seus processos e ativos.
Controles Técnicos	Os controles técnicos geralmente formam a espinha dorsal do *framework* de controle da administração. Portanto, se os controles técnicos são fracos, o impacto afeta toda a estrutura de controle. Por exemplo, ao proteger contra acesso e invasão não autorizados, os controles técnicos fornecem a base para confiar na integridade da informação – incluindo evidências de todas as alterações e de sua autenticidade. Exemplos de controles técnicos são controles do sistema operacional, controles do banco de dados, criptografia e log.

Fonte: Informações adaptadas das seções “6.1 Controles Gerais e de Aplicativos de TI” e “6.2 Governança de TI, Administração e Controles Técnicos” (*Cf*. IIA 2012, p. 16-17)

Em relação a aplicação dos controles internos de TI, destacado no item 4.2 deste Trabalho de Graduação, é importante ressaltar que as classificações e exemplos de controles internos de TI e sua aplicabilidade informados não apenas no Quadro 15, mas ao longo desta Seção, são apenas recomendações das Referências pesquisadas, pois não são exigências para todas as empresas que desejam mitigar os seus riscos, a fim de atender as diretrizes da SOX. Dessa forma, cada empresa deve avaliar as suas necessidades e atividades, a fim de estabelecer um sistema de controles internos eficiente.

Acerca do teste/avaliação dos controles internos de TI, contemplado no item 4.2 deste Trabalho de Graduação, o documento produzido pelo IIA (2012) destaca que “a avaliação dos controles de TI é um processo contínuo. Os procedimentos de negócios mudam constantemente, à medida que a tecnologia continua evoluindo, e as ameaças surgem conforme novas vulnerabilidades são descobertas” (IIA, 2012, p. 14). Assim, pode-se entender que o departamento de TI e de Governança de TI estejam sempre atentos a quaisquer mudanças, internas e externas à empresa. Como foi sublinhado neste Trabalho de Graduação, o mercado atual é altamente volátil, e com a adoção de novas tecnologias, novas oportunidades de negócios surgirão, na mesma proporcionalidade os riscos também.

As mudanças implementadas no ambiente organizacional produzem alterações nos desenhos e nos testes dos controles internos de TI. Para evitar falhas e deficiências (gaps) nos testes executados pela Auditoria Interna e Auditoria Independente, a fim de garantir a integridade da emissão dos relatórios financeiros e que todas as operações da empresa estejam de acordo com as diretrizes da SOX, que estas preocupações não sejam restritas apenas ao departamento de TI e de Governança de TI, mas de todos os entes e departamentos constitutivos da empresa.

Por fim, é importante ressaltar que todas as práticas e diretrizes abordadas ao longo deste Trabalho de Graduação dependem de um importante fator para serem validadas, o fator ético-moral. Para que o cumprimento a SOX e o gerenciamento de riscos sejam atendidos, é necessário que a diretoria e todos os departamentos da empresa estejam dispostos a trabalhar de forma íntegra e harmônica; caso contrário, de nada adiantaria investir na infraestrutura da empresa ou na criação de vários controles internos, se as atividades internas se sucumbirem às eventuais fraudes humanas.

6 CONCLUSÃO

Este Trabalho de Graduação teve como objetivo descrever a importância e as diretrizes da Governança Corporativa e da Lei Sarbanes-Oxley (SOX) para as organizações empresariais, especificando que, para que este objetivo possa ser alcançado, prescinde da atuação do departamento de TI e suas áreas, colaboradores e *frameworks*, atuando desde o suporte as operações de negócios, até a mitigação de riscos e a criação de controles internos.

Por meio da pesquisa bibliográfico-documental realizada, foi observada a importância e a amplitude de operações e serviços que envolvem o departamento de TI, cuja execução impacta diretamente nas operações realizadas pelas áreas de negócios das empresas. Com a evolução e a produção constante de novas tecnologias, as operações e atividades que, eram realizadas manualmente, sejam migradas à automatização; desta forma, o bom uso e a otimização da estrutura do departamento TI tornam-se fundamentais para as empresas que querem se adequar à SOX, sobretudo às de capital aberto; por outro lado, as demais empresas que não tenham esta pretensão, a fim de garantir a integridade de seus sistemas e a segurança das operações de seus respectivos serviços, salientou-se, neste Trabalho de Graduação, a necessidade de uma interrelação entre Governança Corporativa e Governança de Tecnologia da Informação, visto que o departamento de TI está diretamente associado a todas as operações das empresas, passa, com efeito, a ser parte integrante de todo o processo interno e externo da organização empresarial. Daí a necessidade das empresas e, principalmente, das instituições de ensino, no processo formativo gerencial e de Tecnologia da Informação, tratarem desta importante temática.

Além dos dados pesquisados, mediante investigação teórico-conceitual, a prática como profissional de Tecnologia da Informação, obtida pela realização de tarefas em variadas empresas, são as fontes inspiradoras destas análises. Graças aos desafios enfrentados no cotidiano das empresas e na aquisição das experiências vivenciadas, por meio de competências, habilidades e certificações sobre a temática, foi possível atestar e, ao mesmo tempo, compatibilizar a realidade empírica vivida no ambiente interno das empresas e o conteúdo descrito por diferentes autores e autoras lidos e consultados nesta pesquisa bibliográfico-documental.

