Universidade Federal do Rio de Janeiro

Escola Politécnica

MBA em Governança, Projetos e Serviços de TI
(MBGPS)

ANÁLISE SOBRE A ATIVIDADE DE AUDITORIA INTERNA DE TECNOLOGIA DA INFORMAÇÃO EM UMA EMPRESA DE TELECOM

Autor:

Diogo Pereira Gama

Orientador:

Manoel Villas Bôas Júnior, M. Sc.

Coorientador:

Edilberto Strauss, Ph. D.

Examinador:

Cláudio Luiz Latta de Souza, M. Sc.

Examinador:

Jose Airton Chaves Cavalcante Junior, D. Sc.

Examinador:

Vinicius Teixeira do Nascimento, M. Sc.

Rio de Janeiro
Fevereiro de 2021

Declaração de Autoria e de Direitos

Eu, **Diogo Pereira Gama** CPF 097.967.067-50, autor da monografia ***ANÁLISE SOBRE A ATIVIDADE DE AUDITORIA INTERNA DE TECNOLOGIA DA INFORMAÇÃO EM UMA EMPRESA DE TELECOM***, subscrevo para os devidos fins, as seguintes informações:

1. O autor declara que o trabalho apresentado na defesa da monografia do curso de Pós-Graduação, Especialização MBA - ENGEMAN em Engenharia de Manutenção da Escola Politécnica da UFRJ é de sua autoria, sendo original em forma e conteúdo.

2. Excetuam-se do item 1 eventuais transcrições de texto, figuras, tabelas, conceitos e idéias, que identifiquem claramente a fonte original, explicitando as autorizações obtidas dos respectivos proprietários, quando necessárias.

3. O autor permite que a UFRJ, por um prazo indeterminado, efetue em qualquer mídia de divulgação, a publicação do trabalho acadêmico em sua totalidade, ou em parte. Essa autorização não envolve ônus de qualquer natureza à UFRJ, ou aos seus representantes.

4. O autor declara, ainda, ter a capacidade jurídica para a prática do presente ato, assim como ter conhecimento do teor da presente Declaração, estando ciente das sanções e punições legais, no que tange a cópia parcial, ou total, de obra intelectual, o que se configura como violação do direito autoral previsto no Código Penal Brasileiro no art.184 e art.299, bem como na Lei 9.610.

5. O autor é o único responsável pelo conteúdo apresentado nos trabalhos acadêmicos publicados, não cabendo à UFRJ, aos seus representantes, ou ao(s) orientador(es), qualquer responsabilização/ indenização nesse sentido.

6. Por ser verdade, firmo a presente declaração.

Rio de Janeiro, _____ de _____ de _____.

_____

Diogo Pereira Gama

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Escola Politécnica - Departamento de Engenharia Naval e Oceânica
MBA ENGEMAN - Especialização em Engenharia de Manutenção
Av. Athos da Silveira, 149 - Centro de Tecnologia, Bloco C, sala - 203,
Cidade Universitária Rio de Janeiro – RJ - CEP 21949-900.

DEDICATÓRIA

Dedico este trabalho a minha mãe Alcinda, por sempre ter acreditado em mim e não ter medido esforços para investir na minha educação.

Dedico este trabalho a minha esposa Cassiana, por estar sempre ao meu lado com o seu amor e apoio incondicional. Te amo.

AGRADECIMENTO

Agradeço a Deus por ter me dado saúde e forças para superar todas as dificuldades.
Agradeço ao meu orientador Manoel, por todo o apoio, orientação e incentivo prestados durante a elaboração desta pesquisa. Agradeço também a todo corpo docente e funcionários do ITLab.
Agradeço a minha mãe e minha esposa, por sempre estarem ao meu lado, acreditando em mim e me incentivando a ser uma pessoa cada vez melhor.

RESUMO

Dada a relevância cada vez maior que a Tecnologia da Informação (TI) vem assumindo para os negócios, o papel da auditoria de TI se destaca gradativamente como um importante instrumento de controle e avaliação do ambiente tecnológico para as empresas. Neste sentido, o objetivo deste estudo visa analisar a cobertura de atuação da área de auditoria interna de TI de uma empresa de telecomunicações e os resultados obtidos a partir das auditorias realizadas. Para isto, foi realizada a análise de conteúdo dos relatórios de auditorias ocorridas em 2019 e 2020 para levantamento do escopo de atuação da área, das deficiências apontadas e dos benefícios obtidos pela empresa, utilizando o framework COBIT 5 como um guia de melhores práticas para auxiliar na avaliação. Com o resultado deste estudo é possível verificar que a área de auditoria de TI atua na maioria dos projetos de forma abrangente contemplando diferentes abordagens de atuação através de um único trabalho. Além disso, as principais deficiências apontadas são relativas a problemas na gestão de acessos em sistemas e/ou elementos de infraestrutura, nos processos e políticas de TI e nos controles sistêmicos para atendimento de regras de negócio. Por fim, os principais ganhos obtidos a partir das auditorias são referentes às melhorias na gestão e governança da TI e nos controles de segurança dos recursos de tecnologia. O resultado apresentado é importante para auxiliar profissionais e empresas a conhecerem maiores detalhes a respeito sobre as características de atuação da auditoria de TI e sobre as principais deficiências identificadas pela auditoria interna na área TI.

Palavras-Chave: Auditoria de TI, Governança e Gestão da TI, COBIT

ABSTRACT

Given the increasing relevance that Information Technology (IT) is assuming for business, the role of IT auditing is gradually stands out as an important control tool and assessment of the technological environment for companies. In this sense, the objective of this study is to analyze the performance coverage of the IT internal audit area of a telecommunications company and the results obtained from the audits performed. For this, the content analysis was performed of the audit reports of 2019 and 2020 audit projects to identify the scope of the area, the gaps pointed out and the benefits obtained by the company, using the COBIT 5 framework as a guide of best practices to assist in the evaluation. With the result of this study, it is possible to verify that the IT audit area operates in most projects in an extensive way, contemplating different performance approaches through a single job. In addition, the main deficiencies identified are related to problems in access management in systems and / or infrastructure elements, in IT processes and policies and in systemic controls to meet business rules. Finally, the main gains obtained from audits are related to improvements in IT management and governance and in the security controls of technology resources. The result presented will be important to help professionals and companies to know more details about the performance of IT audit characteristics and about the main deficiencies identified by the internal audit in the IT area.

Keywords: IT Audit, IT Governance and Management, COBIT

SIGLAS

APO	Align, Plan and Organise
BAI	Build, Acquire and Implement
CAE	Chief Audit Executive
CARC	Comitê de Auditoria, Riscos e Controles
CEO	Chief Executive Officer
COBIT	Control Objectives for Information and Related Technology
DSS	Deliver, Service and Support
EDM	Evaluate, Direct and Monitor
FUP	Follow-up
ISACA	Information Systems Audit and Control Association
LGPD	Lei Geral de Proteção de Dados
MEA	Monitor, Evaluate and Assess
PBRM	Plan, Build, Run and Monitor
PTA	Pontos de auditoria
Telecom	Telecomunicações
TI	Tecnologia da Informação
UFRJ	Universidade Federal do Rio de Janeiro

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

Sumário

Capítulo 1

Introdução

1.1 – Tema

A Tecnologia da Informação (TI) se tornou um tema obrigatório para todas as empresas e a sua evolução está progredindo de forma cada vez mais acelerada. Cibersegurança, computação em nuvem, exploração de dados e digitalização, além de outros assuntos relacionados à TI, contribuem diretamente para a complexidade e os riscos envolvidos nos negócios das organizações. Neste sentido, é imperativo que as empresas compreendam cada vez mais os benefícios oferecidos pelas auditorias com o foco em TI e, sempre que possível, incentivem a realização de avaliações independentes a respeito dos controles tecnológicos que suportam os processos das organizações.

A proposta deste trabalho é analisar a cobertura da atuação da área de auditoria de TI de uma empresa de telecomunicação (Telecom), bem como analisar os resultados obtidos através dos projetos de auditoria executados pela área, utilizando o framework do COBIT 5 como guia de melhores práticas para auxiliar na análise.

1.2 – Justificativa

Os negócios e a tecnologia estão a convergir rapidamente. Os riscos tecnológicos podem resultar em ameaças concretas e relevantes envolvendo aspectos estratégicos, financeiros, operacionais e de reputação para as organizações. Além disso, cada vez mais as empresas estão aumentando seus orçamentos dedicados à gestão de riscos cibernéticos e à segurança da informação com objetivo de implementar controles que suportem seus ambientes de TI. Neste sentido, a auditoria interna de TI passa a ser inserida na rotina das empresas e estar preparada para monitorar os riscos cibernéticos dentro das organizações.

Segundo Deloitte [1], em pesquisa publicada em 2019, a respeito da gestão dos riscos cibernéticos em empresas na América Latina e Caribe, a segurança cibernética é considerada um tema de relevante importância dentro dos seus modelos de governança e gestão, conforme é possível verificar através da figura 1.1.

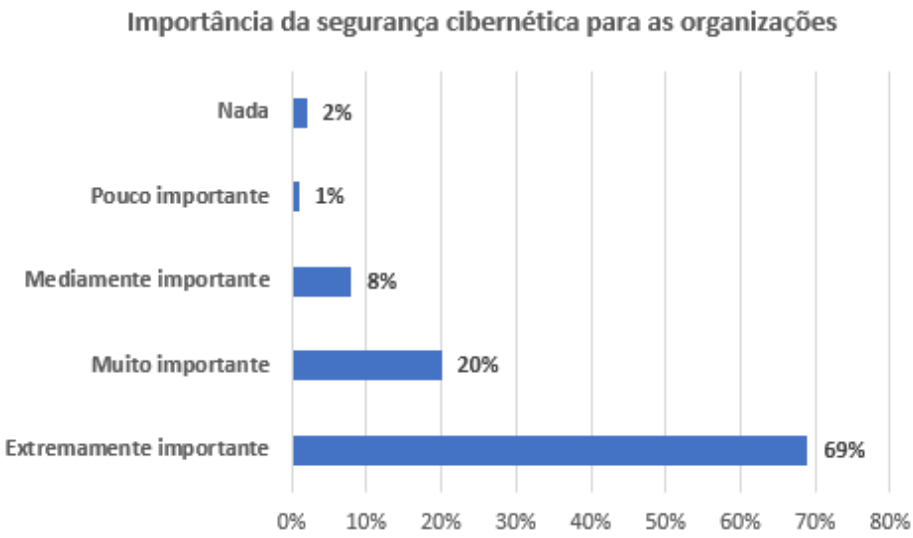

Figura 1.1: Importância da segurança cibernética para as organizações

Fonte: Deloitte [1]

Em contrapartida, segundo pesquisa também publicada em 2019 pela Deloitte [2] a respeito dos principais riscos organizacionais de empresas brasileiras, 83% dos participantes indicaram que os riscos cibernéticos ainda são geridos com grau de maturidade moderado ou baixo, conforme é possível verificar através da figura 1.2.

