A ÁREA DE GOVERNANÇA DE T.I: SUAS DIRETRIZES E PROCESSOS.

THE AREA OF IT GOVERNANCE: ITS GUIDELINES AND PROCESSES.

Flávio Augusto Lourenço, FATEC Araraquara,
flavio.lourenco@hotmail.com

Lucas Adriano Barnabé, FATEC Araraquara,
lucasabarnabe@hotmail.com

Wdson de Oliveira, FATEC Araraquara,
wdson.oliveira@unar.edu.br

Resumo

Esse artigo consiste em apresentar a governança de TI e suas normas, relacionadas ao conjunto de boas práticas dentro da segurança da informação da série ISO, com o objetivo de estabelecer diretrizes e princípios para dar início, implementar, melhorar e manter a gestão da segurança da informação. É uma norma internacional para a governança corporativa de tecnologia da informação onde seus princípios servem para orientar os dirigentes de uma empresa sobre uso eficaz, eficiente e aceitável dentro de uma organização. Abordaremos políticas, metodologias, conjuntos de boas práticas e frameworks utilizados nas empresas, para o alinhamento das diretrizes de TI aos negócios e entrega de valor das organizações. Apresentaremos informações que possam proporcionar a implantação de uma governança de TI eficaz, alinhada com os setores e com o plano estratégico da empresa. Para tal, realizou-se uma pesquisa quantitativa descritiva, o estudo permitiu identificar o perfil das empresas acerca dos principais conceitos abordados pela Governança de TI, frameworks utilizados, conhecimento e implantação sobre a segurança da informação.

Palavras-Chave: Tecnologia da Informação, Governança da Tecnologia da Informação, Gestão de Tecnologia da Informação, segurança da informação.

Abstract

This article consists of presenting IT governance and its standards, related to the set of good practices within the information security of the ISO series, with the objective of establishing guidelines and principles to initiate, implement, improve and maintain the security management of the information. It is an international standard for the corporate governance of information technology where its principles serve to guide a company's

directors on effective, efficient and acceptable use within an organization. We will address policies, methodologies, sets of best practices and frameworks used in companies, for the alignment of IT guidelines to the business and delivery of value to organizations. We will present information that can provide the implementation of an effective IT governance, aligned with the sectors and with the strategic plan of the company. To this end, a descriptive quantitative research was carried out, the study allowed to identify the profile of companies about the main concepts addressed by IT Governance, frameworks used, knowledge and implementation of information security.

Keywords*: Information Technology, Information Technology Governance, Information Technology Management, information security.*

1. Introdução

A segurança da informação é essencial para o desenvolvimento e para proteção dos ativos da organização estando diretamente relacionada com a governança, sendo definida como um subconjunto da governança empresarial que oferece direcionamento estratégico, assegura que os objetivos sejam atingidos, gerencia riscos e monitora o êxito ou a falha do programa de segurança corporativa (FERNANDES, P 15, 2014).

A Governança de Tecnologia da Informação (TI) refere-se, na prática, à associação estruturada de um conjunto de diretrizes, responsabilidades, competências e habilidades, compartilhadas e assumidas dentro das empresas por executivos, gestores, técnicos e usuários de TI, objetivando controlar efetivamente os processos, garantir a segurança das informações, otimizar a aplicação de recursos e dar suporte para a tomada de decisões, tudo isso, de forma alinhada com a missão, visão e metas estratégicas das organizações (IT Governance Institute, 2007b).

O trabalho abordará normas ISO/IEC 38500, políticas e conjunto de boas práticas apontadas pela ISO/IEC 27002 e utilizadas nas empresas para o alinhamento de processos com a estratégia de negócio, gerenciamento de riscos, otimizar recursos e dar suporte à tomada de decisões.

Para desenvolver uma governança de TI eficaz, uma empresa se utiliza de frameworks como o COBIT (Control Objectives for Information and related Technology) e ITIL (Information Technology Infrastructure Library) que são uma série de ações e estratégias que visam dar suporte e orientações para mitigar e até mesmo solucionar um problema.

O artigo consiste em apresentar conceitos utilizados em governança de TI para que as empresas façam a implantação de uma boa governança com base nos conjuntos de boas práticas para realizar processos e entregar resultados com mais agilidade e rapidez garantindo assim a confidencialidade, integridade, disponibilidade e autenticidade das informações.

A governança de TI deve estar alinhada com o plano de negócio da empresa, com os outros setores e os investimentos da implantação não devem afetar os negócios da empresa (FERNANDES, P 15, 2014).

Para isso devemos responder a seguinte pergunta: Como alinhar a governança de TI com o plano de negócios da empresa, bem como o alinhamento com todos os setores e quais frameworks utilizar para o desenvolvimento da mesma?

As respostas a esses questionamentos irão culminar com o desenvolvimento e elaboração de uma Governança de T.I que esteja alinhada com a regra de negócio da empresa.

O objetivo do artigo é apresentar informações que possam auxiliar as empresas a fazerem a implantação de uma governança de TI eficaz alinhando o plano estratégico, entrega de valor, gestão de risco, gestão de recursos e mensuração de desempenho com a necessidade de negócio proporcionando diversas melhorias em todos os setores da organização.

Seguiremos as normas ISO/IEC 38500, framework COBIT e o conjunto de boas práticas ISO/IEC 27002 para elaborar uma governança de TI que possa contribuir com as empresas a identificarem suas necessidades de negócio e desenvolver sua própria governança de TI.