A princípio, este Trabalho de Graduação visava realizar um estudo de caso, mediante o qual, objetivava entrevistar colaboradores do departamento de Governança Corporativa e de Governança de TI, onde este autor trabalha. Entretanto, esta opção foi descartada, pois as informações relacionadas à SOX e afins são consideradas confidenciais pelo corpo diretivo, o que impedem a publicidade destes dados.

Foi ainda considerada a possibilidade de realizar um estudo de caso com estudantes dos Cursos Superiores de Tecnologia em Análise e Desenvolvimento de Sistemas e de Segurança da Informação, da Fatec Americana – Ministro Ralph Biasi. Não obstante, ao analisar criteriosamente os Projetos Pedagógicos destes cursos, notou-se que havia poucas disciplinas que abordavam este tema, o que incidiria diretamente nos resultados, tendo em vista que poucos universitários possuem conhecimento sobre a SOX e o vínculo dela com TI, no tocante à preservação da integridade das operações e como isso impacta nos resultados financeiros das empresas.

Sendo assim, espera-se que este Trabalho de Graduação, em função da importância do tema abordado, possa contribuir para o debate acadêmico e profissional, ao delinear as bases para futuras pesquisas envolvendo a relação da SOX e TI, no intuito de i) avaliar o nível de conhecimento dos colaboradores e executivos de empresas no cumprimento das diretrizes da SOX; e de ii) enfatizar a imprescindibilidade deste conhecimento técnico-operacional, que vincula à TI às legislações, nacionais e internacionais, entre elas a SOX, e que respalda a conduta profissional, principalmente para quem pretende ingressar no cursos relacionados à Tecnologia da Informação e, posteriormente, ingressar neste mercado de trabalho.

Além disso, espera-se que, a partir deste Trabalho de Graduação, as instituições brasileiras de ensino compreendam a importância da SOX, da Governança Corporativa e da Governança de TI, além de dar notoriedade a algumas disciplinas que tratam deste assunto, tais como Ética e Responsabilidade Profissional, Cidadania Digital, Sociologia (Sociedade, Tecnologia e Inovação), Auditoria etc., disponibilizando mais disciplinas na matriz curricular e, se possível, o aumento da carga horária para refletir tais temas e propor as boas diretrizes e práticas no processo de construção dos valores ético-morais, no desenvolvimento e apreço do caráter, da índole e na lisura nas ações e nas tomadas de decisões de seus egressos.

REFERÊNCIAS

ANDRADE, Adriana; ROSSETTI, José Paschoal. **Governança corporativa**: fundamentos, desenvolvimento e tendências. São Paulo: Atlas, 2004.

ANDRADE, Inacilma Rita Silva. Auditoria operacional: uma questão de sobrevivência para micros e pequenas empresas. *In*: ENCONTRO NORDESTINO DE CONTABILIDADE, IV, 1999. Salvador. Anais. Salvador, CRC-CE, 1999. CD-ROM.

ARANDA, Hernan. O que é o Sistema de Valor de Serviço (SVS) na ITIL 4?, 3 jul. 2025. *In*.: **Portal INVGATE**, 2025. Disponível em: https://invgate.com/pt/itsm/itil/service-value-system. Acesso em: 8 out. 2025, às 19h32min.

ARRIVABENE, Adriano. Análise do impacto nos processos operacionais de tecnologia da informação de uma empresa do ramo financeiro adequados às exigências da lei Sarbanes-Oxley. **Universidade Nove de Julho**: Biblioteca Digital de Teses e Dissertações, 2012. Disponível em: https://bibliotecatede.uninove.br/handle/tede/175. Acesso em: 10 set. 2025, às 19h29min.

ARRIVABENE, Adriano; SASSI, Renato Jose; ANDRELO, Pamela Ferreira Alves; MOURA, Maria Luiza Almeida de Oliveira. Análise do impacto da adequação nos processos operacionais de tecnologia da informação às exigências da lei Sarbanes-Oxley em empresa do ramo financeiro. **Research, Society and Development**, v. 10, n. 1, p. e7710111374-e7710111374, 2021. Disponível em: https://rsdjournal.org/rsd/article/view/11374. Acesso em: 9 set. 2025, às 19h21min.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 38500**: Tecnologia da informação: Governança da TI para a organização. 2ª. ed. Rio de Janeiro, 2018.

AXELOS. ITIL® Foundation: ITIL 4 Edition. **Axelos**: Global best practice. 2ª. ed. London, England, 2019. Disponível em: https://abim.go.ug/sites/files/%28ITIL%29%20Axelos%20-%20ITIL%20Foundation%204%20edition-Axelos%20%282019%29%5B1%5D.pdf. Acesso em: 30 set. 2025, às 20h50min.

AZIZ, Nor Azimah Abdul. Managing corporate risk and achieving internal control through statutory compliance. **Journal of Financial crime,** v. 20, n. 1, p. 25-38, 2012. Disponível em: https://dacemirror.sci-hub.ru/journal article/9cecddef3ae7964e103332edbacfa31c/azimahabdulaziz2012.pdf. Acesso em: 20 set. 2025, às 10h06min.

