MESTRADO PROFISSIONAL
EM ADMINISTRAÇÃO PÚBLICA

GOVERNANÇA DE TI EM ESTATAIS: DAS PRESCRIÇÕES FORMAIS AOS ARRANJOS PRATICADOS

FERNANDO HENRIQUE DE SOUZA SANTOS

Brasília-DF, 2023

FERNANDO HENRIQUE DE SOUZA SANTOS

GOVERNANÇA DE TI EM ESTATAIS: DAS PRESCRIÇÕES FORMAIS AOS ARRANJOS PRATICADOS

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Orientador
Professor Doutor Roberto Rocha Coelho Pires

Brasília-DF, 2023

FERNANDO HENRIQUE DE SOUZA SANTOS

GOVERNANÇA DE TI EM ESTATAIS: DAS PRESCRIÇÕES FORMAIS AOS ARRANJOS PRATICADOS

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Aprovado em 06 / 06 / 2023

Banca Examinadora

Prof. Dr. Roberto Rocha Coelho Pires - Orientador

Prof. Dr. Mauro Santos Silva

Prof. Dr. Pedro Luiz Costa Cavalcante

S237g Santos, Fernando Henrique de Souza
Governança de ti em estatais: das prescrições formais aos arranjos praticados / Fernando Henrique de Souza Santos. – Brasília: IDP, 2024.

168 p.
Inclui bibliografia.

Trabalho de Conclusão de Curso (Dissertação) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, Curso de Mestrado Profissional em Administração Pública, Brasília, 2023.
Orientador: Prof. Dr. Roberto Rocha Coelho Pires.

1. Governança. 2. Governança de TI. 3. COBIT. 4. TCU. 5. Arranjos. I. Título.
CDD: 351

Ficha catalográfica elaborada pela Biblioteca Ministro Moreira Alves
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

AGRADECIMENTOS

Aos meus pais, pelo carinho e sabedoria ao ensinar aos filhos que o caminho a ser perseguido é o do conhecimento, como a maior riqueza. Minha admiração eterna. Aos meus irmãos, irmãs, cunhados e sobrinhos, que em suas conquistas se tornaram fontes de inspiração, especialmente à minha irmã, professora Dra. Fátima Santos, pelo carinho, orientações e incentivo.

À Regina, pelo tempo dedicado ao nosso convívio e pela preocupação constante comigo, parceira na vida profissional, pessoal e no maior projeto, a criação dos nossos três queridos filhos-amigos. Aos filhos Bruno, Filipe e Carolina, pelo amor em cada encontro, sempre me encorajando e apoiando nesse desafio-conquista. Vocês, com as noras e o genro, trazem uma alegria especial à minha vida. Ao bruguelinho, meu neto Joaquim, que ainda não tem ideia do quanto me ensinou a perseverar enquanto aprende e insiste em aprender no início de sua vida; a Francisco, irmão de Joaquim, que está a caminho; e aos outros netinhos que ainda virão, essa semente de que sempre é possível conquistar novos caminhos, sem esquecer que infelizmente, para muitos outros, as porteiras estão fechadas e que ao abri-las mais do que um exemplo, devem ser vistas como a exceção em uma luta desigual.