2. Referencial teórico

Neste capítulo, são descritos os conceitos pesquisados para o desenvolvimento do artigo em questão.

2.1 Governança

A governança de TI pode ser entendida como um conjunto de políticas, normas, procedimentos e atividades que têm o objetivo de estruturar o setor tecnológico da empresa.

Com a governança de TI é possível administrar adequadamente os recursos humanos e técnicos, ferramentas e serviços, melhorando o fluxo e a produtividade do setor.

Por meio das boas práticas que envolvem a governança de TI, o objetivo é que a empresa alcance melhorias como: maior segurança de informações, economia de recursos e atualização de processos.

O primeiro passo é sempre o alinhamento de estratégias e metas com a equipe responsável pelo TI. Assim, os resultados podem ser alcançados de forma assertiva, com melhor gerenciamento do tempo.

Existem três tipos de governanças dentro de uma empresa:

a) Governança de Corporativa: Governança corporativa ou governo das sociedades ou das empresas é o conjunto de processos, costumes, políticas, leis, regulamentos e instituições que regulam a maneira como uma empresa é dirigida, administrada ou controlada.

b) Governança Corporativa de TI: **“**Tem como objetivo o futuro da área de TI dentro de uma organização. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar planos. Inclui a estratégia e as políticas de uso da TI dentro da organização” (NBR ISO/IEC 38500:2009).

c) Governança de TI: “É a especificação de regras e responsabilidades para estimular que a TI da empresa sustente e estenda as estratégias e os objetivos da organização” (Weill, Ross, P8, 2006)

2.2 ISO/IEC 38500

É uma norma internacional para a governança corporativa de tecnologia da informação onde seus princípios servem para orientar os dirigentes de uma empresa sobre uso eficaz, eficiente e aceitável dentro de uma organização.

A ISO/IEC 38500 (2009) está fundamentada em seis princípios aplicáveis para qualquer porte de organização, oferecendo as diretrizes básicas para a implementação e manutenção para uma governança de TI eficaz.

a) Responsabilidade: Para garantir a conduta ética da governança de TI, todos precisam compreender suas responsabilidades no fornecimento dos serviços de TI, trazendo resultados melhores para o mercado e seus parceiros.
b) Estratégia: A estratégia da organização precisa considerar a atual capacidade de TI e planejar a futura, respeitando como será desenvolvida a abordagem da organização para a execução da governança de TI.

c) Aquisições: As aquisições de TI são desenvolvidas com base em análise progressiva, transparente e em conjunto. Deve haver equilíbrio entre oportunidade e risco, a curto e longo prazo.

d) Desempenho: O desempenho deve ser medido em conjunto com a disponibilidade de serviços, suporte e objetivos da empresa. Assim, os resultados obtidos serão monitorados a fim de viabilizar a tomada de decisão e correções para o processo de governança.

e) Conformidade: A TI deve estar em conformidade com a legislação e regulamentos aplicáveis, buscando uma postura transparente e adequada para com o mercado, a sociedade e a sustentabilidade.

f) Comportamento Humano: As políticas, práticas e decisões na TI trazem o respeito pelo comportamento humano, incluindo todas as pessoas no processo. Os recursos humanos jamais podem ser negligenciados na governança de TI. Aqui, a importância das pessoas é o foco para o sucesso na implementação da governança de TI.

2.3 ISO/IEC 27002

Relacionada com um conjunto de boas práticas dentro da segurança da informação da série ISO 27000, com o objetivo de estabelecer diretrizes e princípios para dar início, implementar, melhorar e manter a gestão da segurança da informação (Editora ABNT, 2013a, p.1).

A distribuição da Norma ISO 27000 segue os itens abaixo relacionados:

2.3.1 Política de Segurança da Informação

Deve ser elaborado um documento sobre política de segurança da informação para a empresa, o qual deve conter conceitos de segurança e uma estrutura para estabelecer objetivos e o engajamento da direção com a política, entre outros fatores.

2.3.2 Organização da Segurança da Informação

Para implementação da Segurança da Informação em uma organização, se faz necessário estabelecer o gerenciamento de maneira adequada. Para isso, as atividades de segurança da informação devem ser orientadas e coordenadas por representantes da empresa, que devem ter responsabilidades definidas para proteger as informações sensíveis.

2.3.3 Gestão de ativos

Segundo as normas e diretrizes da Segurança da Informação, ativos são quaisquer coisas que tenham valor para a organização e que necessita ser protegido. Os ativos devem ser classificados e identificados, para que possa ser elaborado um inventário e posteriormente mantido. As regras devem ser documentadas e definidas para a permissão e uso dos ativos.

2.3.4 Segurança em recursos humanos

Para realizar a admissão de novos colaboradores ou fornecedores é importante que ele seja devidamente analisado, principalmente se for lidar com informações sigilosas. A intenção desta seção é atenuar o risco de fraude, roubo ou mau uso dos recursos. Os colaboradores devem estar cientes das ameaças relativas à segurança da informação, suas obrigações e responsabilidades.

2.3.5 Segurança física e do ambiente

As instalações e equipamentos de processamento de informação sensíveis, devem estar em locais seguros, com controle de níveis de acesso e proteção para prevenir ameaças físicas e ambientais.

2.3.6 Segurança das operações e comunicações

É importante definir as responsabilidades e procedimentos pela operação e gestão de todos os equipamentos que processão as informações. Incluindo o planejamento para minimizar o risco de falhas, gerenciar serviços terceirizados, criar procedimentos para realização de backups de segurança e sua recuperação e gerir a segurança de redes e comunicações internas.