BADMAN, Annie; KOSINSKI, Matthew. O que são dados? 2025. *In*.: **Portal IBM**, 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/data?mhsrc=ibmsearch_a&mhq=o%20que%20s%26atilde%3Bo%20dadoss. Acesso em: 7 out. 2025, às 18h03min.

BECHT, Marco; BOLTON, Patrick; RÖELL, Ailsa. Corporate governance and control. *In*.: **NBER working paper series**, Dec. 2002. Disponível em: https://www.nber.org/system/files/working_papers/w9371/w9371.pdf. Acesso em: 3 set. 2025, às 0h41min.

BERGAMINI JUNIOR, Sebastião. A crise de credibilidade corporativa. **Revista do BNDES**, Rio de Janeiro, v. 9, n. 18, p. 33-84, 2002. Disponível em: https://web.bndes.gov.br/bib/jspui/handle/1408/11576. Acesso em: 4 set. 2025, às 22h13min.

BERGAMINI JUNIOR, Sebastião. Controles internos como um instrumento de governança corporativa. **Revista do BNDES**, Rio de Janeiro, v. 12, n. 24, p. 149-188, 2005. Disponível em: https://www.luisguilherme.adm.br/download/IUESO_Governanca/rev2406.pdf. Acesso em: 3 set. 2025, às 0h42min.

BERGER, Adam J. WorldCom scandal. 2022. *In*.: **EBSCO Information Services**, 2025. Disponível em: https://www.ebsco.com/research-starters/business-and-management/worldcom-scandal. Acesso em: 3 set. 2025, às 19h56min.

BERLE, A. A.; MEANS, G. C. **The Modern Corporation and Private Property**. New York: Macmillan, 1932. *Apud* PEIXOTO, Fernanda Maciel. **Governança corporativa, desempenho, valor e risco**: estudo das mudanças em momentos de crise. 2012. 216f. Tese (Doutorado em Administração), Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, Belo Horizonte, 2012. Disponível em: https://repositorio.ufmg.br/bitstream/1843/BUBD-92MJUW/1/tese_fernanda_revisada_28_09___final.pdf. Acesso em: 3 set. 2025, às 1h13min.

BISHARA, Norman David. Governance and Corruption Constraints: The Business Ethics Glass Ceiling in Middle East Corporate Governance. **Michigan Ross School of Business Paper**, University of Michigan, n. 1143, Apr. 2010. Disponível em: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/69255/1143_NBishara.pdf?sequence=1&isAllowed=y. Acesso em: 18 set. 2025, às 21h45min.

BLOG IMPACTA. ITIL e Cobit: entenda as principais diferenças e suas aplicações. Setembro, 2017. *In*.: **Portal BLOG IMPACTA**, 2025. Disponível em: https://www.impacta.com.br/blog/itil-e-cobit-entenda-as-principais-diferencas-e-suas-aplicacoes/. Acesso em: 28 set. 2025, às 18h49min.

BONOTTO, Pietro Vinicius. As fraudes contábeis da Enron e Worldcom e seus efeitos nos Estados Unidos. 2010, 23f. TG (Trabalho de Graduação de Ciências Contábeis), Universidade Federal do Rio Grande do Sul, 2010. *In*.: **UFRGS Lume**: Repositório digital da Universidade Federal do Rio Grande do Sul, 2010. Disponível em: https://lume.ufrgs.br/handle/10183/27203. Acesso em: 3 set. 2025, às 0h45min.

BORGERTH, Vania Maria da Costa. **A Lei Sarbanes-Oxley**: um caminho para a informação transparente. 2005. 142f. Dissertação (Mestrado em Administração e Economia), Programa de Pós-Graduação e Pesquisa em Administração e Economia das Faculdades IBMEC (Instituto Brasileiro de Mercado de Capitais), 2005.

Disponível em: https://web.bndes.gov.br/bib/jspui/handle/1408/10055. Acesso em: 4 set. 2025, às 21h55min

BORGERTH, Vania Maria da Costa. **SOX**: entendendo a Lei Sarbanes-Oxley. São Paulo: Thomson Learning, 2007.

BROWNING, E. S. Is the Praise for WorldCom Too Much? Estados Unidos, **Wall Street Journal**, p. C-24, v. 8, 1997. *Apud* BONOTTO, Pietro Vinicius. As fraudes contábeis da Enron e Worldcom e seus efeitos nos Estados Unidos. 2010, 23f. TG (Trabalho de Graduação de Ciências Contábeis), Universidade Federal do Rio Grande do Sul, 2010. *In*.: **UFRGS Lume**: Repositório digital da Universidade Federal do Rio Grande do Sul, 2010. Disponível em: https://lume.ufrgs.br/handle/10183/27203. Acesso em: 3 set. 2025, às 0h45min.

BRUM, Maria Cecilia da Silva. Controles Internos e de tecnologia da informação na mitigação dos riscos de conformidade das informações contábeis. 2014. 107f. Dissertação (Mestrado em Ciências Contábeis), Programa de Pós-Graduação em Ciências Contábeis, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo. **RDBU**: Repositório Digital da Biblioteca da Unisinos, 2014. Disponível em: https://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/3926/Maria%20Cecilia%20da%20Silva%20Brum.pdf?sequence=1&isAllowed=y. Acesso em: 27 abr. 2025, às 21h08min.