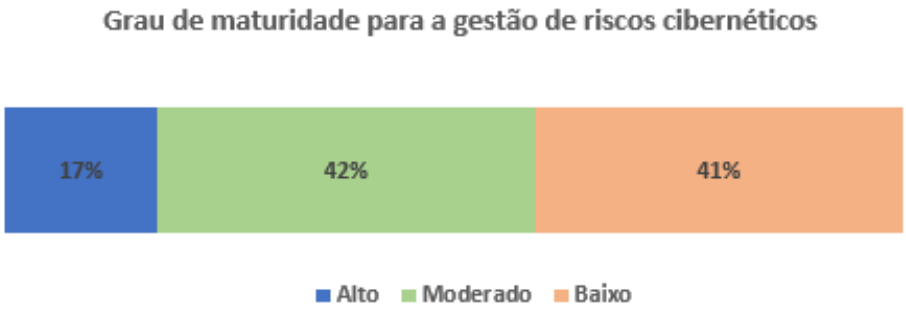

Figura 1.2: Grau de maturidade para a gestão de riscos cibernéticos

Fonte: Deloitte [2]

Por fim, embora a avaliação de riscos cibernéticos seja de grande relevância para as empresas, e por isso, a auditoria interna possa ser uma das linhas de defesa que consiga auxiliar na identificação e no tratamento destes tipos de riscos, foi verificado através de publicação em 2018 da pesquisa realizada pela Deloitte juntamente com o Instituo de Auditores Internos [3] a respeito das tendências e desafios da auditoria interna, que apenas 37% dos líderes da auditoria interna de empresas brasileiras participantes da pesquisa, e 51% de empresas dos demais países,

realizavam avaliações de riscos cibernéticos, conforme é possível verificar através das figura 1.3 e 1.4.

Figura 1.3: Avaliação de risco com foco cibernético – Brasil

Fonte: Deloitte e Instituto de Auditores Internos [3]

Figura 1.4: Avaliação de risco com foco cibernético – Mundo

Fonte: Deloitte e Instituto de Auditores Internos [3]

1.3 – Objetivos

O objetivo principal deste trabalho é analisar a cobertura de atuação da auditoria interna de TI de uma empresa de Telecom, bem como avaliar as deficiências identificadas e os benefícios obtidos através das auditorias realizadas no ambiente tecnológico da empresa. Como objetivos específicos, foram definidos:

- Classificar e analisar as abordagens de atuação das auditorias executadas, bem como identificar os principais processos do COBIT 5 impactados;
- Classificar e analisar os pontos de auditoria encontrados nos trabalhos executados, identificando os principais processos do COBIT 5 impactados. Além disso, verificar se foram identificadas deficiências que impactam no cumprimento pela empresa à Lei Geral de Proteção de Dados (LGPD);
- Classificar e analisar os benefícios obtidos através dos pontos de auditoria levantados.

A importância deste estudo encontra-se na ampliação da visibilidade da atividade de auditoria de TI como um importante instrumento independente de controle e gestão para análise da sistemática da TI das organizações. Além disso, esta pesquisa será relevante para auxiliar gestores na identificação e atuação antecipada em deficiências relacionadas à TI de empresas públicas e privadas, especialmente, de Telecom.

1.4 – Delimitação

O escopo desta pesquisa contemplará a análise dos trabalhos executados nos anos de 2019 e 2020 pela área de auditoria interna de TI de uma empresa que presta serviços de Telecom para todo o Brasil desde 1998 e está situada na cidade do Rio de Janeiro, na qual o autor atua na área desde 2011.

Foi adotada a estratégia de utilizar o período para análise supracitado pois no ano de 2019 foi implementado um novo modelo de governança corporativa na empresa, sendo os trabalhos de auditoria definidos com base no novo planejamento estratégico organizacional. Além disso, esta pesquisa foi executada com base nos relatórios das auditorias executadas entre janeiro de 2019 e novembro de 2020, sendo a coleta e a análise dos dados realizadas entre os meses de julho e novembro de 2020. É válido ressaltar que os projetos de auditoria que compõe o plano anual de trabalhos são distribuídos através de cronograma iniciado sempre no mês de janeiro de cada ano, sendo o último trabalho concluído até o mês de novembro.

Adicionalmente, o escopo desta pesquisa não contemplará a análise sobre os planos de ação acordados pelos auditados para tratamento e correção das deficiências apontadas pela auditoria interna, visto que nem todas as ações definidas para o tratamento dos pontos de auditoria ainda haviam sido implementadas até a conclusão desta pesquisa.

Por fim, este estudo foi realizado com o auxílio do framework COBIT versão 5.

1.5 – Metodologia

Esta pesquisa se classifica como descritiva, pois busca apresentar as características dos trabalhos executados pela área de auditoria de TI da empresa de Telecom analisada. De acordo com Prodanov [4], a pesquisa descritiva é demonstrada quando o pesquisador apenas registra e descreve os fatos observados sem interferir neles. Visa a descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis a partir do uso de técnicas padronizadas de coleta de dados: questionário e observação sistemática. Assume, em geral, a forma de levantamento de informações.

Em relação aos meios, trata-se de pesquisa documental, uma vez que a investigação é realizada com base relatórios internos emitidos pela área de auditoria de TI da empresa de Telecom. Gil [5] destaca que a pesquisa documental se baseia em materiais que não receberam ainda um tratamento analítico ou que podem ser reelaborados de acordo com os objetivos da pesquisa.

A abordagem utilizada nesta pesquisa é a qualitativa no que tange a apresentação dos resultados obtidos, e de acordo com Bogdan & Biklen [6], este tipo de abordagem preocupa-se em compreender um fenômeno em seu ambiente natural, onde esses ocorrem e do qual faz parte. Quanto aos procedimentos técnicos, utilizou-se a técnica de pesquisa documental com análise de conteúdo dos relatórios de auditorias de TI realizadas no período de 2019 a 2020.

1.6 – Descrição

No capítulo 2 apresenta todo o embasamento teórico da pesquisa, definindo o conceito de auditoria interna e auditoria de TI, apresentando a forma de atuação da auditoria interna de TI na empresa de Telecom analisada e explicará o framework COBIT 5.

O capítulo 3 apresenta a metodologia utilizada nesta pesquisa, definindo-se o universo para análise e a forma de coleta, tratamento e análise dos dados utilizados para este trabalho.

O capítulo 4 apresenta os resultados encontrados, sendo analisada a cobertura do escopo de atuação da auditoria de TI, a relação das principais deficiências existentes na área de TI da empresa e os benefícios obtidos com os resultados das auditorias realizadas.

O capítulo 5 contém a conclusão deste trabalho e a sugestão para pesquisas futuras.

Capítulo 2

Embasamento Teórico

2.1 – Auditoria interna

2.1.1 – Definição e objetivo da auditoria interna

Gherman [7] define que os controles internos são definidos pela totalidade das políticas, procedimentos e práticas estabelecidas pela administração, para assegurar que os riscos inerentes às atividades da instituição sejam identificados e gerenciados adequadamente, com a finalidade maior de fornecer razoável garantia à administração de que os objetivos de negócio sejam continuamente alcançados.

Estruturar, implementar e manter eficaz um ambiente de controles internos se tornou indispensável para o êxito das empresas, tanto para detectar e controlar os riscos operacionais, quanto para ajustar políticas e procedimentos internos para atenderem aos regimentos.

Neste sentido, a auditoria interna realiza um importante papel no processo de governança e no ambiente de controles internos das empresas. De acordo com Instituto de Auditores Internos [8] ela tem a seguinte definição: “A auditoria interna é uma atividade independente e objetiva de avaliação e consultoria, criada para agregar valor e melhorar as operações de uma organização. Ela auxilia a organização a atingir seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada à avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, controle e governança”.

Ainda segundo o Instituto de Auditores Internos [8], a auditoria interna tem como missão dentro de uma organização: “Aumentar e proteger o valor organizacional, fornecendo avaliação (assurance), assessoria (advisory) e conhecimento (insight) objetivos baseados em riscos”.

Carneiro [9] define auditoria interna como sendo: “Uma técnica de controle de gestão que, mediante a análise, verificação e avaliação independente das atividades da empresa, e da eficácia e conformidade do funcionamento das demais técnicas de controle, tem em vista auxiliar os gestores no desempenho das suas funções e responsabilidades”.

Crepaldi [10] apresenta a auditoria interna como sendo um processo de controle gerencial: “É executada por um profissional ligado à empresa, ou por uma seção própria para tal fim, sempre em linha de dependência da direção empresarial. O auditor interno é a pessoa de confiança dos dirigentes, está vinculado à empresa por contrato trabalhista continuando e sua intervenção é permanente. Sua área de atuação envolve todas as atividades da empresa, predominam a verificação constante dos controles internos, a manipulação de valores e a execução de rotinas administrativas”.

De acordo com os princípios do modelo das três linhas do Instituto de Auditores Internos [11], dentro de uma estrutura organizacional a auditoria interna assume o papel da terceira linha de defesa, sendo responsável pela avaliação e assessoria independente e objetiva sobre questões relativas ao atingimento dos objetivos. Com isso, reporta as deficiências e oportunidades de melhoria identificadas durante as avaliações à gestão e ao órgão de governança a fim de promover a melhoria contínua. Segue abaixo a figura 2.1 apresentando o modelo de três linhas:

Figura 2.1: O modelo das três linhas
Fonte: Instituto de Auditores Internos [11]

Diante do contexto apresentado, entende-se que a auditoria interna é, portanto, um instrumento dentro da organização responsável por verificar de forma sistemática os processos de controles internos e atestar de forma independente que os controles existentes para mitigar os riscos da organização são adequados e efetivos.

2.1.2 – Tipos de auditoria interna

De acordo com Dias [12], os serviços de auditoria interna podem ser subdivididos através dos seguintes tipos:

- Auditoria contábil e financeira: Tem como objetivo avaliar os processos que suportam as demonstrações financeiras da empresa, através da análise de procedimentos e controles contábeis, além da aderência destes aos regulamentos contábeis;
- Auditoria de processos/operação; Visa melhorar a eficiência dos processos, bem como minimizar custos, através da avaliação quanto aderência dos controles internos da organização em relação aos procedimentos e regulamentos formalizados junto à alta administração;
- Auditoria fiscal: Tem como objetivo realizar uma avaliação sobre os aspectos fiscais e tributários de uma organização a fim de evitar que a empresa seja notificada pelo fisco devido a erros tributários;
- Auditoria de gestão: Tem como objetivo avaliar o desempenho da gestão sobre a rentabilidade da organização. Nesta linha de atuação, a ação da auditoria de gestão tem como enfoque as análises sobre fatores como custo/ benefício, riscos e processo decisório dos gestores;
- Auditoria de TI: Tem como objetivo avaliar os controles de infraestrutura, políticas e operações de TI de uma organização. Ela verifica se os controles de TI protegem os ativos corporativos, garantem a integridade dos dados e estão alinhados com os objetivos gerais de negócio da empresa;

2.2 – Auditoria de TI

2.2.1 – Importância e conceito

A TI tornou-se um instrumento obrigatório, pois possibilita acelerar o processamento da informação, trazendo revolução ao substituir os antigos livros contábeis e documentações em papel, além de fornecer maior velocidade no processamento e saída de informações essenciais para a tomada de decisão nas companhias.