2.3.7 Controle de acesso

O acesso à informação, deve ser controlado com base nos requisitos de negócio e na segurança da informação. Deve ser garantido o acesso apenas ao usuário autorizado e retido os acessos não autorizados ao sistema de informação, prevenindo assim danos a documentos e recursos da organização.

2.3.8 Aquisição, desenvolvimento e manutenção de sistemas

As requisições devem ser identificadas e acordadas antes da sua implementação, com o objetivo de proteger, visando a manutenção de sua confidencialidade, autenticidade e integridade por meios criptográficos.

2.3.9 Gestão de incidentes de segurança da informação

Os procedimentos de registro e escalonamento devem ser elaborados a fim de

identificar, analisar e corrigir o problema. Os colaboradores, fornecedores e terceiros devem ter ciência sobre os processos da gestão de incidentes para identificar os eventos de segurança da informação e assegurar que eles sejam corrigidos em tempo hábil.

2.3.10 Gestão da continuidade do negócio

Projetos para continuidade do negócio devem ser desenvolvidos e implementados, os quais devem impedir a paralização das atividades e assegurar que as operações essenciais sejam rapidamente reestabelecidas.

2.3.11 Conformidade

É necessário garantir estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, a fim de evitar a violação de qualquer lei civil ou criminal. A empresa pode contratar uma consultoria especializada, para verificar sua conformidade e aderência a requisitos regulamentares e legais.

2.4 COBIT

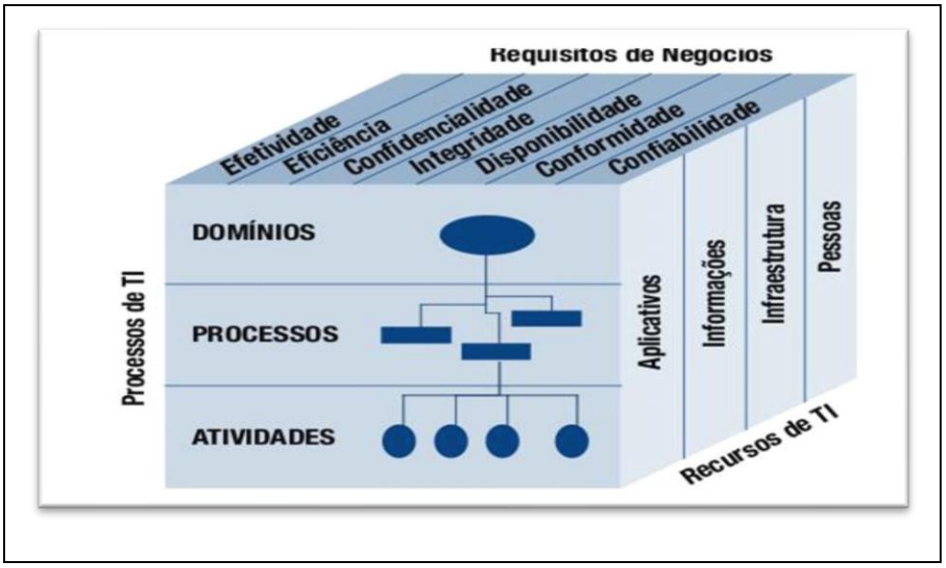
O Controle de Objetivos para a Informação e Tecnologia Relacionadas (COBIT), conforme Figura 1, é um modelo de estrutura para o entendimento e o gerenciamento de riscos em Tecnologia da informação, e para a alinhar a TI com a regra de negócio da empresa sendo o foco mais no gerenciamento do que na parte de execução. (ISACA, 2012).

São as diretrizes para gerenciar e controlar todos os elementos que compõe a governança de TI e são divididos em 3 categorias.

2.4.1 Critérios da Informação

a) Efetividade: informação pertinente para a gestão do negócio, bem como entregue no prazo determinado, consistente e utilizável.
b) Eficiência: entrega da informação de forma mais produtiva e econômica.
c) Confidencialidade: proteção das informações sigilosas a fim de se evitar seu vazamento indevido.
d) Integridade: autenticidade e totalidade da informação, para a validação do negócio.
e) Disponibilidade: a informação deve ser acessível e utilizável quando exigida pelo negócio. Possuindo relação dos recursos necessários e sua capacidade.
f) Conformidade: com as leis, obrigações contratuais e regulamentos relacionados ao negócio.
g) Confiabilidade: garantir a entrega da informação para tomada de decisão

Figura 1. Cubo do COBIT.



Fonte: ITGI, 2007.

2.4.2 Recursos de TI

a) Aplicações: sistemas de informação usados na organização.
b) Infraestrutura: tecnologia utilizada, como os equipamentos, sistemas operacionais, redes de comunicação de dados que processam as aplicações.
c) Informações**:** são os dados em todas as suas formas utilizados nos sistemas de informação e usados pelos processos de negócios.
d) Pessoas**:** as pessoas requeridas para planejar, organizar, adquirir, entregar, dar suporte e monitorar os aplicativos, processos e serviços de TI.

2.4.3 Processos de TI

Os processos do COBIT são organizados por 4 domínios, 34 processos, 318 atividades e objetivos de controle.

Segue o exemplo de alguns processos e controles na **Tabela 1**, demonstrando os 4 domínios e objetivos detalhados.

Tabela 1 - Exemplo de processos de TI.