CADBURY, Adrian. The financial aspects of corporate governance: Cadbury Report. *In*.: **The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd**. London Stock Exchange. 1992. Disponível em: https://www.jbs.cam.ac.uk/wp-content/uploads/2024/10/cadbury-report.pdf. Acesso em: 31 ago. 2025, às 20h46min.

CARIOCA, Karla Jeanny Falcão; LUCA, Márcia Martins Mendes de; PONTE, Vera Maria Rodrigues. Implementação da Lei Sarbanes-Oxley e seus impactos nos controles internos e nas práticas de governança corporativa: um estudo na companhia energética do Ceará–Coelce. **Revista Universo Contábil**, v. 6, n. 4, p. 50-67, 2010. Disponível em: https://ojsrevista.furb.br/ojs/index.php/universocontabil/article/view/1388/1422. Acesso em: 31 ago. 2025, às 20h46min.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi. **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010. *Apud* BRUM, Maria Cecilia da Silva. Controles Internos e de tecnologia da informação na mitigação dos riscos de conformidade das informações contábeis. 2014. 107f. Dissertação (Mestrado em Ciências Contábeis), Programa de Pós-Graduação em Ciências Contábeis, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo. **RDBU**: Repositório Digital da Biblioteca da Unisinos, 2014. Disponível em: https://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/3926/Maria%20Cecilia%20da%20Silva%20Brum.pdf?sequence=1&isAllowed=y. Acesso em: 27 abr. 2025, às 21h08min.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. Internal control: Integrated framework. *In.:* **COSO**, 1992. Disponível em: https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1199&context=aicpa_assoc. Acesso em: 31 ago. 2025, às 9h37min.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. Internal control: Integrated framework. *In.:* **COSO,** 2012. Disponível em: https://ce.jalisco.gob.mx/sites/ce.jalisco.gob.mx/files/coso_mejoras_al_control_interno.pdf. Acesso em: 31 ago. 2025, às 9h37min.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION; SOCIETY OF CORPORATE COMPLIANCE AND ETHICS; HEALTH CARE COMPLIANCE ASSOCIATION. Enterprise Risk Management: Compliance Risk Management: Applying the COSO ERM framework, nov. 2020. *In*.: **COSO; SCCE; HCCA**, 2020. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2023/08/compliance-risk-management-applying-the-coso-erm-framework.pdf. Acesso em: 14 set. 2025, às 10h47min.

DALLAGNOL, Evelyze Cruz; SOUSA, Henrique Adriano de; PASSOS, Gabriela de Abreu; DUARTE JUNIOR, Joacir Celso; COSTA, Mayla Cristina. Os princípios da governança corporativa: o enfoque dado pelas empresas listadas na B3. XVI CONGRESSO USP DE INICIAÇÃO CIENTÍFICA EM CONTABILIDADE. Julho, 2019. Disponível em: https://congressousp.fipecafi.org/anais/19UspInternational/ArtigosDownload/1374.pdf. Acesso em: 31 ago. 2025, às 9h37min.

DANTAS, José Alves; RODRIGUES, Fernanda Fernandes; MARCELINO, Gileno Fernandes; LUSTOSA, Paulo Roberto Barbosa. Custo-benefício do controle: proposta de um método para avaliação com base no COSO. **Contabilidade Gestão e Governança**, v. 13, n. 2, 2010. Disponível em: https://revistacgg.org/index.php/contabil/article/download/255/224. Acesso em: 20 set. 2025, às 11h44min.

DARONCO, José Máximo. **Análise de processos de controles internos e de TI no requisito de conformidade da governança corporativa**: estudo de caso SESCOOP/RS, 2013. 136f. Dissertação (Mestrado em Ciências Contábeis), Programa de Pós-Graduação em Ciências Contábeis, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2013. Disponível em: https://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/3933/josemaximo.pdf?sequence=1&isAllowed=y. Acesso em: 20 set. 2025, às 11h18min.

DELOITTE TOUCHE TOHMATSU. Lei Sarbanes-Oxley: guia para melhorar a governança corporativa através de eficazes controles internos. **Consultoria Deloitte Touche Tohmatsu,** São Paulo, maio 2003. Disponível em: https://www.legiscompliance.com.br/images/pdf/sarbanes_oxley_portugues_delloite.pdf. Acesso em 05 setembro 2025, às 18h54min.

DRUCKER, Phyllis. Entendendo as práticas de gerenciamento da ITIL 4, 28 fev. 2025. *In*.: **Portal ManageEngine**, 2025. Disponível em: https://www.manageengine.com/br/service-desk/itsm/what-is-itil-4-management-practices.html. Acesso em: 18 out. 2025, às 15h07min.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. Implementando a Gestão de riscos no setor público: Módulo 2 – Estrutura do COSO ERM. **Portal ENAP**, Brasília/DF, 2018. Disponível em: https://files.core.ac.uk/download/pdf/227078683.pdf. Acesso em: 12 set. 2025, às 18h06min.

EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING; FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS. Guidance on the 8th EU Company Law Directive: article 41. **ECIIA; FERMA**, 21 set. 2010. Disponível em: https://www.ferma.eu/wp-content/uploads/2011/09/eciia-ferma-guidance-on-the-8th-eu-company-law-directive.pdf. Acesso em: 26 set. 2025, às 20h20min.