De acordo com Braz [13], as organizações que possuem ambientes de controles internos fortes tendem a apresentar melhores e mais confiáveis ambientes de tecnologia da informação. Desta forma, cada vez mais cresce a importância dada aos processos organizacionais de governança e de gestão de TI, que nada mais são do que controles internos da organização. Com isso, a disponibilidade, integridade e confidencialidade das informações em um ambiente suportado pela tecnologia passou a ter grande relevância.

Neste contexto, a modalidade da auditoria de TI, também conhecida como auditoria de sistemas, computacional ou informática, passou a ganhar cada vez mais espaço dentro do escopo de atuação na terceira linha de defesa proposto pelo Instituto de Auditores Internos [11] já que ela tem como viés avaliar os controles de infraestrutura, políticas e operações de TI dentro das empresas.4

De acordo com Braz [13], é possível entender a auditoria de TI como um tipo de fiscalização voltada à avaliação da utilização e da gestão dos recursos tecnológicos pelas empresas.

Dias [14] define a auditoria de TI como sendo um tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informação, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências.

Segundo Chaves [15]: “A auditoria de sistemas analisa o ambiente computacional e a segurança de informações testando e avaliando com profundidade todos os controles num sistema informatizado, abrangendo suas aplicações e produtos”.

2.2.2 – Abordagens das auditorias de TI

Devido à complexidade da estrutura de um ambiente tecnológico, o serviço de auditoria de TI pode ser dividido em distintas abordagens de atuação, diferenciadas pelo objetivo e escopo do trabalho a ser executado, bem como do objeto a ser auditado.

Segundo Braz [13], estas abordagens possuem intersecções que se correlacionam dentro de uma estrutura de governança de TI. Por isso, objetos focais de avaliação dentro de uma abordagem são também abordados perifericamente em outras, não sendo raro que os trabalhos de auditoria adotem procedimentos inerentes a mais de uma abordagem. A figura 2.2 ilustra as principais abordagens definidas por Braz [13]:

Figura 2.2: Abordagens da auditoria de TI
Fonte: Elaborado pelo autor

Ao estabelecer uma abordagem, é viável identificar quais são as principais particularidades que uma auditoria apresentará, a quantidade de recursos necessários, o prazo estimado para execução e os possíveis riscos existentes no trabalho. Seguem abaixo maiores detalhes a respeito das abordagens apresentadas acima por Braz [13]:

- Auditoria de governança e de gestão de TI: Atua em aspectos de liderança, de planejamento e de gerenciamento da área de TI e objetiva avaliar que a gestão dos serviços, dos investimentos, das despesas, das políticas, dos processos e da própria estrutura organizacional convirjam para que a companhia atinja seus objetivos de forma efetiva;
- Auditoria de segurança da informação: Avalia como a empresa atua na gestão da segurança da informação, no controle dos ativos e na gestão dos riscos envolvidos em seus sistemas e ambiente;
- Auditoria de contratações de TI: Atua na avaliação sobre os processos de planejamento e execução de pagamentos e contratações, bem como na gestão dos contratos da área de TI;
- Auditoria de sistemas de informação: Avalia diversos aspectos em um sistema de informação: integridade, disponibilidade, confidencialidade, aderência às regras de negócio e normas (conformidade), controles de entrada, processamento e saída de dados, efetividade, satisfação e usabilidade;
- Auditoria de tecnologia: Aborda aspectos técnicos da infraestrutura tecnológica, como os de sistema operacional, de redes de comunicação e de banco de dados, além de aspectos operacionais de processamento dos recursos tecnológicos, como os de configuração e de produção;

Foram escolhidas as cinco abordagens apresentadas acima para embasarem esta pesquisa, já que estas propostas apresentadas por Braz [13] estão em linha com os trabalhos executados pela área de auditoria de TI analisada através desta pesquisa.

2.3 – Atuação da auditoria interna de TI

2.3.1 – Objetivos e atuação

A área de auditoria interna de TI observada nesta pesquisa faz parte da diretoria de auditoria interna da empresa Telecom analisada. Ela presta serviços de avaliação (assurance) e consultoria com o objetivo de adicionar valor e melhorar as operações da organização. Além disso, ela auxilia a companhia a realizar seus objetivos estratégicos de negócio e de TI a partir da aplicação de uma abordagem de nível técnico para avaliar e melhorar a eficácia de seus processos de gerenciamento de riscos, controle e governança.

Para conduzir as responsabilidades da atividade de auditoria interna, o chief audit executive (CAE) tem acesso direto e irrestrito ao Conselho e à alta administração da companhia, tendo assim o apoio para executar seus trabalhos de maneira imparcial e independente. Essa independência se divide em dois aspectos: organizacional (posição da área na empresa e sua linha de reporte) e comportamental (objetividade de seus membros na execução dos trabalhos).

A auditoria interna reporta-se funcionalmente ao presidente do conselho de administração e administrativamente ao diretor presidente da empresa. Isso permite à auditoria interna estar próxima ao negócio, enquanto sua ligação direta ao Comitê de Auditoria, Riscos e Controles (CARC) garante que está livre de interferências na determinação do escopo das auditorias, execução de trabalhos e comunicação de resultados. O CARC é composto por membros do conselho de administração da empresa e possui, entre suas atribuições, a responsabilidade pela supervisão da função de Auditoria Interna. A figura 2.3 ilustra o posicionamento da auditoria interna dentro do organograma da empresa.

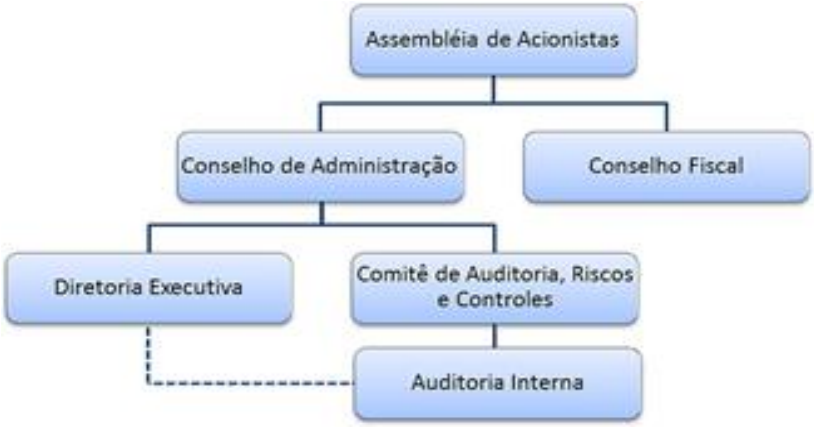

Figura 2.3: Organograma Auditoria Interna
Fonte: Elaborado pelo autor

2.3.2 – Metodologia de execução da auditoria

A auditoria interna de TI deve executar suas atividades de maneira sistemática e disciplinada, com o zelo profissional devido e de forma padronizada. Para isso, ela possui processo e metodologia padronizados para assegurar a qualidade e controle dos trabalhos realizados. As principais etapas das atividades executadas pela auditoria são:

- *PLAN* (Planejamento): Etapa onde é realizado o entendimento sobre a matéria auditada. Para isso, é desenvolvido e documentado um planejamento para cada trabalho, com um maior detalhamento dos objetivos, escopo (abrangência e exclusão), prazos, recursos, riscos preliminarmente identificados e os seus controles chave. Ao final são definidos os testes para execução da auditoria;

- FIELDWORK (Trabalho de campo): Para cada risco preliminarmente identificado na fase de planejamento, os controles devem ser avaliados quanto ao seu funcionamento e eficácia a fim confirmar a mitigação dos respectivos riscos. Para isto, devem ser realizados testes que evidenciem se os controles avaliados são eficazes, ineficazes ou inexistentes. Caso seja encontrada durante os testes alguma inconformidade ou inexistência de controle, são definidos Pontos de Auditoria (PTA) a fim de apresentar as deficiências identificadas. Além disso, os riscos associados aos PTA são

analisados e classificados pelos auditores de acordo com sua probabilidade de ocorrência e impacto (rating). Seguem abaixo as classificações adotadas para os riscos envolvidos:

- Baixo;
- Moderado;
- Significativo;
- Alto.

A tabela 2.1 e o quadro 2.1 apresentam detalhes a respeito dos critérios adotados para definição da probabilidade e do impacto que determinam a classificação dos riscos:

Tabela 2.1: Probabilidade dos riscos

%	Descrição	Detalhes dos critérios de probabilidade
1% a 30%	Baixa	Não é provável que aconteça ou pode ser que ocorra uma vez dentro de um ano.
31% a 50%	Moderada	Pode ser que ocorra mais de uma vez dentro de um ano.
51% a 70%	Significativa	Pode ser que ocorra mensalmente.
71% a 90%	Alta	Pode ser que ocorra semanalmente.

Fonte: Elaborado pelo autor

Quadro 2.1: Impacto dos riscos

Impacto	Detalhes dos critérios de impacto
Baixo	Os riscos possuem consequências pouco significativas ou consequências reversíveis em curto e médio prazo com custos pouco significativos.
Moderado	Os riscos possuem consequências reversíveis em curto e médio prazo com custos baixos.
Significativo	Os riscos possuem consequências reversíveis em curto e médio prazo com custos altos.
Alto	Os riscos possuem consequências irreversíveis ou com custos inviáveis.

Fonte: Elaborado pelo autor

- REPORT (Comunicação dos Resultados): O relatório de auditoria é o documento elaborado pelo auditor responsável para formalizar junto à

organização a comunicação dos resultados obtidos, onde são detalhados os PTA identificados, as classificações de risco associados aos PTA e os planos de ação definidos pelos auditados para resolver as deficiências em questão. O reporte, seja ele no ambiente interno, quanto para eventual disponibilização de material para partes externas à organização, deve ser previamente avaliado e aprovado pelo CAE;

- FUP (Follow-up, acompanhamento dos planos de ação): O acompanhamento da implementação dos planos de ação (follow-up) é um instrumento do processo de auditoria, pois, apesar de não ser responsável pela implementação dos planos de ação, a auditoria interna deve acompanhar a implementação deles visando garantir que as soluções acordadas sejam efetivamente aplicadas e os riscos associados mitigados. O cumprimento e a realização das ações corretivas ou de melhoria, dentro do prazo estabelecido, denota que a área auditada reconhece a importância das mudanças geradas e o valor agregado com base na adoção das ações recomendadas;

A figura 2.4 ilustra de forma resumida o fluxo das fases que compõe a metodologia da auditoria:

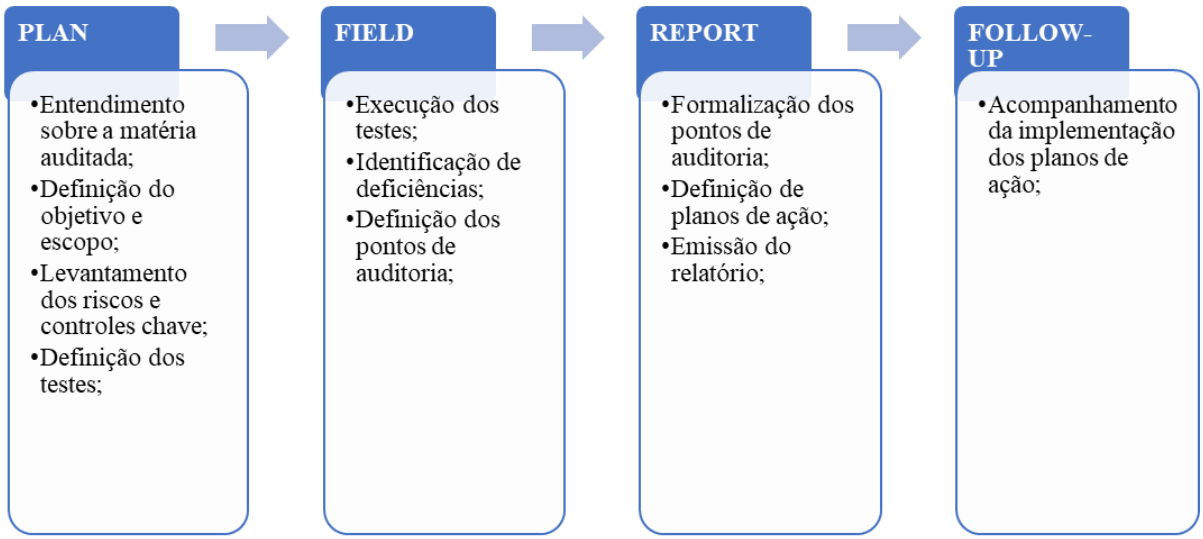

Figura 2.4: Fases da metodologia da auditoria
Fonte: Elaborado pelo autor

Todas as fases supracitadas são interdependentes, formando um ciclo cujo produto é o valor adicionado pela auditoria à organização. Adicionalmente, todos os assuntos abordados como tema dos projetos de auditoria são estrategicamente definidos no plano anual de auditoria. A elaboração deste plano ocorre previamente ao ano vigente, através de um processo estruturado baseado em riscos, considerando a estrutura de Gerenciamento de Riscos da companhia (Enterprise Risk Management), que envolve também uma série de reuniões com o corpo de diretores da companhia, componentes do conselho de administração, análise de informações suporte e de documentações estratégicas da empresa.

2.4 – COBIT 5

O COBIT 5 é um framework elaborado pelo ISACA (Information Systems Audit and Control Association) que fornece uma estrutura para auxiliar as empresas a alcançarem seus objetivos de governança e gestão de TI. Ele foi desenvolvido para auxiliar as empresas a atingirem maior valor através da TI, mantendo um balanceamento entre a realização de benefícios e a otimização de recursos e níveis de risco assumidos. De acordo com o ISACA [16], "O COBIT 5 permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI".

Adicionalmente, o COBIT 5 também pode ser utilizado por auditores como um guia que apresenta uma série de melhores práticas que podem servir como base para avaliação da conformidade do ambiente de TI das organizações. Conforme definido pelo ISACA [16], o COBIT 5 é baseado nos cinco princípios chave para a governança e gestão de TI das empresas, conforme demonstrado através da figura 2.5:

Figura 2.5: Os cinco princípios do COBIT 5.
Fonte: ISACA [16]

O modelo do COBIT 5 apresenta uma clara diferenciação entre as práticas de governança e gestão, conforme segue abaixo:

- Governança: "A governança garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos" [16].
- Gestão: "A gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos" [16].

Na maioria das organizações, a gestão é de responsabilidade da diretoria executiva sob a liderança do Chief Executive Officer (CEO). Adicionalmente, o COBIT 5 sugere a implementação de processos de governança e gestão de tal forma que as principais áreas sejam cobertas, conforme demonstrado na figura 2.6:

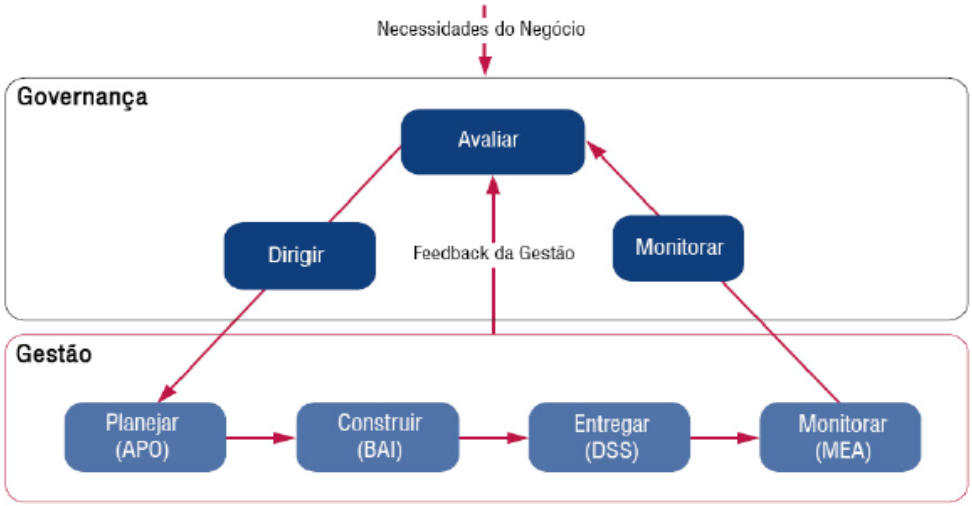

Figura 2.6: Modelo de referência de processo
Fonte: ISACA [16]

Neste sentido, conforme apresentado na figura 2.7, o COBIT 5 inclui um modelo de referência de processos, que determina e explica detalhadamente uma cadeia de 37 processos de governança e gestão. Este modelo de referência divide os processos de governança e gestão de TI da organização em dois domínios de processo principais:

- Governança – Inclui cinco processos de governança onde são definidas práticas para Avaliar, Dirigir e Monitorar (Evaluate, Direct and Monitor – EDM).

- Gestão – Inclui quatro domínios, em concordância com as áreas das empresas responsáveis por planejar, construir, executar e monitorar (Plan, Build, Run and Monitor – PBRM), e oferece cobertura de TI de ponta a ponta, conforme apresentado detalhadamente abaixo:

    - Alinhar, Planejar e Organizar (Align, Plan and Organise – APO);
    - Construir, Adquirir e Implementar (Build, Acquire and Implement – BAI);
    - Entregar, Serviços e Suporte (Deliver, Service and Support – DSS);
    - Monitorar, Avaliar e Analisar (Monitor, Evaluate and Assess – MEA);

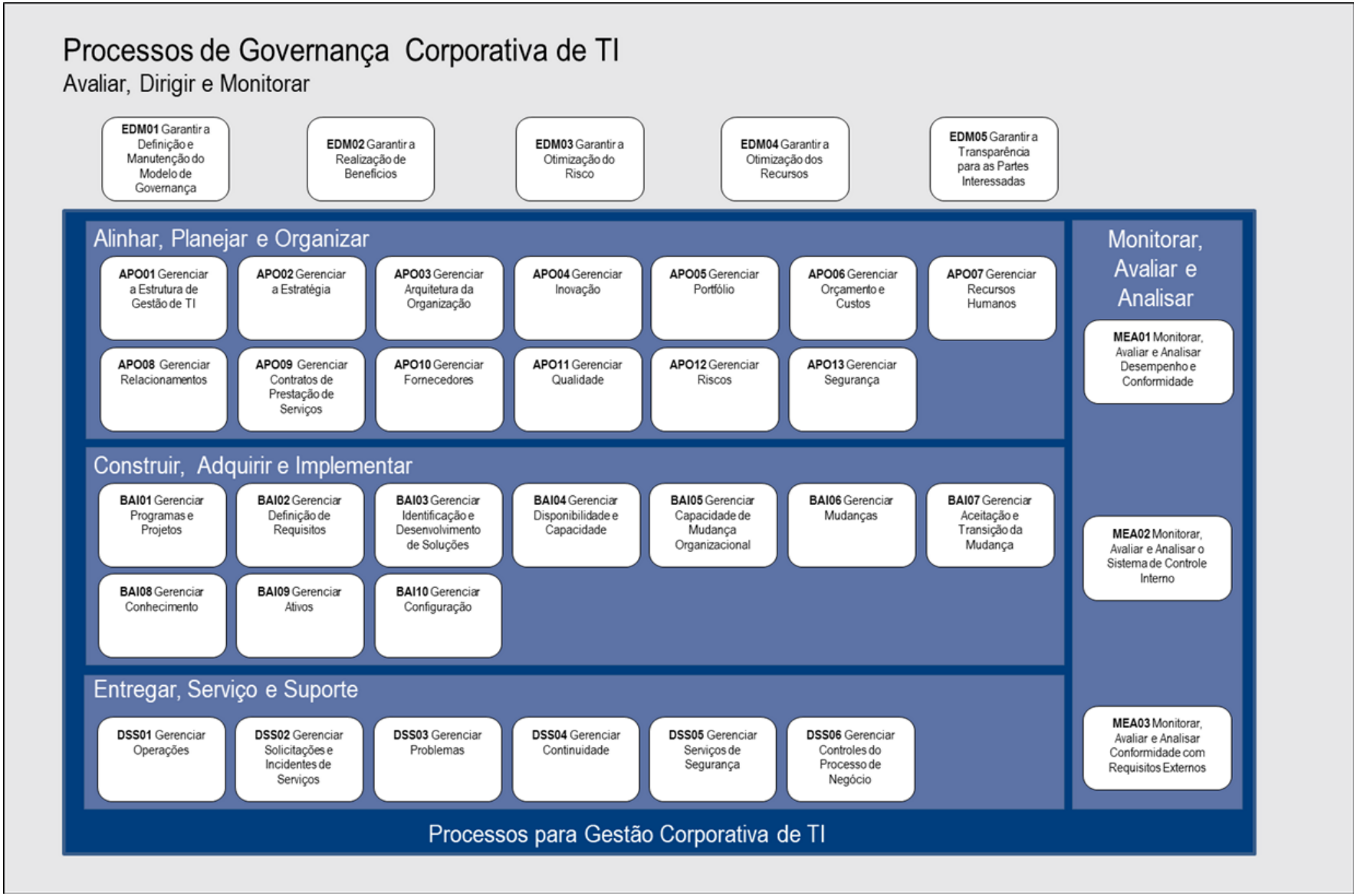

Figura 2.7: Processos de Gestão e Governança Corporativa de TI.
Fonte: ISACA [16]

2.5 – LGPD

Dada a importância cada vez maior sobre a informação, juntamente com o avanço digital, surgiu a necessidade das empresas protegerem os dados pessoais pertencentes aos seus clientes e profissionais em razão do crescente risco de manipulação e utilização desses dados contra seus detentores. Diante deste cenário, surgiu no Brasil [17] a lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), como objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei estabelece os direitos e as obrigações relacionados ao tratamento de dados pessoais, em qualquer meio, seja ele digital ou material, por pessoa física ou jurídica, calcados nesses direitos fundamentais, tendo como premissa a boa-fé. Neste sentido, ela determina regras sobre a coleta, armazenamento, tratamento e compartilhamento de dados, impondo mais proteção e penalidades para o não cumprimento. A lei entende por "dados pessoais" qualquer informação relacionada à pessoa natural identificada ou identificável, e por "tratamento de dados" toda operação realizada com dados pessoais.