	Processos de TI
EDM (Avaliar, Dirigir e Monitorar	EDM01 - Assegurar o estabelecimento e a manutenção do framework de Governança EDM02 - Assegurar a entrega dos benefícios EDM03 - Assegurar a otimização dos riscos EDM04 - Assegurar a otimização dos recursos EDM05 - Assegurar a transparência para as partes interessadas
APO (Alinhar, Planejar e Organizar)	APO01 - Gerenciar o framework de gestão de TI APO02 - Gerenciar a estratégia APO03 - Gerenciar a arquitetura corporativa APO04 - Gerenciar a inovação APO05 - Gerenciar o portfólio APO06 - Gerenciar orçamento e custos APO07 - Gerenciar recursos humanos APO08 - Gerenciar relacionamentos APO09 - Gerenciar acordos de serviço APO10 - Gerenciar fornecedores APO11 - Gerenciar a qualidade APO12 - Gerenciar riscos APO13 - Gerenciar a segurança
BAI (Construir, Adquirir e Implementar)	BAI01 - Gerenciar programas e projetos BAI02 - Gerenciar a definição de requisitos BAI03 - Gerenciar a identificação e a construção de soluções BAI04 - Gerenciar disponibilidade e capacidade BAI05 - Gerenciar a habilitação da mudança organizacional BAI06 - Gerenciar mudanças BAI07 - Gerenciar o aceite e a transição das mudanças BAI08 - Gerenciar o conhecimento BAI09 - Gerenciar ativos BAI10 - Gerenciar a configuração
DSS (Entregar, Serviços e Suporte)	DSS01 - Gerenciar operações DSS02 - Gerenciar requisições de serviços e incidentes DSS03 - Gerenciar problemas DSS04 - Gerenciar a continuidade DSS05 - Gerenciar os serviços de segurança DSS06 - Gerenciar controles de processos de negócios
MEA (Monitorar, Avaliar e Analisar)	MEA01 - Monitorar, avaliar e medir o desempenho e a conformidade MEA02 - Monitorar, avaliar e medir o sistema de controles internos MEA03 - Monitorar, avaliar e medir a conformidade com requisitos externos

Fonte: Adaptado de ISACA (2012b)

2.4.4 Requisitos de Negócios

Os objetivos de controle definem as metas da TI, que devem estar alinhadas às metas do negócio. O COBIT, conforme **Figura 2,** foca em cinco pontos, alinhamento estratégico, entrega de valor, gestão de recursos, gestão de riscos e medir o desempenho.

Figura: 2 – Focos da Governança de TI

Fonte: portal.tcu.gov.br

3 Metodologia

A metodologia utilizada no desenvolvimento do artigo foi uma pesquisa bibliográfica que deu o embasamento teórico para a contextualização dos conceitos utilizados. A pesquisa foi formulada com base nas diretrizes da ISO/IEC 38500 e da ISO/IEC 27002. Além da pesquisa bibliográfica, também, foi realizada uma pesquisa quantitativa com a elaboração de um instrumento de pesquisa baseado em perguntas objetivas. Posteriormente foi coletado e analisado o conteúdo das respostas para gerar uma comparação entre a teoria e a prática, respondendo a problemática do artigo.

Os dados foram obtidos a partir da medição do nível de maturidade dos serviços atuais de TI. Os dados quantitativos foram obtidos a partir da pesquisa entregue para o setor de governança das organizações, questionando quais seriam os processos de governança de TI ideais para a empresa estudada tendo como base os conceitos e normas da Governança de TI.

4 Resultados e Discussões

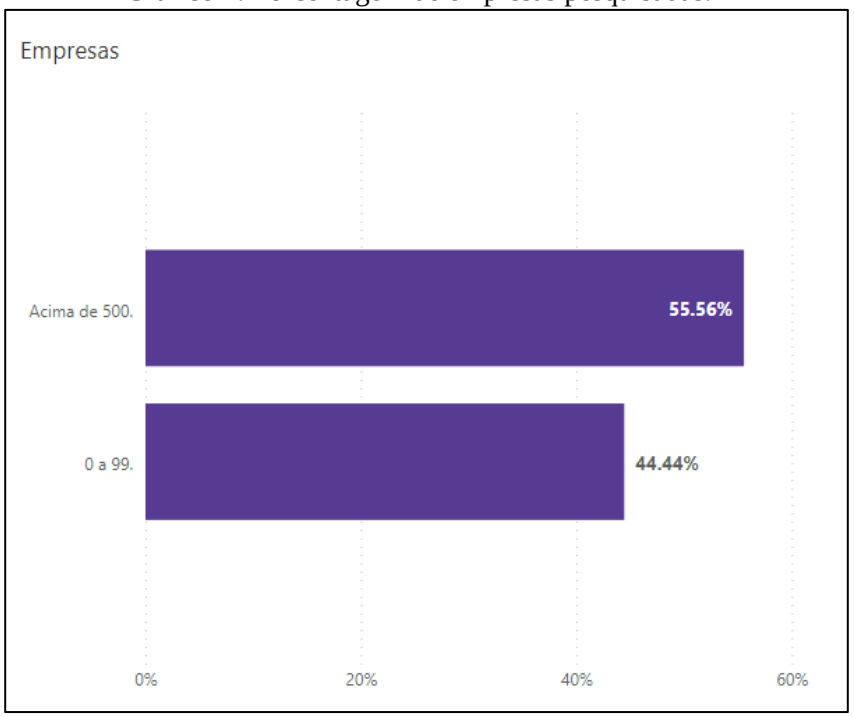
A pesquisa foi realizada com empresas onde foi obtido os resultados para o alinhamento da Governança de TI.
Os dados coletados foram tratados e analisados quantitativamente pela ferramenta Power BI da Microsoft.