FARIAS, Rômulo Paiva; LUCA, Márcia Martins Mendes de; MACHADO, Marcus Vinicius Veras. A metodologia COSO como ferramenta de gerenciamento dos controles internos. **Contabilidade Gestão e Governança**, v. 12, n. 3, 2009. Disponível em: https://revistacgg.org/index.php/contabil/article/view/132/pdf_117. Acesso em 20 set. 2025, às 11h52min.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. Implantando a Governança de TI: da Estratégia à Gestão de Processos e Serviços. 4a. ed. São Paulo: Brasport, 2014. Disponível em: https://www.kufunda.net/publicdocs/Implantando%20a%20Governan%C3%A7a%20de%20TI%20(%20etc.).pdf. Acesso em: 25 set. 2025, às 21h48min.

FIORINI, Filipe Antônio; ALONSO JUNIOR, Nelson; ALONSO, Vera Lucia Chaves. Governança corporativa: conceitos e aplicações. SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA (SEGet), v. 13, p. 30-31, 2016. Disponível em: https://www.aedb.br/seget/arquivos/artigos16/19524178.pdf. Acesso em: 31 ago. 2025, às 9h30min.

GELATTI, Cristiane Braida; MENEGHETTI, Daniela. **Análise da adequação das empresas brasileiras à Lei Sarbanes-Oxley.** 2008. 51f. TG (Trabalho de Graduação em Ciências Contábeis), Universidade Federal de Santa Maria, Santa Maria/RS, 2008. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/25208/141-cristiane%20e%20daniela.pdf?sequence=1. Acesso em: 25 maio 2025, às 11h52min.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. COBIT® 2019 Framework: Introduction and Methodology. **ISACA**, 2018. Disponível em: https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf. Acesso em: 29 set. 2025, às 22h25min.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. Risk IT Framework: 2nd Edition. **ISACA**, 2020. Disponível em: https://community.mis.temple.edu/mis5206sec701fall2025/files/2022/08/Risk-IT-Framework-2nd-Edition_fmk_Eng_0620-1.pdf. Acesso em: 3 out. 2025, às 18h22min.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Guia de Orientação para Gerenciamento de Riscos Corporativos**. São Paulo: IBGC, 2007. Disponível em: https://repositorio.secont.es.gov.br/bitstream/123456789/128/1/IBGC.pdf. Acesso em: 4 out. 2025, às 10h23min.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 6a. ed. São Paulo: IBGC, 2023. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 31 ago. 2025, às 9h05min.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Sistema de integridade**: fundamentos e boas práticas. São Paulo: IBGC, 2025. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24725&assessment=1. Acesso em: 27 out. 2025, às 23h27min.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA; INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. Auditoria Interna: Aspectos essenciais para o Conselho de Administração. São Paulo: IBGC, 2018 (Série IBGC Orienta). *In*.: **IBGC; IIA Brasil**, 2018. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/23980/Publicao-IBGCOrienta-AuditoriaInterna%20-%202018.pdf. Acesso em 27 abril 2025, 20h56min.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. Declaração de posicionamento do IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles, jan. 2013. **IIA Brasil**, 2013. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/as-trs-linhas-d-ippf-00000010-28082019095801.pdf. Acesso em: 20 set. 2025, às 10h45min.

IT GOVERNANCE INSTITUTE. COBIT® 4.1: Modelo, Objetivos de Controle, Diretrizes de Gerenciamento e Modelos de Maturidade. **IT Governance Institute** (ITGI), 2007. Disponível em: https://drive.google.com/file/d/0B7TPEf35oSMiZGU5MDMyZjktZGYwMi00ZDgwLThlZDUtMTlmNDI3NTg1MDg0/view?hl=en&resourcekey=0-YoNFpf-zbW8Kcak-CK-Tuw. Acesso em: 22 set. 2025, às 20h53min.

JAMALI, Dima; SAFIEDDINE, Asem M.; RABBATH, Myriam. Corporate governance and corporate social responsibility synergies and interrelationships. **Corporate governance**: an international review, v. 16, n. 5, p. 443-459, 2008. Disponível em: https://iri.hse.ru/data/994/481/1225/Oct%2028%20corporate%20governance%20and%20csr.pdf. Acesso em: 3 set. 2025, às 0h49min.

JENSEN, Michael C.; MECKLING, William H. **Theory of the firm**: Managerial behavior, agency costs and ownership structure. v. 3, n. 4, p. 305-360, 1976. *Apud* PEIXOTO, Fernanda Maciel. **Governança corporativa, desempenho, valor e risco**: estudo das mudanças em momentos de crise. 2012. 216f. Tese (Doutorado em Administração), Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, Belo Horizonte, 2012. Disponível em: https://repositorio.ufmg.br/bitstream/1843/BUBD-92MJUW/1/tese_fernanda_revisada_28_09___final.pdf. Acesso em: 3 set. 2025, às 1h13min.

JORDÃO, Ricardo Vinícius Dias; SOUZA, Antônio Artur de; TEDDO, Anna Carolina. Governança corporativa e ética de negócios: Uma análise nos principais modelos internacionais de controle interno. **Sistemas & Gestão**, v. 7, n. 1, p. 76-92, 2012. Disponível em: https://web.archive.org/web/20200321113752id_/http://www.revistasg.uff.br/index.php/sg/article/viewFile/V7N1A5/V7N1A5. Acesso em: 20 set. 2025, às 11h32min.