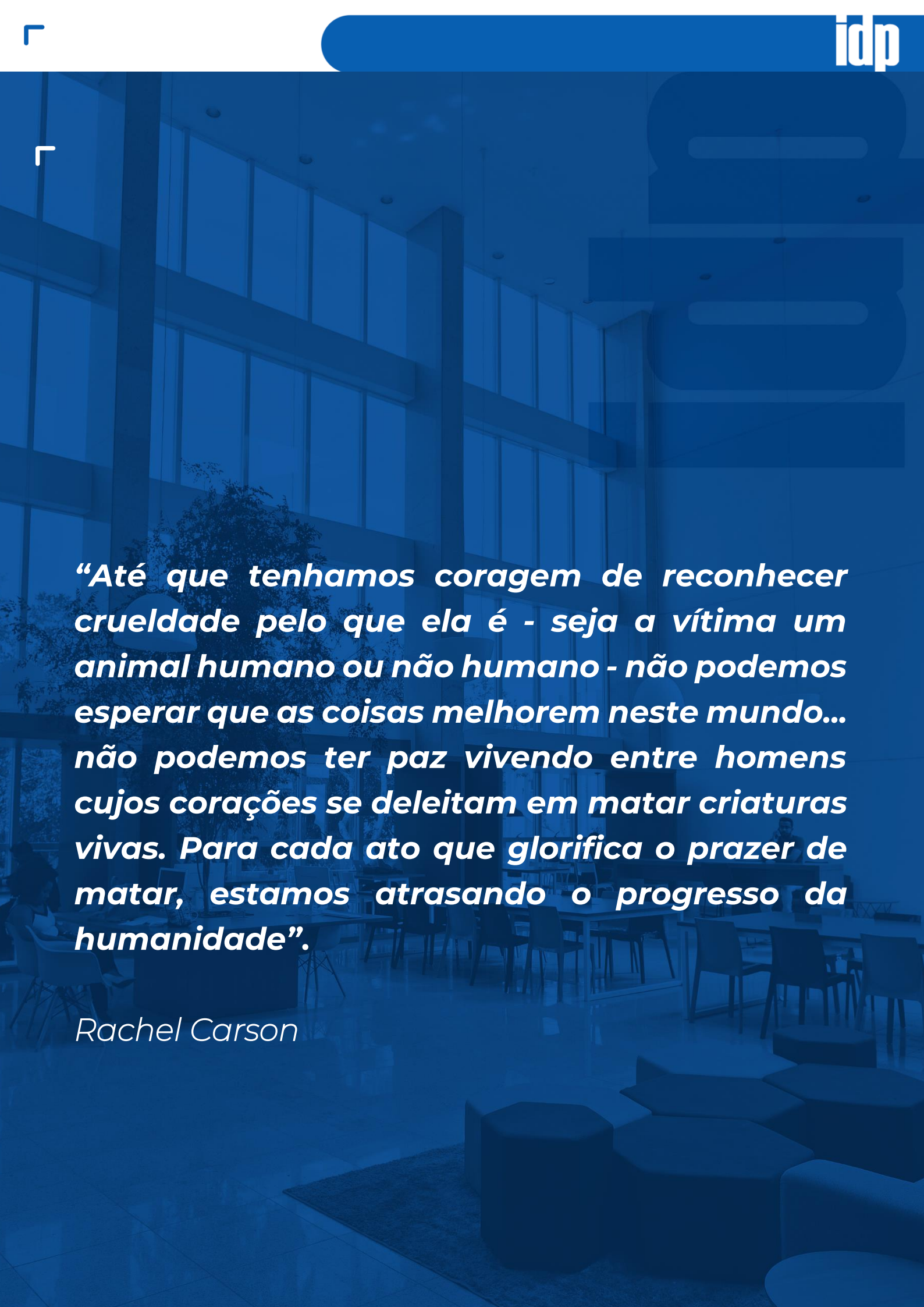
Aos meus amigos, colegas de trabalho e a todos que colaboraram com esta pesquisa, pela ajuda, apoio e compreensão, vocês são grandes parceiros. Muito obrigado.

Agradeço ao Programa de Pós-Graduação em Administração Pública do IDP, representado por seus docentes, equipe de apoio à pesquisa, equipes administrativas e coordenador, que estiveram sempre presentes com muita dedicação, profissionalismo e zelo durante um período particularmente complicado devido à pandemia. Obrigado por estarem sempre atentos aos detalhes.

Aos colegas de turma, um grupo muito especial, pelo companheirismo e conhecimento, elevando a qualidade dos debates ao longo de toda a jornada.