4.1 Porte das empresas pesquisadas.

Os dados quantitativos foram obtidos a partir da pesquisa entregue para o setor de governança das organizações. De acordo com o Gráfico 1 56 % das empresas que

responderam ao questionário tem o porte acima de 500 funcionários e 44 % entre 0 a 99.

Gráfico 1: Porcentagem de empresas pesquisadas.



Fonte: Autoria própria (2022).

4.2 Alinhamento de Governança de TI

Os dados quantitativos foram obtidos a partir da pesquisa entregue para o setor de governança das organizações. Para responder esse tópico foram elaboradas cinco perguntas baseadas na ISO\IEC 38500 e no capítulo 5 do livro Governança de TI.

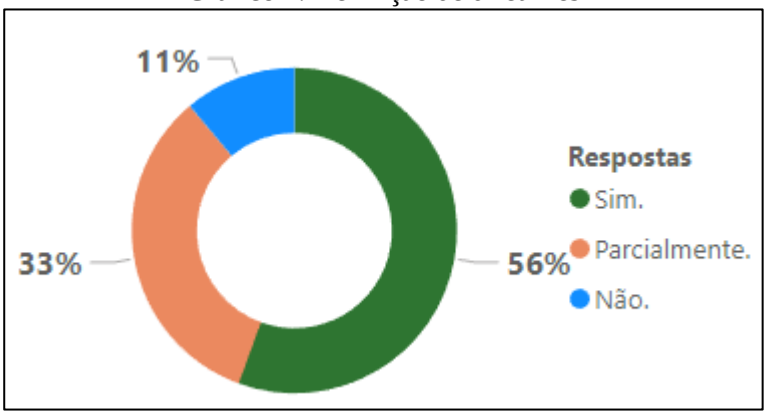
a) A empresa define formalmente as diretrizes de governança para o planejamento de TI?

No geral as respostas foram de 56 % para sim, 33 % para parcialmente e 11 % para não.

Empresas pesquisadas com o porte de 500 funcionários ou mais: 60% sim e 40 % Parcialmente.

Empresas de 0 a 99 funcionários: 50 % para sim, 25 % para parcialmente e não.

Gráfico 2: Definição de diretrizes



Fonte: Autoria própria (2022).

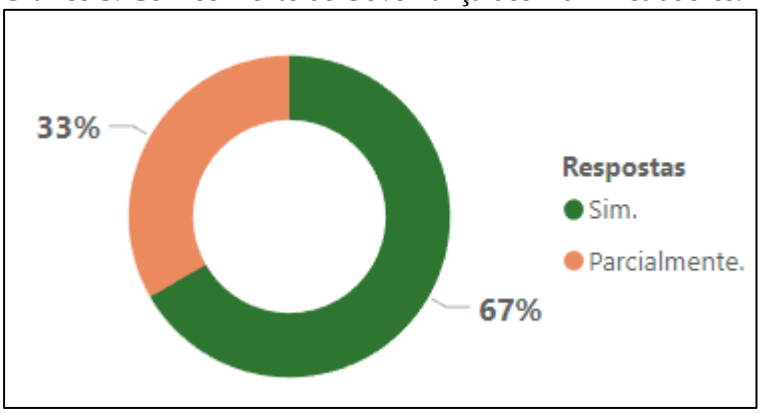
b) Os administradores em posições de liderança são capazes de descrever a Governança de TI?

Foram no geral 67 % para Sim e 33% para parcialmente.

Empresas pesquisadas com o porte de 500 funcionários ou mais: 60% Sim e 40 % Parcialmente.

Empresas de 0 a 99 funcionários: 75 % para sim, 25 % para parcialmente.

Gráfico 3: Conhecimento de Governança dos Administradores.



Fonte: Autoria própria (2022).

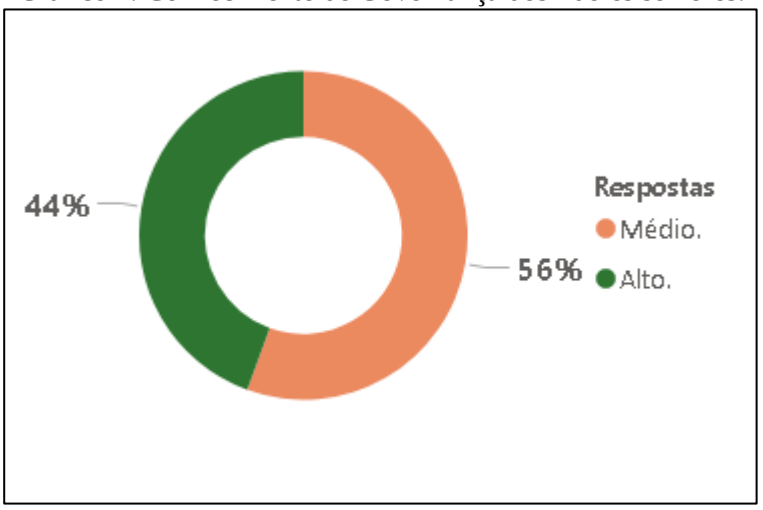
c) Como é o envolvimento dos líderes Seniores em relação a Governança de TI?