KAARST-BROWN, Michelle L.; KELLY, Shirley. IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function? *In*: PROCEEDINGS OF THE 38TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES. IEEE, 2005. p. 1-10. Disponível em: https://www.computer.org/csdl/proceedings-article/hicss/2005/22680236a/12OmNzahbWa. Acesso em: 3 set. 2025, às 0h53min.

KARANJA, Erastus; ZAVERI, Jigish. Effect of the SOX Act on IT Governance. In.: **AIS Electronic Library**, 2012. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1002&context=amcis2012. Acesso em: 7 out. 2025, às 19h03min.

KAWAGUTI, Cleyton Takashi. **Governança corporativa em tecnologia da informação**: um diferencial na obtenção de vantagem competitiva entre instituições financeiras. 2008. 51f. TG (Trabalho de Graduação do Curso de Administração), UniCEUB – Faculdade de Tecnologia e Ciências Sociais Aplicadas, Área de Administração de Sistema da Informação, Brasília/DF, 2008. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/123456789/773/2/20137173.pdf. Acesso em: 30 maio 2025, 20h57min.

KPMG AUDITORES INDEPENDENTES. Seção 404 da Lei Sarbanes-Oxley: Certificação dos Controles Internos pela Administração. **Portal da Consultoria KPMG**, 2006. Disponível em: https://www.legiscompliance.com.br/images/pdf/sox_404_perguntas_frequentes.pdf. Acesso em: 5 set. 2025, às 18h33min.

KPMG AUDITORES INDEPENDENTES. Controles internos e as deficiências reportadas pelas empresas abertas brasileiras. **Portal da Consultoria KPMG**, 2024. Disponível em: https://assets.kpmg.com/content/dam/kpmg/br/pdf/2024/01/As-Deficincias-nos-Controles-Internos.pdf. Acesso em: 17 set. 2025, às 18h51min.

LABADESSA, Edson; ROSINI, Alessandro Marco, PALMISANO, Angelo; CONÇEIÇÃO, Marcio Megera. Boa governança hospitalar: ajustes planejados para

resultados na melhoria do atendimento público aos pacientes. **Research, Society and Development**, v. 9, n. 2, p. 1-20, 2019. Disponível em: https://www.researchgate.net/publication/338314313_Boa_governanca_hospitalar_ajustes_planejados_para_resultados_na_melhoria_do_atendimento_publico_aos_pacientes. Acesso em: 3 set. 2025, às 0h54min.

LAHTI, Christian B.; PETERSON, Roderick. **Sarbanes-Oxley:** Conformidade TI usando COBIT e ferramentas open source. Rio de Janeiro, Alta Books, 2005. *Apud* PINHEIRO, José Maurício dos Santos. O Ato Sarbanes-Oxley e o Impacto sobre a Governança de TI das Corporações. **Cadernos UniFOA**, v. 1, n. 2, p. 33-42, 2006. Disponível em: https://unifoa.emnuvens.com.br/cadernos/article/view/890/734. Acesso em: 19 set. 2025, às 19h10min.

LIMA, Douglas Araújo de; MACIEL, Caroline Veloso; LIBONATI, Jeronymo José. Os impactos gerados na adequação da estrutura de controles internos de uma empresa brasileira às exigências da seção 404 da Lei Sarbanes-Oxley: um estudo de caso. ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PÓS-GRADUAÇÃO E PESQUISA EM ADMINISTRAÇÃO, v. 32, 2008. Disponível em: https://arquivo.anpad.org.br/abrir_pdf.php?e=OTU3NQ==. Acesso em: 3 set. 2025, às 0h57min.

MONTEIRO, G. Governança corporativa. **Equidade no tratamento de seus acionistas, independentemente de sua classe ou categoria**. 2005, 4p. Disponível em: http://www.dlminvista.com.br/arquivos/exchange3.pdf. Acesso em: 12 maio 2008. *Apud* GELATTI, Cristiane Braida; MENEGHETTI, Daniela. **Análise da adequação das empresas brasileiras à Lei Sarbanes-Oxley**. 2008. 51f. TG (Trabalho de Graduação em Ciências Contábeis), Universidade Federal de Santa Maria, Santa Maria/RS, 2008. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/25208/141-cristiane%20e%20daniela.pdf?sequence=1. Acesso em: 25 maio 2025, às 11h52min.

MURPHY, Vawns. A Cadeia de valor de Serviço da ITIL. Janeiro, 2025. *In*.: **Portal ManageEngine**, 2025. Disponível em: https://www.manageengine.com/br/service-desk/itsm/what-is-itil-4-service-value-chain.html. Acesso em: 8 out. 2025, às 19h32min.

OLIVEIRA, Djalma de Pinho Rebouças de. **Governança corporativa na prática**: integrando acionistas, conselho de administração e diretoria executiva na geração de resultados: conceitos, estruturação, atuação, prática. Atlas, 2006. *Apud* DALLAGNOL, Evelyze Cruz; SOUSA, Henrique Adriano de; PASSOS, Gabriela de Abreu; DUARTE JUNIOR, Joacir Celso; COSTA, Mayla Cristina. Os princípios da governança corporativa: o enfoque dado pelas empresas listadas na B3. XVI CONGRESSO USP DE INICIAÇÃO CIENTÍFICA EM CONTABILIDADE. Julho, 2019. Disponível em: https://congressousp.fipecafi.org/anais/19UspInternational/ArtigosDownload/1374.pdf. Acesso em: 31 ago. 2025, às 9h37min.