Aos professores que, desde o processo de seleção e durante toda essa jornada, dedicaram parte de seu tempo para nos trazer novos conhecimentos e depositaram confiança, principalmente em minha força de vontade. Muito obrigado. Um agradecimento especial ao professor Dr. Alexandre Gomide, que, com seu grande conhecimento,

tranquilidade e didática, me instigou a criar um olhar mais crítico ao longo do curso ele que junto com o professor Pedro Cavalcante, me deram a grande satisfação de ser premiado com seus vastos conhecimentos durante o processo de qualificação. Suas orientações permaneceram comigo e estão presentes em várias partes deste trabalho, seja por imprimir um olhar diferente, ou através dos alertas sobre os obstáculos que encontraria pelo caminho. Muito obrigado a ambos! Ao professor Dr. Mauro Silva, obrigado por dedicar parte do seu tempo a este trabalho. Sua presença como parte desta banca é muito enriquecedora e, ao mesmo tempo, dá maior prestígio ao trabalho. Ao meu orientador, professor Dr. Roberto Pires, cujo agradecimento não veio ao final por acaso, mas por uma atenção especial. Em primeiro lugar pela aceitação em ser meu orientador, o que me deixou muito honrado; e que com sua formação e vasto conhecimento dedicou parte do seu tempo me instigando a buscar novas leituras e a caminhar cada vez mais com autonomia e, como um bom mestre, foi habilmente me provocando para que eu delineasse minha estrada, como se faz em uma verdadeira jornada construtivista. Em segundo lugar pela facilidade com que em perguntas de poucas palavras me assegurou horas de reflexão, e que da mesma forma como o professor Dr. Gomide, me abriu a visão, me permitindo acreditar que poderia sair de um voo de perdiz para o das águias, mesmo sendo perdiz. E finalmente, porque além do conhecimento e qualidades como orientador, demonstrou a sensibilidade necessária, em alguns momentos difíceis deste trabalho, trazendo a tranquilidade que me permitiu transpor alguns obstáculos, comuns a quem faz parte da vida, minha admiração e agradecimento especial, espero poder ter correspondido. Me senti feliz e muito honrado em ter a ajuda e parceria de todos nessa jornada.



“Até que tenhamos coragem de reconhecer crueldade pelo que ela é - seja a vítima um animal humano ou não humano - não podemos esperar que as coisas melhorem neste mundo... não podemos ter paz vivendo entre homens cujos corações se deleitam em matar criaturas vivas. Para cada ato que glorifica o prazer de matar, estamos atrasando o progresso da humanidade”.

Rachel Carson

RESUMO

Este trabalho tem como objetivo fazer estudo exploratório dos fatores que influenciam a governança de TI, tomando como referência a opinião dos gestores de TI de uma grande empresa estatal, que utilizam os questionários com os indicadores de governança de TI do TCU e identificar como eles percebem a importância dessa ferramenta para a melhoria da governança de TI. Tais indicadores possuem viés fortemente prescritivo formal da "boa governança" que encontra na academia debates sobre sua efetividade, principalmente no que diz respeito a empresas estatais, com a perspectiva de que a governança pública pode ser mensurada, pautada em modelos de boas práticas, com padrão pré-definido de uma administração universalizada e de mercado. Outro viés é o de empresas estatais influenciadas por um modelo analítico, dependente da interação da organização com o ambiente e contexto onde está inserida, sofrendo influências da história da organização, da política e como estes diversos fatores interagem. Por intermédio de um estudo de caso foram submetidos questionários para os gestores de TI, de uma grande empresa estatal brasileira e uma das maiores do mundo, em sua área de atuação, e através de análise de Conteúdo Categorial buscou-se identificar, na percepção de executivos e gestores a importância dos indicadores adotados pelo TCU para avaliar a governança e contribuir para a gestão interna da organização, pela qual eles respondem. Este trabalho apoiou-se em análises qualitativa e quantitativa dos questionários e apresenta descobertas importantes, do ponto de vista destes gestores, de fatores que não são capturados pelo questionário como fatores políticos, culturais e de comportamento organizacional, na governança de TI de empresas públicas e que os indicadores prescricionais, usados pelo TCU, não são capazes de avaliar a governança da área onde atuam. Traz como achados a influência dos arranjos e do envelhecimento dos processos como fatores que influenciam a governança de TI. Estes resultados, contribuem para o debate, no que tange a governança e abre espaços para novas pesquisas na área de TI, que carece de outros estudos comparativos.