No geral as respostas foram de 44 % para o nível envolvimento alto e de % 56 para o nível de envolvimento médio.

Empresas com o porte de 500 funcionários ou mais: 40% para nível de envolvimento alto e 60 % para nível de envolvimento médio.

Empresas com o porte de 0 a 99 funcionários: 50 % para nível de conhecimento alto e médio.

Gráfico 4: Conhecimento de Governança dos líderes seniores.



Fonte: Autoria própria (2022).

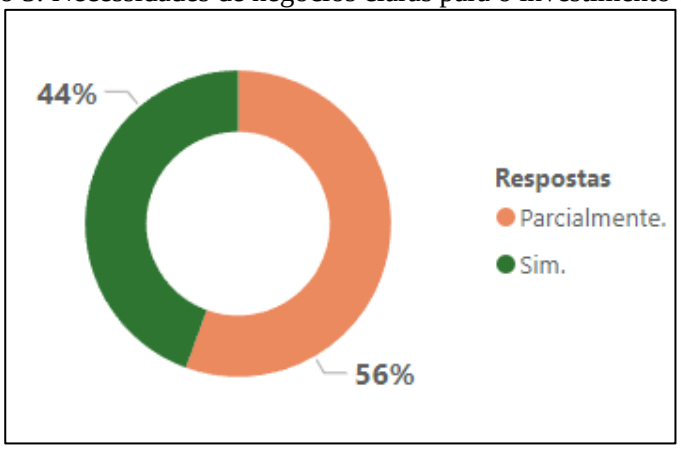
d) As necessidades de negócios são claras e objetivas para que haja o investimento em TI?

Foram no geral 44 % para Sim e 56% para parcialmente.

Empresas com o porte de 500 ou mais funcionários: 40 % Sim e 60% Parcialmente.

Empresas de 0 a 99 funcionários: 50 % para sim e para parcialmente.

Gráfico 5: Necessidades de negócios claras para o investimento em TI.



Fonte: Autoria própria (2022).

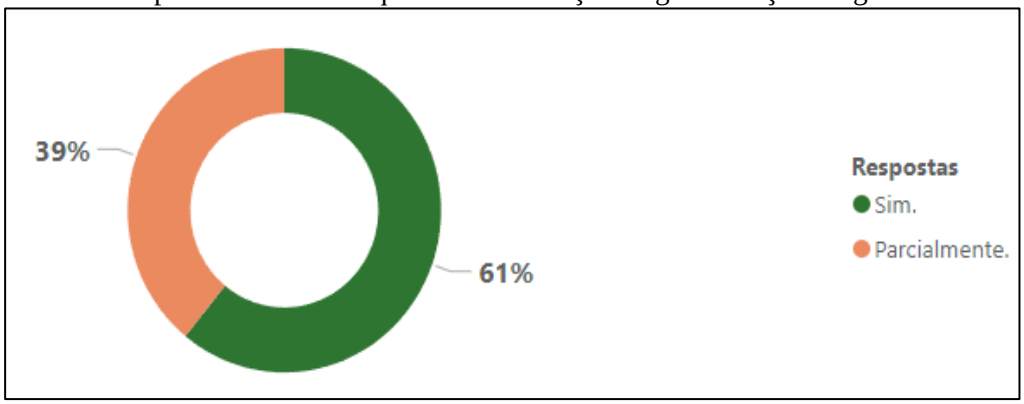
e) A organização aprova, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI?

Foram no geral 61 % para Sim e 39% para parcialmente.

Empresas com o porte de 500 ou mais funcionários: 47 % Sim e 53% Parcialmente.

Empresas de 0 a 99 funcionários: 88 % para sim e 12 % para parcialmente.

Gráfico 6: plano de auditoria que inclua avaliação da governança e da gestão de TI



Fonte: Autoria própria (2022).

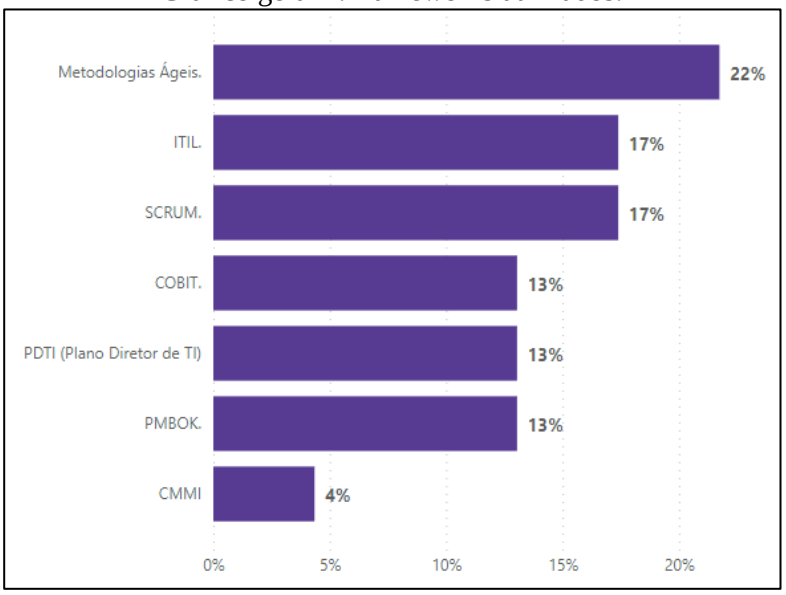
4.3 Quais são os frameworks e as metodologias utilizadas na empresa para que os times estejam em Compliance com as normas e diretrizes da governança de TI?