A lei define os seguintes princípios para as organizações obedecerem quanto ao tratamento de dados:

- Finalidade: O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados.

- Adequação: Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela empresa.

- Necessidade: As empresas devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades.

- Livre acesso: A pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito. Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo.

- Qualidade dos dados: Deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.

- Transparência: Todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras. Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas de forma oculta.

- Segurança: É responsabilidade das empresas buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de acessos por terceiros, ainda que não sejam autorizados, como nos casos de invasões por hackers. Além disso, devem ser tomadas medidas para solucionar situações acidentais, como destruição, perda, alteração, comunicação ou difusão dos dados pessoais de suas bases.

- Prevenção: O princípio da prevenção objetiva que as empresas adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais.

- Não Discriminação: Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares.

- Responsabilização e Prestação de Contas: Além de se preocuparem em cumprir integralmente a Lei, as empresas devem ter provas e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência.

Capítulo 3

Proposta Metodológica

As etapas que compõe a proposta metodológica definida para a realização deste estudo estão ilustradas através da figura 3.1, elas são detalhadas nas subseções seguintes e permitem entender as atividades realizadas para a definição da população e amostra para a pesquisa. A forma utilizada para a coleta dos dados necessários, além do tratamento e das análises realizadas para atingir os objetivos propostos para este estudo.

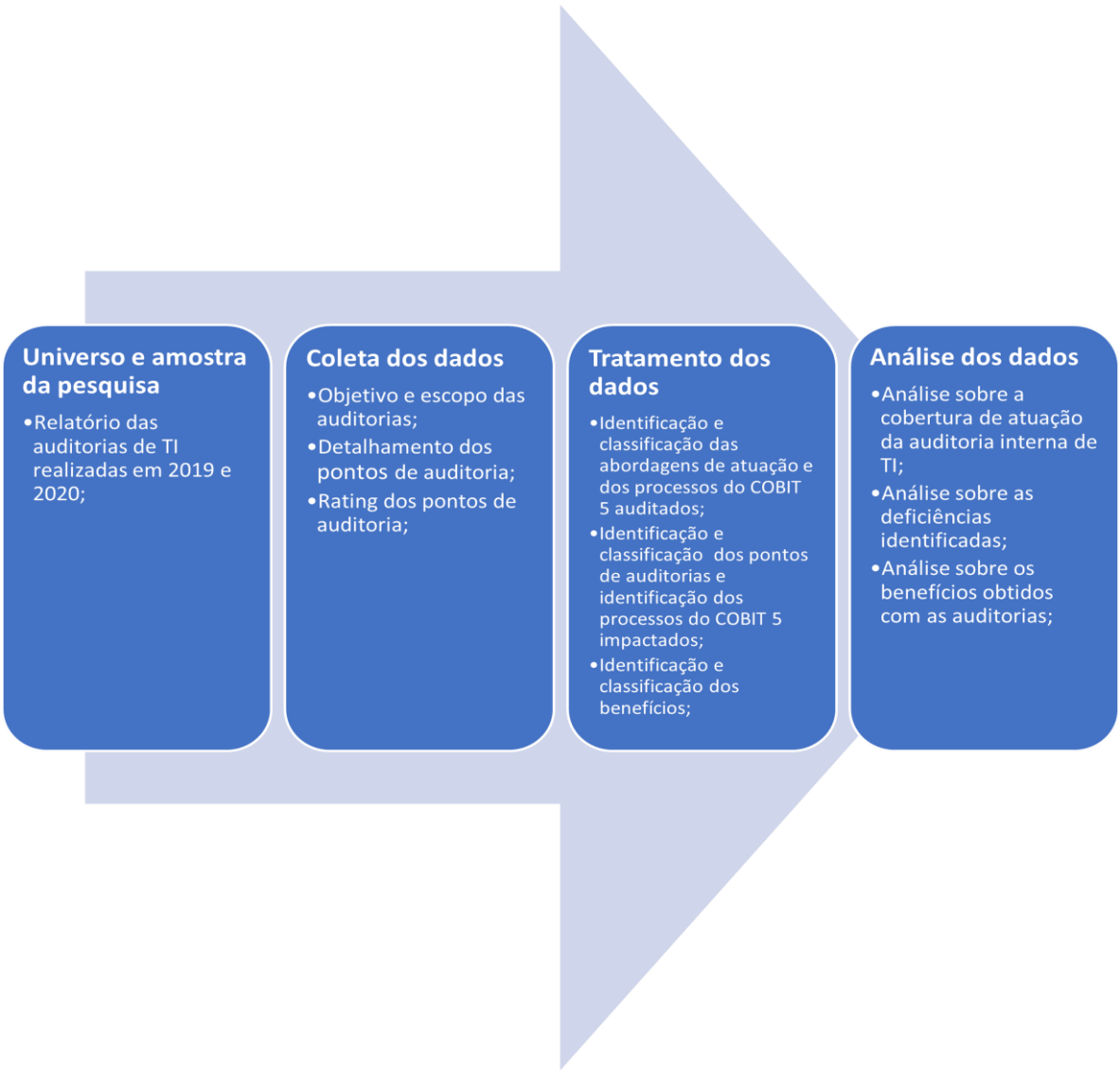

Figura 3.1: Etapas da proposta metodológica
Fonte: Elaborado pelo autor

3.1 – Universo e amostra da pesquisa

De acordo com VERGARA [18], o universo é o conjunto de elementos que possuem as características que serão objeto do estudo, e a amostra, ou população amostral, é uma parte do universo escolhido selecionada a partir de um critério de representatividade. Para a realização deste estudo, o universo utilizado foi composto dos 39 relatórios de auditoria emitidos em 2019 e 2020 pela área de auditoria interna TI. Adicionalmente, não foi necessária seleção de uma amostra para a realização da pesquisa, visto que foram utilizados 100% dos relatórios de auditoria emitidos pela área no período analisado.

3.2 – Coleta dos dados

A coleta dos dados para esta pesquisa foi realizada partir da verificação de conteúdo de 39 relatórios emitidos pela auditoria interna de TI em 2019 e 2020, onde foram levantadas as seguintes informações:

- Objetivo e escopo dos trabalhos;
- Detalhamento dos pontos de auditoria;
- Rating dos pontos de auditoria;

Neste sentido, os relatórios de auditoria serviram como fonte de dados para identificação das abordagens de atuação nas auditorias, das deficiências observadas nos trabalhos, da classificação dos apontamentos reportados e dos benefícios ou ganhos financeiros obtidos com os trabalhos.

3.3 – Tratamento e análise dos dados

A partir da verificação do conteúdo de cada um dos 39 relatórios e com o objetivo de identificar os temas das auditorias apresentadas no universo foi realizado o relacionamento do objetivo e escopo de cada um dos projetos às abordagens de atuação da auditoria de TI sugeridas por Braz [13], já que estas estão em linha com os trabalhos executados pela área analisada nesta pesquisa. Após a definição das abordagens de atuação relacionadas a cada um dos trabalhos, foram identificados os processos do COBIT 5 relacionados ao objetivo e escopo de cada um

dos projetos apresentados no universo. A análise dos dados levantados seguiu com base na quantificação das auditorias realizadas a partir dos tipos de abordagem sugeridas por Braz [13] e, principalmente, dos processos do COBIT 5 associados, possibilitando avaliar a regularidade e cobertura de atuação da área de auditoria.

Posteriormente, foi efetuada a categorização dos PTA através do entendimento a respeito da natureza das deficiências relacionadas aos respectivos pontos, sendo realizado o agrupamento dos PTA de acordo as suas categorias. Em seguida, foram identificados os processos do COBIT 5 impactados através das deficiências em questão. A análise dos PTA também seguiu com base na quantificação das suas categorias, possibilitando identificar quais as deficiências no ambiente de TI da empresa apontadas regularmente nas auditorias, as deficiências identificadas que impactam à adequação da organização à LGDP, além dos processos do COBIT 5 frequentemente avaliados.

Por fim, foi realizado o levantamento sobre os benefícios obtidos a partir do conteúdo dos PTA apresentados, sendo realizada a análise e classificação dos ganhos obtidos, considerando também as suas naturezas. A análise dos benefícios também seguiu com base na quantificação das suas categorias, possibilitando identificar quais os principais ganhos obtidos com as auditorias. Com base nos levantamentos supracitados, foram definidas estruturas de tabelas a fim de auxiliar nas análises dos dados coletados nos relatórios de auditorias, sendo também elaborados gráficos para auxiliar na representação do resultado das análises realizadas.

Capítulo 4

Resultados Obtidos

Neste capítulo serão apresentados maiores detalhes a respeito dos resultados das análises de conteúdo realizadas nos 39 relatórios emitidos para os 39 trabalhos executados em 2019 e 2020 pela área de auditoria interna de TI da empresa de Telecom, os quais resultaram na definição de 103 PTA referentes às deficiências apontadas pela auditoria. O Apêndice 1 apresenta o total de PTA definidos para cada trabalho realizado.

4.1 – Análise da cobertura de atuação da auditoria interna de TI

A tabela 4.1 apresenta o relacionamento dos trabalhos de auditoria TI às propostas de abordagem de atuação sugeridas por Braz [13]. Ao analisá-la é possível verificar que 24 trabalhos (62%) tiveram mais de uma abordagem como escopo de atuação nas auditorias. Neste sentido, é possível constatar que a maioria dos trabalhos de auditoria de TI apresentam objetivos e escopos abrangentes e transversais que integram mais de uma abordagem para avaliação do objeto a ser auditado. Adicionalmente, a figura 4.1 apresenta o gráfico da quantidade de trabalhos realizados segmentados pela quantidade de abordagens de atuação adotadas para um trabalho:

Tabela 4.1: Trabalhos de auditoria relacionados às abordagens de atuação

Ano	Códigos dos trabalhos	Auditoria de governança e de gestão de TI	Auditoria de segurança da informação	Auditoria de sistemas de informação	Auditoria de tecnologia	Auditoria de contratações de TI
2019	AUD_TI901		X			
	AUD_TI902	X				
	AUD_TI903	X	X	X	X	
	AUD_TI904	X	X	X	X	
	AUD_TI905	X				X
	AUD_TI906	X				
	AUD_TI907	X				
	AUD_TI908					X
	AUD_TI909	X				
	AUD_TI910	X				
	AUD_TI911	X	X	X	X	X
	AUD_TI912	X	X	X	X	
	AUD_TI913	X	X	X	X	
	AUD_TI914	X	X	X	X	
	AUD_TI915	X	X	X	X	
	AUD_TI916	X	X	X	X	
	AUD_TI917	X	X	X	X	
	AUD_TI918	X	X	X	X	
	AUD_TI919	X	X	X	X	
	AUD_TI920	X				
2020	AUD_TI2001	X				
	AUD_TI2002	X				
	AUD_TI2003	X	X	X	X	
	AUD_TI2004	X	X	X	X	
	AUD_TI2005	X	X	X	X	
	AUD_TI2006	X	X	X	X	
	AUD_TI2007	X	X	X	X	
	AUD_TI2008					X
	AUD_TI2009	X	X	X	X	
	AUD_TI2010		X			
	AUD_TI2011					X
	AUD_TI2012	X				
	AUD_TI2013	X	X	X	X	
	AUD_TI2014	X	X	X	X	
	AUD_TI2015	X	X	X	X	
	AUD_TI2016	X	X	X	X	
	AUD_TI2017	X	X	X	X	
	AUD_TI2018	X				
	AUD_TI2019	X	X	X	X	
Total		**34**	**25**	**23**	**23**	**5**