OLIVEIRA, Marcelle Colares; LINHARES, Juliana Silva. A implantação de controle interno adequado às exigências da Lei Sarbanes-Oxley em empresas brasileiras-Um

estudo de caso. **Revista Base de Administração e Contabilidade da UNISINOS**, v. 4, n. 2, p. 160-170, 2007. Disponível em: https://www.redalyc.org/pdf/3372/337228632007.pdf. Acesso em: 3 set. 2025, às 1h10min.

OLIVEIRA, Marisa Silva de; CINTRA, Denise Gomes Barros. Os impactos da Lei Sarbanes Oxley no mercado de capitais e na auditoria externa. **Revista de Estudos Interdisciplinares do Vale do Araguaia**, v. 2, n. 2, p. 1-17, 2019. Disponível em: https://reiva.unifaj.edu.br/reiva/article/view/86/68. Acesso em: 31 ago. 2025, às 9h25min.

PEIXOTO, Fernanda Maciel. **Governança corporativa, desempenho, valor e risco**: estudo das mudanças em momentos de crise. 2012. 216f. Tese (Doutorado em Administração), Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, Belo Horizonte, 2012. Disponível em: https://repositorio.ufmg.br/bitstream/1843/BUBD-92MJUW/1/tese_fernanda_revisada_28_09___final.pdf. Acesso em: 3 set. 2025, às 1h13min.

PETER, Maria da Glória Arrais; MACHADO, Marcus Vinícius Veras. **Manual de Auditoria Governamental**. São Paulo: Atlas, 2003. *Apud* OLIVEIRA, Marcelle Colares; LINHARES, Juliana Silva. A implantação de controle interno adequado às exigências da Lei Sarbanes-Oxley em empresas brasileiras-Um estudo de caso. **Revista Base de Administração e Contabilidade da UNISINOS**, v. 4, n. 2, p. 160-170, 2007. Disponível em: https://www.redalyc.org/pdf/3372/337228632007.pdf. Acesso em: 3 set. 2025, às 1h10min.

PINHEIRO, José Maurício dos Santos. O Ato Sarbanes-Oxley e o Impacto sobre a Governança de TI das Corporações. **Cadernos UniFOA**, v. 1, n. 2, p. 33-42, 2006. Disponível em: https://unifoa.emnuvens.com.br/cadernos/article/view/890/734. Acesso em: 19 set. 2025, às 19h10min.

QUALITOR: inteligência em processos. Qual a diferença de aplicação entre ITIL e Cobit?, 15 out. 2022. *In*.: **Portal Qualitor**, 2022. Disponível em: https://www.qualitor.com.br/qual-a-diferenca-de-aplicacao-entre-itil-e-cobit. Acesso em: 28 set. 2025, às 18h38min.

REHAGE, Kirk; HUNT, Steve; NIKITIN, Fernando. Developing the IT Audit Plan. *In*.: **The Institute of Internal Auditors**: Global Technology Audit Guide: IPPF: Practice Guide, Jul. 2008. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/developingtheit-ippf-00000001-24012018121142.pdf. Acesso em: 1 jun. 2025, às 12h40min.

RICARDINO, Álvaro; MARTINS, Sofie Tortelboom Aversari. Governança corporativa: um novo nome para antigas práticas? **Revista Contabilidade & Finanças**, v. 15, p. 50-60, 2004. Disponível em: https://www.scielo.br/j/rcf/a/vkm8PrJKq3JpvPxJdHw3TNf/?format=html&lang=pt. Acesso em: 3 set. 2025, às 1h14min.

RODRIGUEZ, Peter; SIEGEL, Donald S.; HILLMAN, Amy; EDEN, Lorraine. Three lenses on the multinational enterprise: Politics, corruption, and corporate social responsibility. **Journal of international business studies**, v. 37, n. 6, p. 733-746, 2006. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=900544. Acesso em: 3 set. 2025, às 1h16min.

SANTOS, Renato Almeida dos; GUEVARA, Arnoldo José de Hoyos; AMORIM, Maria Cristina Sanches; FERRAZ-NETO, Ben-Hur. Compliance e liderança: a suscetibilidade dos líderes ao risco de corrupção nas organizações. **Revista Einstein**, São Paulo, v. 10, p. 1-10, 2012. Disponível em: https://www.scielo.br/j/eins/a/KtNqFbyQ5XWsDvJ7TfbGC3w/?lang=pt. Acesso em: 3 set. 2025, às 1h17min.

SASSI, Renato José; ARRIVABENE, Adriano; VICENTE, Cleber William; PASSOS, Rogerio Lopes. Sustentabilidade Corporativa garantida por uma Governança de Business Intelligence adequada às regulações da lei Sarbanes-Oxley. **Brazilian Journal of Business,** v. 5, n. 1, p. 693-707, 2023. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/58329/42511. Acesso em: 24 set. 2025, às 20h08min.