Os dados quantitativos foram obtidos a partir da pesquisa entregue para o setor de governança das organizações para mensurar a utilização de frameworks.

Empresas com o porte de 500 ou mais funcionários: 20 % utilizam ITIL, 20 % elaboram plano diretor (PDTI), 13 % utilizam o COBIT, Metodologias Ágeis, PMBOK e SCRUM.

Empresas com o porte de 0 a 99 funcionários: 38 % utilizam Metodologias Ágeis, 25 % utilizam SCRUM, 13 % utilizam o COBIT, ITIL, PMBOK.

Gráfico geral 7: frameworks utilizados.



Fonte: Autoria própria (2022).

4.4 Alinhamento da Segurança da Informação na Empresa

O alinhamento da Segurança será analisado a fim de verificar a adequação das empresas de acordo com a LGPD e a Gestão de Riscos.

Para responder esse tópico foram elaboradas 4 questões baseadas na ISO/27002. Os dados quantitativos foram obtidos a partir da pesquisa entregue para o setor de governança das organizações.

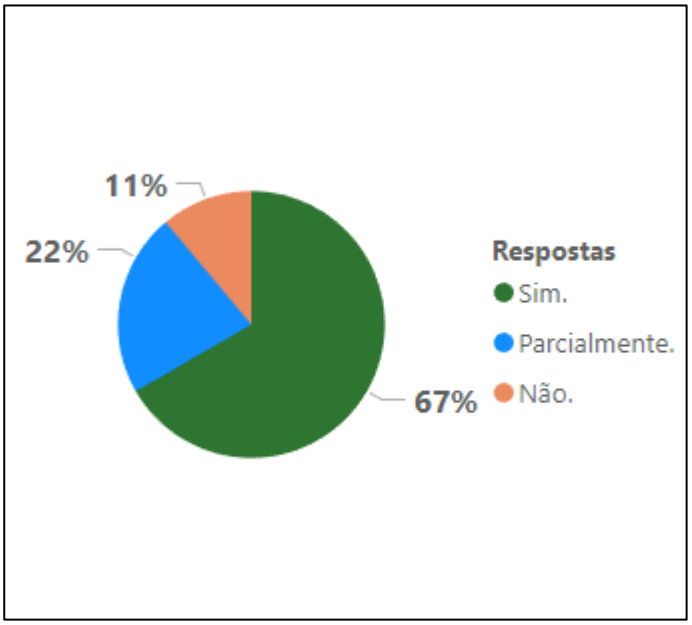
a) A empresa utiliza/conhece as normas de boas práticas da ISO/27002?

Das respostas obtidas 67 % das empresas responderam Sim, 22 % responderam parcialmente e 11 % responderam que não utilizam ou conhecem as normas de boas práticas da ISO/IEC 27002.

Empresas com o porte de 500 ou mais funcionários: 80 % das respostas foram que Sim e 20 % foram não.

Empresas de 0 a 99 funcionários: 50 % foram Sim e 25 % para Parcialmente e Não.

Gráfico 8: Conhecimento da ISO 27002.



Fonte: Autoria própria (2022).

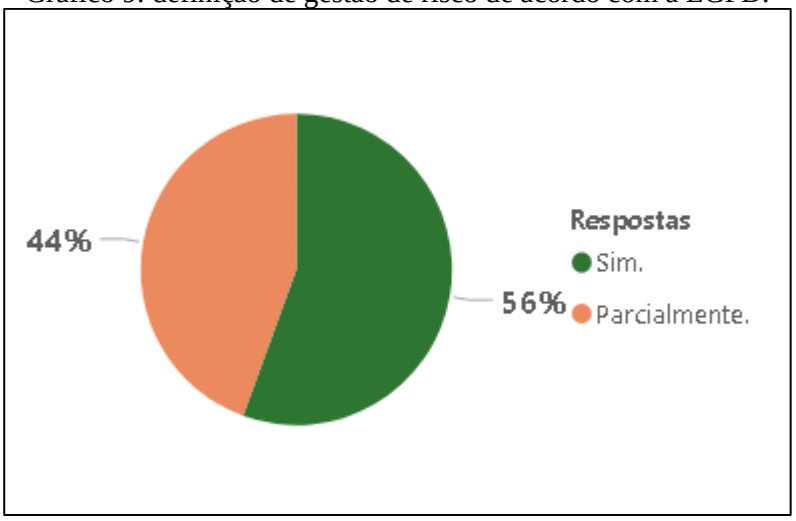
b) A organização define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto de acordo com a LGPD?

Foram no geral 56 % para Sim e 44% para parcialmente.

Empresas com o porte de 500 ou mais funcionários: 60 % Sim e 40% Parcialmente.

Empresas de 0 a 99 funcionários: 50 % para sim e 50 % para parcialmente.

Gráfico 9: definição de gestão de risco de acordo com a LGPD.



Fonte: Autoria própria (2022).