Fonte: Elaborado pelo autor

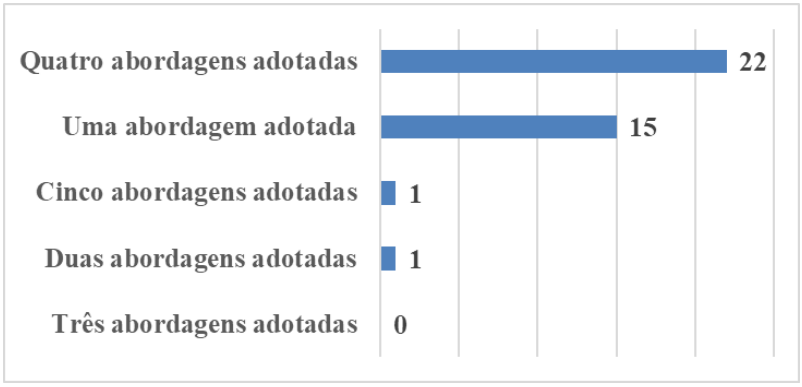

Figura 4.1: Trabalhos *versus* Abordagens de atuação
Fonte: Elaborado pelo autor

Adicionalmente, analisando ainda a tabela 4.1, é possível verificar que a dimensão Governança e Gestão de TI foi a que mais esteve presente dentro do escopo de atuação da auditoria de TI, sendo avaliada em 34 trabalhos (87%). As abordagens "Segurança da Informação" (25 trabalhos – 64%), "Sistemas de Informação" (23 trabalhos – 59%) e "Tecnologia" (23 trabalhos – 59%) também fizeram parte do escopo de mais da metade dos trabalhos. Abaixo, encontra-se a figura 4.2, ilustrando a quantidade de trabalhos por tipo de abordagem de atuação:

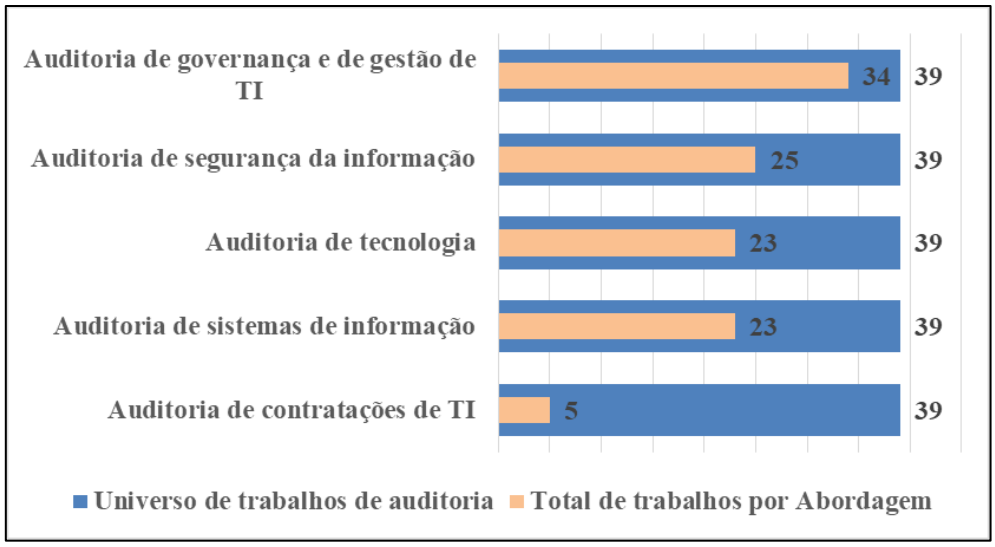

Figura 4.2: Trabalhos *versus* Tipos de abordagens de atuação
Fonte: Elaborado pelo autor

Posteriormente, a tabela 4.2 apresenta a relação dos 39 trabalhos de auditoria de TI relacionados aos processos do COBIT 5 a partir do objetivo e escopo de cada trabalho:

Tabela 4.2: Trabalhos de auditoria relacionados aos processos do COBIT 5

Ano	Códigos dos trabalhos	Processos COBIT 5												
		APO02	APO05	APO06	APO09	APO10	APO13	BAI01	BAI07	BAI09	DSS04	DSS05	DSS06	MEA03
2019	AUD_TI901						X							X
	AUD_TI902									X				
	AUD_TI903										X	X	X	
	AUD_TI904										X	X	X	
	AUD_TI905				X	X								
	AUD_TI906	X												
	AUD_TI907	X												
	AUD_TI908											X	X	
	AUD_TI909											X	X	
	AUD_TI910		X		X			X		X				
	AUD_TI911											X	X	
	AUD_TI912										X	X	X	
	AUD_TI913				X	X						X	X	
	AUD_TI914											X	X	
	AUD_TI915											X	X	
	AUD_TI916										X	X	X	
	AUD_TI917								X				X	
	AUD_TI918				X	X					X	X	X	
	AUD_TI919											X	X	
	AUD_TI920									X				X
2020	AUD_TI2001			X	X								X	
	AUD_TI2002			X									X	
	AUD_TI2003											X	X	
	AUD_TI2004											X	X	
	AUD_TI2005										X	X	X	
	AUD_TI2006											X	X	
	AUD_TI2007										X	X	X	
	AUD_TI2008			X	X	X								
	AUD_TI2009											X	X	
	AUD_TI2010						X							X
	AUD_TI2011			X	X	X								
	AUD_TI2012			X	X			X						
	AUD_TI2013										X	X	X	
	AUD_TI2014										X	X	X	
	AUD_TI2015										X	X	X	
	AUD_TI2016										X	X	X	
	AUD_TI2017											X	X	
	AUD_TI2018											X	X	X
	AUD_TI2019											X	X	X
Total		2	1	5	8	5	2	2	1	3	11	25	28	5

Fonte: Elaborado pelo autor

Ao examinar a tabela 4.2 percebe-se que, conforme o resultado da análise das auditorias em relação às abordagens de atuação apresentadas por Braz [13], o objetivo e escopo dos trabalhos também estão relacionados a mais de um processo do COBIT 5, ou seja, um trabalho de auditoria pode abranger a avaliação de mais de um processo do COBIT 5. Segue abaixo a

figura 4.3 apresentando o resumo da quantidade de trabalhos realizados segmentados pela quantidade de processos do COBIT 5 analisados em um trabalho:

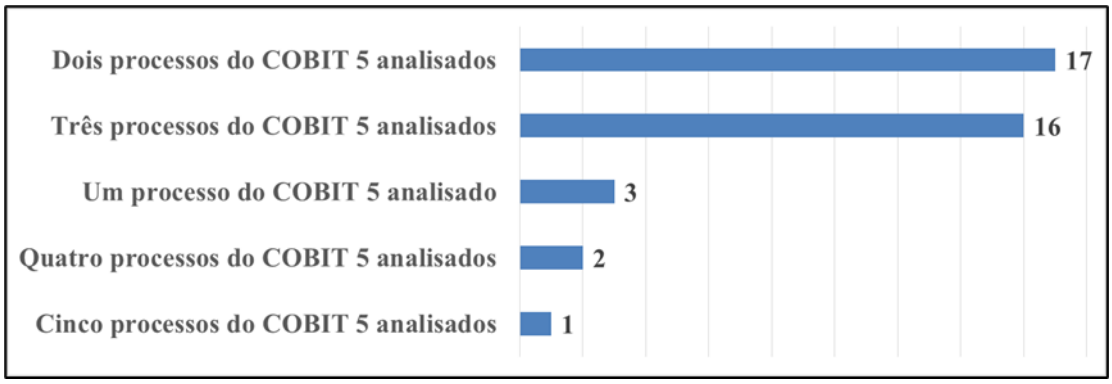

Figura 4.3: Trabalhos *versus* Processos COBIT 5
Fonte: Elaborado pelo autor

Em relação a cobertura de avaliação dos processos do COBIT 5, é possível verificar que do total de 37 processos de governança e gestão disponibilizados no framework, 13 foram analisados em 2019 ou 2020, que corresponde a 35%. Além disso, foi observado que a auditoria de TI atuou com maior frequência (acima de 50%) na avaliação dos processos "DSS06 Gerenciar Controles do Processo de Negócio" (28 trabalhos – 72%) e "DSS05 Gerenciar Serviços de Segurança" (25 trabalhos – 64%), e com menor frequência (abaixo de 10%) nos processos "APO05 Gerenciar Portfólio" (1 trabalho – 3%), "BAI07 Gerenciar Aceitação e Transição da Mudança" (1 trabalho – 3%), "APO02 Gerenciar a Estratégia" (2 trabalhos – 5%), "APO02 Gerenciar Segurança" (2 trabalhos – 5%), "BAI01 Gerenciar Programas e projetos" (2 trabalhos – 5%) e "BAI09 Gerenciar Ativos" (3 trabalhos – 8%), conforme é possível é possível verificar através do gráfico na figura 4.4:

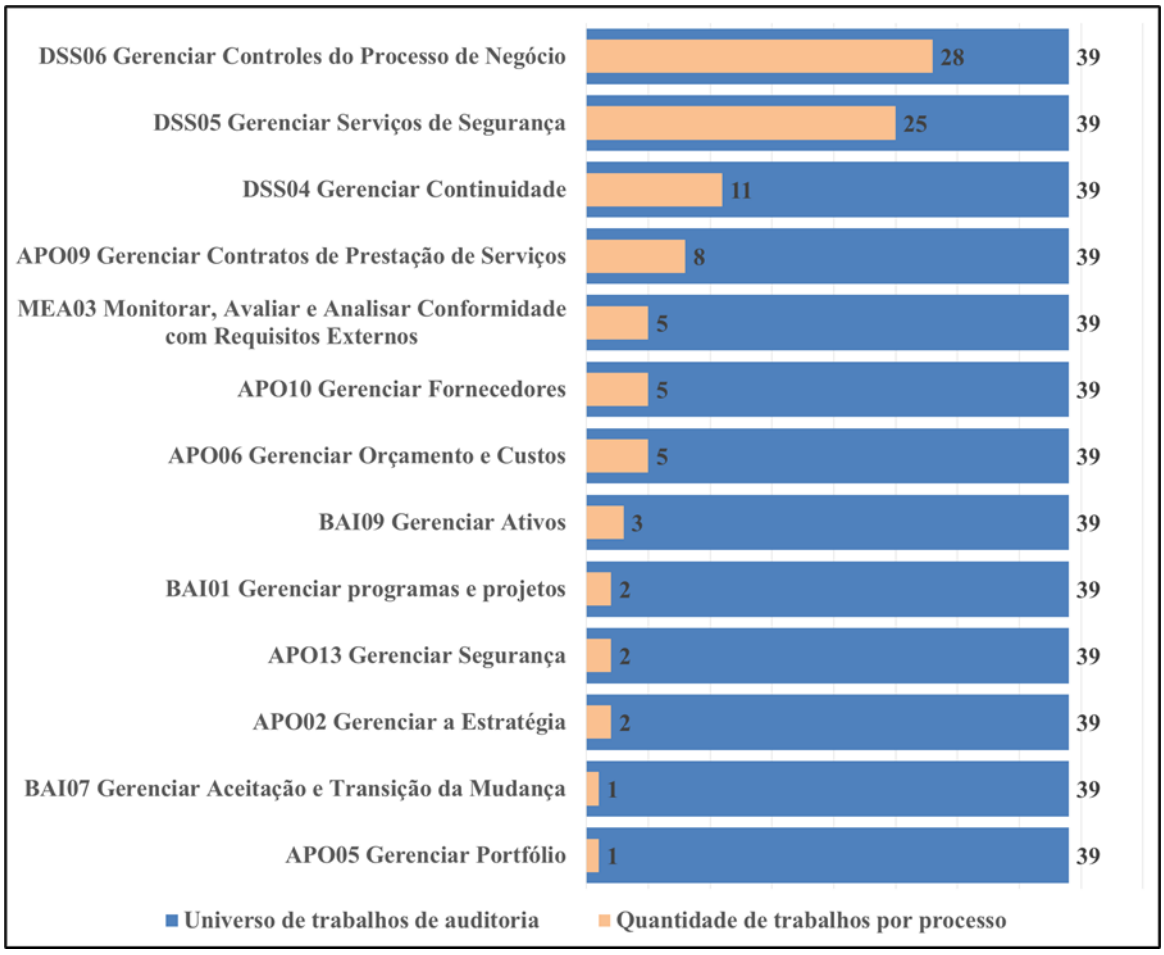

Figura 4.4: Trabalhos *versus* Processos COBIT 5
Fonte: Elaborado pelo autor

4.2 – Análise das deficiências identificadas pela auditoria interna de TI

Para analisar os 103 PTA apresentados nos relatórios dos trabalhos, primeiramente, foi realizada a categorização e o agrupamento das deficiências de acordo com a natureza e similaridade de cada um dos PTA. Neste sentido, foram identificadas 16 categorias que foram relacionadas aos processos do COBIT 5 impactados em cada um dos 39 trabalhos, conforme é possível verificar através da tabela 4.3.

Tabela 4.3: Categorias de PTA

#	Categoria PTA	Quantidade de PTA	%
1	Inexistência ou deficiência de gestão de acessos à sistemas e/ou elementos de infraestrutura (banco de dados ou sistema operacional)	24	23%
2	Inexistência ou deficiência de processos, políticas, planos ou procedimentos de TI	18	17%
3	Inexistência ou deficiência de controles sistêmicos para atendimento de regras de negócio	13	13%
4	Inexistência ou deficiência de parametrizações de segurança configuradas em sistemas ou elementos de infraestrutura (banco de dados e sistema operacional)	6	6%
5	Inexistência ou deficiência de controles de monitoramento de desempenho da TI	6	6%
6	Inexistência ou deficiência nos processos de atendimento ao usuário ou cliente	5	5%
7	Inexistência ou deficiência de gestão de ativos, recursos e capacidades de TI	5	5%
8	Inconformidade da TI com leis, regulações ou requerimentos contratuais (requisitos externos)	5	5%
9	Pagamento indevido ou incorreto de serviços prestados por fornecedores ou parceiros	4	4%
10	Informações divergentes, inconsistentes e/ou incompletas entre sistemas	4	4%
11	Inexistência ou deficiência na gestão de indicadores de monitoramento de desempenho da TI	4	4%
12	Faturamento indevido ou incorreto de serviços prestados por fornecedores ou parceiros	4	4%
13	Deficiência de segregação de funções nos ambientes de desenvolvimento e produção de sistemas	2	2%
14	Inexistência ou deficiência em mecanismos de redundância e contingência	1	1%
15	Dependência excessiva de fornecedores	1	1%
16	Deficiência na governança do plano estratégico da TI	1	1%

Fonte: Elaborado pelo autor

Ao analisar a tabela 4.3, percebe-se que a categoria com a maior quantidade de PTA associados (24 PTA - 23%) é a “Inexistência ou deficiência de gestão de acessos a sistemas e/ou elementos de infraestrutura (banco de dados ou sistema operacional)”, a qual está relacionada à existência de profissionais desligados com acesso incorretamente ativos nos sistemas e/ou elementos de infraestrutura, existência de contas de usuários com perfis privilegiados ou administrativos sob a responsabilidade de profissionais indevidos ou incorretos, e a erros no processo de cadastro de contas de usuários.

A categoria “Inexistência ou deficiência de processos, políticas, planos ou procedimentos de TI” está relacionada 17% do total de PTA (18), e é referente à inexistência ou insuficiência de documentação formal a respeito dos processos e controles da área de TI da empresa. A categoria “Inexistência ou deficiência de controles sistêmicos para atendimento de regras de negócio” está relacionada a 13% do total de PTA (13), e é referente a falhas de controles automáticos executados por sistemas devido a erros ou ausência de regras de negócio implementadas.

Por fim, foi verificado que as demais 13 categorias estão relacionadas cada uma a menos de 10% do total de PTA apresentados nos relatórios de auditoria.

Posteriormente, foram apresentadas na tabela 4.4 as categorias de PTA relacionadas às deficiências que impactam os princípios definidos na LGPD para tratamento de dados pessoais, que representam 31% do total de categorias de PTA levantados. Estas deficiências são referentes a problemas de processos, de gestão de acesso de usuários, de parametrizações de segurança em sistemas e de controles automatizados de aplicações, e podem contribuir para a exposição da empresa a riscos que comprometem o tratamento de dados dos seus clientes e profissionais. Adicionalmente, foram observados 53 PTA referentes às 5 categorias em questão, representando 51% do total de PTA apontados nos trabalhos de auditoria. É válido ressaltar que, ao analisar os objetivos e escopos das 39 auditorias realizadas, não foram identificados projetos específicos para avaliação da adequação da empresa à LGPD. Além disso, apenas 3 processos do COBIT 5 (“DSS05 Gerenciar Serviços de Segurança”, “DSS06 Gerenciar Controles do Processo de Negócio” e “BAI09 Gerenciar Ativos”) apresentavam análises de auditoria relacionadas aos princípios definidos na LGPD, sendo observadas deficiências em 100% dos processos em questão.

Tabela 4.4: PTA versus LGPD

#	Categoria PTA	Quantidade de PTA
1	Inexistência ou deficiência de gestão de acessos à sistemas e/ou elementos de infraestrutura (banco de dados ou sistema operacional)	24
2	Inexistência ou deficiência de controles sistêmicos para atendimento de regras de negócio	13
3	Inexistência ou deficiência de parametrizações de segurança configuradas em sistemas ou elementos de infraestrutura (banco de dados e sistema operacional)	6
4	Inexistência ou deficiência nos processos de atendimento ao usuário ou cliente	5
5	Inexistência ou deficiência de gestão de ativos, recursos e capacidades de TI	5

Fonte: Elaborado pelo autor

A tabela 4.5 apresenta a relação dos processos do COBIT 5 que foram impactados por deficiências ou oportunidades de melhoria juntamente com a quantidade de PTA segmentados pelos seus respectivos ratings de avaliação.

Tabela 4.5: Processos COBIT 5 versus Rating PTA

#	Processos COBIT 5	Quantidade de PTA	%
1	DSS06 Gerenciar Controles do Processo de Negócio	41	40%
2	DSS05 Gerenciar Serviços de Segurança	32	31%
3	APO09 Gerenciar Contratos de Prestação de Serviços	11	11%
4	APO02 Gerenciar a Estratégia	7	7%
5	MEA03 Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos	4	4%
6	BAI09 Gerenciar Ativos	4	4%
7	APO10 Gerenciar Fornecedores	2	2%
8	APO06 Gerenciar Orçamento e Custos	1	1%
9	DSS04 Gerenciar Continuidade	1	1%

Fonte: Elaborado pelo autor

Ao analisar a tabela 4.5, percebe-se que os processos “DSS06 Gerenciar Controles do Processo de Negócio” (41 PTA – 40%), “DSS05 Gerenciar Serviços de Segurança” (32 PTA – 31%) e “APO09 Gerenciar Contratos de Prestação de Serviços” (11 PTA – 11%) são os que apresentam a maior quantidade de PTA associados.

Adicionalmente, os demais processos que também foram impactados por deficiências (6 processos) apresentam cada um menos de 10% do total de PTA associados apresentados nos relatórios de auditoria. É válido ressaltar que do total de 13 processos do COBIT que foram objeto de análise através dos trabalhos de auditoria executados em 2019 e 2020, 9 (69%) apresentaram deficiências e, por isso, tiveram ao menos um PTA apontado.

Por fim, ao analisar a tabela 4.6 consolidando os *ratings* de classificação de riscos, foi verificado que 93% dos PTA (96) foram classificados como "Moderado" (71 PTA – 69%) ou "Baixo" (25 PTA – 24%). Neste sentido, de acordo com os critérios definidos pela área de auditoria interna da empresa, é possível afirmar que a maioria das deficiências possuem a probabilidade de ocorrer mais uma vez dentro do intervalo de um ano, e podem acarretar consequências reversíveis em curto e médio prazo com custos baixos.

Tabela 4.6: Ratings dos PTA

Rating do PTA	Quantidade de PTA	%
Moderado	71	69%
Baixo	25	24%
Significativo	6	6%
Alto	1	1%

Fonte: Elaborado pelo autor

4.3 – Análise sobre os benefícios obtidos com a auditoria interna de TI

Para analisar os benefícios obtidos a partir do apontamento dos PTA apresentados nos relatórios de auditoria, primeiramente, foi realizada a análise do conteúdo dos pontos a fim de identificar os possíveis ganhos a serem alcançados a partir do descritivo dos resultados das auditorias realizadas. Após o levantamento, foram definidas 5 classificações de benefícios de acordo com as suas naturezas e similaridades. Por fim, foi realizado o agrupamento das 16 categorias de PTA de acordo com os seus respectivos benefícios associados, conforme é possível verificar detalhadamente através da tabela 4.7 e resumidamente através do gráfico na figura 4.5.