SCHMITT, Cecília. Entenda o caso ENRON. Rio de Janeiro: Núcleo de computação do Instituto de Economia da Universidade Federal do Rio de Janeiro e Eletrobrás. artigo online publicado em 2002. Disponível em: http://www.provedor.nuca.ie.ufrj.br/eletrobras/artigos/schmitt1.htm. Acesso em: 20 maio 2013. *Apud* OLIVEIRA, Marisa Silva de; CINTRA, Denise Gomes Barros. Os impactos da Lei Sarbanes Oxley no mercado de capitais e na auditoria externa. **Revista de Estudos Interdisciplinares do Vale do Araguaia**, v. 2, n. 2, p. 1-17, 2019. Disponível em: https://reiva.unifaj.edu.br/reiva/article/view/86/68. Acesso em: 31 ago. 2025, às 9h25min.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. Gestão de Riscos e Controles, 29 ago. 2025. *In*.: **Portal SERPRO**, 2025. Disponível em: https://www.transparencia.serpro.gov.br/governanca/governanca-corporativa/gestao-de-riscos. Acesso em: 14 set. 2025, às 15h20min.

SILVEIRA, Alexandre Di Miceli da. **Governança corporativa no Brasil e no mundo**: teoria e prática. Rio de Janeiro, Elsevier, 2010. Disponível em: https://pdfcoffee.com/governana-corporativa-no-brasil-e-no-mundo-pdf-free.html. Acesso em: 31 ago. 2025, às 9h34min.

SOUZA, José Carlos de; SCARPIN, Jorge Eduardo. Fraudes Contábeis: As respostas da contabilidade nos Estados Unidos e na Europa. III SEGET: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, v. 3, 2006. Disponível em: https://www.aedb.br/seget/arquivos/artigos06/493_Fraudes%20-%20SEGET.pdf. Acesso em: 4 set. 2025, às 22h02min.

SOUZA NETO, João; MACEDO, Leandro Pfeifer (ORG.). **Cartilha COBIT 2019:** versão 1, Out. 2021. Brasília/DF: João Souza Neto, 2021. Disponível em: https://www.researchgate.net/publication/355397119_Cartilha_COBIT_2019_versao_1. Acesso em: 21 set. 2025, às 15h02min.

THE INSTITUTE OF INTERNAL AUDITORS. Global Technology Audit Guide 1: Riscos e Controles de Tecnologia da Informação. Tradução ao português patrocinada pela Fundación Latinoamericana de auditores internos (FLAI). 2ª ed., mar. 2012. *In*.: **IIA**, 2012. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/livro-3-riscos--ippf-00000001-11122018175610.pdf. Acesso em: 3 out. 2025, às 18h04min.

THE INSTITUTE OF INTERNAL AUDITORS. Global Technology Audit Guide 4: Management of IT Auditing: 2nd Edition, Jan. 2013.*In*.: **IIA**, 2013. Disponível em: https://pdfcoffee.com/gtag-04-management-of-it-auditing-2nd-edition-pdf-free.html. Acesso em: 3 out. 2025, às 17h41min.

UNITED STATES OF AMERICA. Sarbanes-Oxley Act of 2002, Public Law 107-204. *In*.: **Portal United States Departament of Labor**: Office of Administrative Law Judges, 2025. Disponível em: https://www.dol.gov/agencies/oalj/PUBLIC/WHISTLEBLOWER/REFERENCES/STATUTES/SARBANES_OXLEY_ACT_OF_2002. Acesso em: 27 out. 2025, às 22h52min.

VIEIRA, Sergio Arnor. A auditoria e os sistemas de controles internos no Brasil: antecedentes e evolução. **Revista de Economia Mackenzie**, v. 5, n. 5, 2007. Disponível em: https://editorarevistas.mackenzie.br/index.php/rem/article/view/801/495. Acesso em: 20 set. 2025, às 11h20min.

WEILL, Peter. Don't just lead, govern: How top-performing firms govern IT. **MIS Quarterly Executive**, v. 3, n. 1. Março, 2004. Disponível em: https://www.umsl.edu/~lacitym/topperform.pdf. Acesso em: 25 set. 2025, às 21h33min.

WEILL, Peter; ROSS, Jeanne Wenzel. **Governança de tecnologia da informação**: como as empresas com melhor desempenho administram dos direitos decisórios de TI na busca por resultados superiores. São Paulo: Makron, 2006. *Apud* KAWAGUTI, Cleyton Takashi. **Governança corporativa em tecnologia da informação**: um diferencial na obtenção de vantagem competitiva entre instituições financeiras. 2008. 51f. TG (Trabalho de Graduação do Curso de Administração), UniCEUB – Faculdade de Tecnologia e Ciências Sociais Aplicadas, Área de Administração de Sistema da Informação, Brasília/DF, 2008. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/123456789/773/2/20137173.pdf. Acesso em: 30 maio 2025, 20h57min.

WOLTERS KLUWER. Pontos fracos do controle interno: Identificação e soluções para auditores internos, 29 ago. 2025. *In*.: **Portal Wolters Kluwer,** 2025. Disponível em: https://www.wolterskluwer.com/pt-br/expert-insights/internal-control-weaknesses-identification-solutions-internal-auditors. Acesso em: 17 set. 2025, às 22h42min.