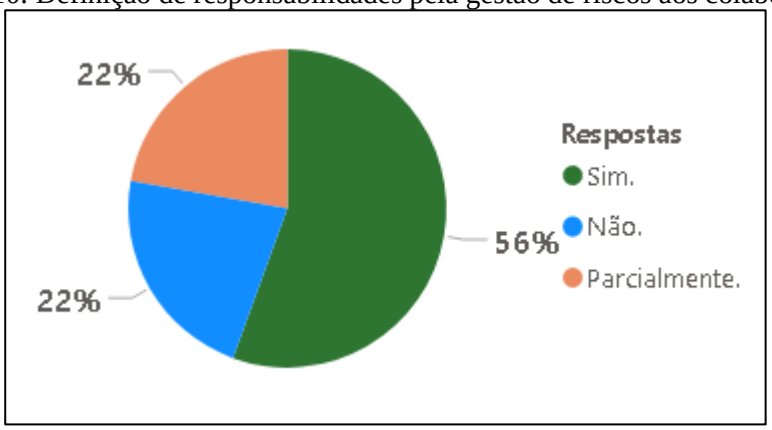
c) A organização define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI aos colaboradores?

Foram no geral 56 % para Sim, 22% para parcialmente e 22% para Não.

Empresas com o porte de 500 ou mais funcionários: 80 % Sim e 20% Parcialmente.

Empresas de 0 a 99 funcionários: 50 % para não, 25 % para parcialmente e 25% para Sim.

Gráfico 10: Definição de responsabilidades pela gestão de riscos aos colaboradores.



Fonte: Autoria própria (2022).

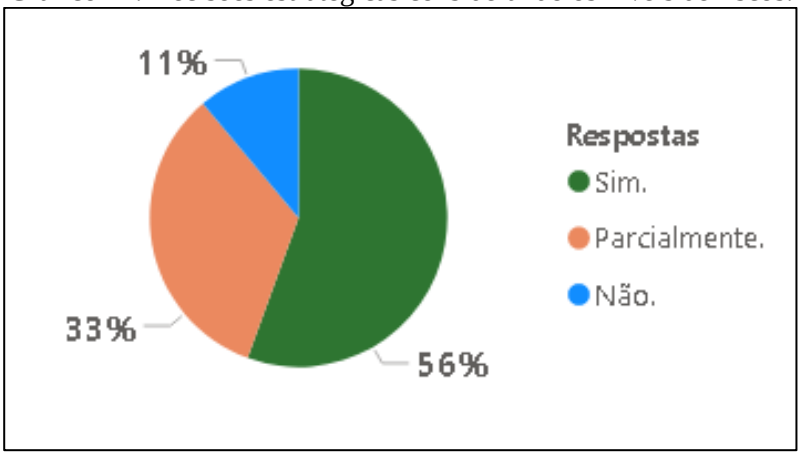
d) A organização toma decisões estratégicas considerando os níveis de risco de TI definidos?

Foram no geral 56 % para Sim, 33% para parcialmente e 11% para Não.

Empresas com o porte de 500 ou mais funcionários: 80 % Sim e 20% Parcialmente.

Empresas de 0 a 99 funcionários: 50 % para não, 25 % para parcialmente e 25% para Sim.

Gráfico 11: Decisões estratégicas considerando os níveis de riscos.



Fonte: Autoria própria.

5 Considerações Finais

De acordo com a pesquisa realizada, para alinhar a governança de TI com o plano

de negócios da empresa. Deve-se definir formalmente as diretrizes de governança tais como a clareza das regras dos negócios para o investimento no setor de TI, conhecimento e envolvimento de administradores e líderes seniores com os princípios descritos na ISO/IEC 38500 e executar auditorias periódicas para a avaliação da eficácia do alinhamento de TI ao negócio e entrega de valor.

As principais metodologias e frameworks utilizados pelas organizações para o desenvolvimento da governança de TI foram: Metodologias Ágeis com 22%, Scrum e ITIL com 17%, COBIT, PDTI (Plano Diretor de TI) e PMBOK com 13 % das respostas obtidas.

Sobre a segurança da informação, verificamos que a maioria das empresas entrevistadas estão de acordo com as normas de boas práticas da ISO/IEC 27002 e estão cientes dos riscos aos quais os negócios da organização estão expostos segundo a LGPD.

Com os resultados obtidos concluímos a resposta para a problemática.

Como alinhar a governança de TI com o plano de negócios da empresa, bem como o alinhamento com todos os setores e quais frameworks utilizar para o desenvolvimento da mesma.

"Governança de TI: a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização da TI." (WEILL, 2006).

Referências

ABNT. NBR ISO/IEC 38500. Governança corporativa de tecnologia da informação. Associação brasileira de normas técnicas. Rio de Janeiro, 2009. 21p.

Bruno Bellard Gomes. Estudo de caso sobre o Impacto da implementação da Norma NBR ISO/IEC 27002 em micro e pequenas empresas. São Paulo, 2009.

FERNANDES, AGUINALDO ARAGON; ABREU, VLADIMIR FERRAZ DE. Implantando a governança de TI: da estratégia à gestão dos processos e serviços. Brasport, 2014.

ISACA. COBIT 5: Modelo Corporativo para Governança e Gestão de TI. Rolling Meadows, IL (EUA): Information Systems Audit and Control Association, 2012. 98p.

IT Governance Institute: COBIT® 4.1. Framework Control Objectives Management Guidelines Maturity Models (2007)

Norma Brasileira ABNT ISO/IEC 27002. Tecnologia da Informação – Técnicas de Segurança – Código de prática para gestão da segurança da informação, Rio de Janeiro 2005.

TRIBUNAL DE CONTRAS DA UNIÃO. Governança de TI. Disponível em: < https://portal.tcu.gov.br/ >

WEILL, Peter; ROSS Jeanne W. Governança de TI: Tecnologia da Informação. São Paulo: M. Books, 2006.