Tabela 4.7: Benefícios das auditorias

Classificação Benefício	Quantidade de PTA	%
Adequação ou melhoria de eficiência na gestão ou governança de processos e recursos de TI	53	51%
Adequação ou melhoria de eficiência em controles de segurança dos recursos de TI	32	31%
Redução de custos com pagamentos ou faturamentos incorretos ou indevidos	8	8%
Alinhamento das práticas de TI às exigências contratuais ou externas	5	5%
Melhoria nos processos de atendimento aos clientes internos ou externos da empresa	5	5%

Fonte: Elaborado pelo autor

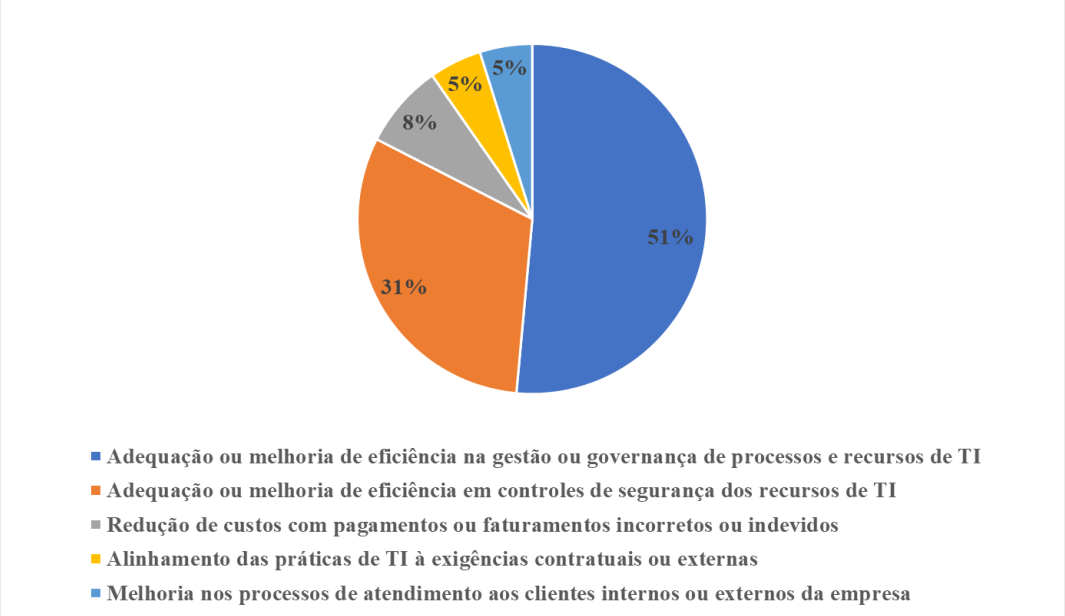

Figura 4.5: Benefícios das auditorias
Fonte: Elaborado pelo autor

Conforme é possível verificar, o benefício “Adequação ou melhoria de eficiência na gestão ou governança de processos e recursos de TI” foi o que apresentou maior frequência de ganho em relação ao total de pontos levantados nas auditorias de TI (51%). Este benefício está relacionado, principalmente, à melhoria de processos e de configurações em recursos de TI.

O benefício “Adequação ou melhoria de eficiência em controles de segurança dos recursos de TI” foi o que apresentou em seguida a maior frequência de ganho em relação ao

total de pontos levantados nas auditorias de TI (31%). Este benefício está relacionado à identificação e ajuste de vulnerabilidades de segurança nos recursos de TI (sistemas, banco de dados e sistemas operacionais).

Por fim, é possível verificar que os benefícios “Redução de custos com pagamentos ou faturamentos incorretos ou indevidos”, “Alinhamento das práticas de TI à exigências contratuais ou externas” e “Melhoria nos processos de atendimento aos clientes internos ou externos da empresa” estão cada um relacionados com menos de 10% do total de pontos levantados nas auditorias de TI. É válido ressaltar que, por motivo de confidencialidade de informações, não foi possível apresentar o detalhamento em relação aos valores financeiros envolvidos com a eliminação de desperdícios ou economia de custos para a empresa.

Capítulo 5

Conclusão e Trabalhos Futuros

5.1 – Conclusão

Verificou-se que a auditoria de TI atua de forma abrangente contemplando diferentes abordagens de atuação e analisando diferentes processos do COBIT 5. Neste sentido, foi possível confirmar que o objetivo e escopo de apenas uma auditoria pode contemplar distintas abordagens de atuação e analisar diferentes processos, sendo este cenário identificado na maior parte do universo de trabalhos executados (87%). Adicionalmente, foi verificado que no período de 2 anos foram realizados trabalhos que cobriram 37% do universo total de processos de governança e gestão disponibilizados no COBIT 5, sendo os processos "DSS06 Gerenciar Controles do Processo de Negócio" e "DSS05 Gerenciar Serviços de Segurança" tendo maior destaque, já que eles foram os únicos processos analisados em mais da metade do total de trabalhos realizados.

Adicionalmente, no que tange os pontos de auditoria identificados nos trabalhos executados, 53% são referentes a apenas 3 deficiências ("Inexistência ou deficiência de gestão de acessos a sistemas e/ou elementos de infraestrutura", "Inexistência ou deficiência de processos, políticas, planos ou procedimentos de TI" e "Inexistência ou deficiência de controles sistêmicos para atendimento de regras de negócio") do total das 16 categorias mapeadas, sendo a maioria das deficiências apontadas classificadas com risco "Moderado" ou "Baixo" (93%). Em relação à associação dos pontos de auditoria aos processos do COBIT 5, foi verificado que 77% dos processos analisados geraram apontamentos da auditoria. Por fim, embora não tenham sido identificados projetos específicos para avaliação da adequação da empresa à LGPD, a auditoria interna de TI já atua contribuindo no levantamento de deficiências que impactam na LGPD, mostrando que a área se preocupa com a avaliação de riscos relacionados à proteção de dados críticos para a empresa e seus clientes.

Por fim, em relação aos benefícios alcançados através das auditorias, foi verificado que os principais ganhos a serem conquistados pela empresa são relacionados a "Adequação ou melhoria de eficiência na gestão ou governança de processos e recursos de TI" e "Adequação

ou melhoria de eficiência em controles de segurança dos recursos de TI", que são referentes a 83% do total dos pontos de auditoria gerados nos trabalhos.

5.2 – Trabalhos Futuros

Como trabalhos futuros, sugere-se verificar se os planos de ação, os quais são definidos para tratamento dos PTA, foram implementados e alcançaram efetivamente como resultado os benefícios identificados para as deficiências levantadas nas auditorias. Adicionalmente, sugere-se que o resultado deste trabalho possa ser utilizado como fonte de informação para auxiliar a área de Auditoria de TI da empresa de Telecom analisada na elaboração do plano anual de trabalhos de auditoria, já que esta pesquisa apresenta informações que podem contribuir para a área definir a sua estratégia de atuação nos próximos anos.

Por fim, sugere-se que esta pesquisa também possa ser utilizada como base pela empresa, bem como por outras empresas privadas ou públicas, para criação de uma metodologia a ser implementada e executada periodicamente a fim de avaliar o escopo de atuação da área de auditoria de TI e auxiliar no direcionamento estratégico da área.

Referências Bibliográficas

1. DELOITTE, *Riscos cibernéticos e segurança da informação na América Latina e Caribe*, https://www2.deloitte.com/content/dam/Deloitte/br/Documents/risk/Cyber-survey-2019-portugu%C3%AAs.pdf, 2019, (Acesso em: 08 de agosto de 2020).

2. DELOITTE, *Os Cinco Pilares de Riscos - Visão abrangente e integrada sobre os principais riscos empresariais*, https://www2.deloitte.com/br/pt/pages/risk/articles/os-cinco-pilares-dos-riscos-empresariais.html, 2019, (Acesso em: 10 de agosto de 2020).

3. DELOITTE e INSTITUTO DE AUDITORES INTERNOS, *Auditoria Interna no Brasil Rumo à consolidação do impacto e da influência*, http://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/auditoriaintern-editorHTML-00000001-12122018135129.pdf, 2018, (Acesso em: 05 de julho. de 2020).

4. PRODANOV, C. C.; FREITAS, E. C. de. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico*. 2. ed. Novo Hamburgo, Feevale, 2013.

5. GIL, A. C. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo, Atlas, 2008.

6. BOGDAN, R; BIKLEN, S. *Investigação qualitativa em educação: uma introdução à teoria e aos métodos*. Lisboa, Porto Editora, 1994.

7. GHERMAN, M. *Controles internos: buscando a solução adequada*, http://www.modulo.com.br/checkuptool/artigo_04.htm, 2005, (Acesso em: 10 de agosto 2020).

8. INSTITUTO DE AUDITORES INTERNOS, *Instituto de Auditores Internos: Missão da Auditoria Interna*, https://iiabrasil.org.br/ippf/missao-da-auditoria-interna, 2020, (Acesso em: 05 de agosto de 2020).

9. CARNEIRO, Sílvia Eunice da Silva Martins. *Quais os atributos que um auditor interno deve ter*, http://recipp.ipp.pt/bitstream/10400.22/1840/1/DM_SilviaCarneiro_2013.pdf, 2013, (Acesso em: 05 de setembro de 2020).

10. CREPALDI, Silvio Aparecido. *Curso básico de contabilidade: resumo da teoria, atendendo as novas demandas da gestão empresarial, exercícios e questões com respostas*. São Paulo, Atlas, 2002.

11. INSTITUTO DE AUDITORES INTERNOS, *Modelo das Três Linhas do IIA*, https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf, 2020, (Acesso em: 25 de agosto de 2020).

12. DIAS, Sergio Vidal dos Santos, *Auditoria de processos organizacionais: teoria, finalidade, metodologia de trabalho e resultados esperados*. São Paulo, Atlas, 2006.

13. BRAZ, Msc. Marcio Rodrigo, *Auditoria de Ti: O Guia de Sobrevivência em Auditoria*. São Paulo, ASE Editorial, 2017.

14. DIAS, Claudia, *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro, Axcel Books, 2000.

15. CHAVES, Renato Santos, *Auditoria e controladoria no setor público: fortalecimento dos controles internos – com jurisprudência do TCU*. 2. Curitiba, Juruá, 2011.

16. ISACA, *COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização*. 2012.

17. BRASIL, *Lei N° 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais*, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm, Brasília, (Acesso em: 13 fevereiro de 2020).

18. VERGARA, Sylvia C. *Projetos e relatórios de pesquisa em administração*. São Paulo, Atlas, 1997.

Apêndice 1

Total de PTA x Trabalhos de auditoria de TI

Total de PTA formalizados em cada um dos 39 trabalhos de auditoria de TI executados em 2019 e 2020:

Ano	Códigos dos trabalhos	Total de PTA
2019	AUD_TI901	1
	AUD_TI902	2
	AUD_TI903	3
	AUD_TI904	3
	AUD_TI905	4
	AUD_TI906	5
	AUD_TI907	2
	AUD_TI908	2
	AUD_TI909	3
	AUD_TI910	4
	AUD_TI911	1
	AUD_TI912	3
	AUD_TI913	3
	AUD_TI914	2
	AUD_TI915	2
	AUD_TI916	4
	AUD_TI917	6
	AUD_TI918	2
	AUD_TI919	2
	AUD_TI920	1
2020	AUD_TI2001	3
	AUD_TI2002	3
	AUD_TI2003	1
	AUD_TI2004	2
	AUD_TI2005	1
	AUD_TI2006	6
	AUD_TI2007	3
	AUD_TI2008	2
	AUD_TI2009	1
	AUD_TI2010	4
	AUD_TI2011	2
	AUD_TI2012	1
	AUD_TI2013	2
	AUD_TI2014	4
	AUD_TI2015	7
	AUD_TI2016	2
	AUD_TI2017	4
	AUD_TI2018	1
	AUD_TI2019	3
Total Geral		103