Palavras-chaves: Governança; Governança de TI; COBIT; TCU; Brasil; Arranjos; Indicadores da governança de TI; Indicadores prescricionais.

ABSTRACT

This work aims to carry out an exploratory study of the factors that influence IT governance, taking as reference the opinion of IT managers of a large state-owned company, who use the questionnaires with TCU's IT governance indicators and to identify how they perceive the importance of this tool for improving IT governance. Such indicators have a strong formal prescriptive bias of “good governance” that finds debates about its effectiveness in academia, especially with regard to state-owned companies, with the perspective that public governance can be measured, based on models of good practices, with pre-defined standard of a universalized and market administration. Another bias is that of state-owned companies influenced by an analytical model, dependent on the organization's interaction with the environment and context in which it operates, suffering influences from the organization's history, politics and how these various factors interact. Through a case study, questionnaires were submitted to IT managers, from a large Brazilian state-owned company and one of the largest in the world, in its area of activity, and through Categorical Content analysis, an attempt was made to identify, in the perception of executives and managers the importance of the indicators adopted by TCU to assess governance and contribute to the internal management of the organization, for which they are responsible. This work was based on qualitative and quantitative analyzes of the questionnaires and presents important discoveries, from the point of view of these managers, of factors that are not captured by the questionnaire, such as political, cultural and organizational behavior factors, in the IT governance of public companies and that the prescriptive indicators used by the TCU are not able to assess the governance of the area where they operate. Brings as findings the influence of arrangements and aging of processes as factors that influence IT governance. These results contribute to the debate regarding governance and open spaces for new research in the IT area, which lacks other comparative studies.

Keywords: Governance; IT Governance; COBIT; TCU; Brazil; Arrangements; IT governance indicators; Prescription indicators.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO


1

1 INTRODUÇÃO

Ao abordar o tema da governança pública no Brasil, é importante compreender que estamos nos referindo a ativos totais no valor de R$ 4.684,8 bilhões (exercício financeiro de 2017), dos quais 96% correspondem a empresas dos setores financeiros, de energia elétrica, petrolíferas e de gás (SILVA; SCHIMDT; KLIASS; 2019, p. 14 e 15). Conforme mencionado pelos autores, essas empresas possuem importantes relações fiscais, são imobilizadoras de capital pelo governo federal e exercem efeitos significativos sobre a vida econômica e social do país, sendo, portanto, de grande importância nacional. Nessa perspectiva, que ressalta a relevância de estudos e pesquisas na área de governança pública, incluindo a identificação do modelo de governança e desempenho dessas estatais, entre outros aspectos, situa-se esta pesquisa sobre governança de TI em estatais. A fim de compreender melhor o termo governança e suas perspectivas, é importante ter um entendimento básico das mudanças ocorridas na gestão pública.

Entre 1950 e 1960, a gestão pública era vista sob um viés técnico e jurídico, no qual as preocupações estavam voltadas para as mudanças organizacionais e procedimentais (POLLITT; BOUCKAERT, 2011). Na década de 1970, iniciaram-se os primeiros debates sobre a reforma pública. Surgiu, em meio a vários outros debates, uma preocupação com a governança voltada para resultados, decorrente da visão da NPM (New Public Management), com foco em um governo mais eficiente e direcionado para métodos amplamente utilizados pela iniciativa privada, como indicadores de desempenho e metas de contratos competitivos (POLLITT; BOUCKAERT, 2011).

Durante o período de 1990 a 2000, em decorrência da diminuição da confiança nos governos, surge uma preocupação crescente em relação à participação dos cidadãos e às interações com empresas privadas e organizações não governamentais, visando resgatar a confiança na esfera política. Nesse sentido, novos elementos são incorporados, uma vez que a governança passa a ser concebida como

algo mais abrangente, englobando os contextos políticos, a participação dos cidadãos e suas relações em um processo dinâmico.

Como resultado, surge uma segunda abordagem da governança, que passa a abranger a relação cooperativa e interdependente do Estado com outros atores sociais. Na visão de Rhodes (1996), a visão da governança corporativa limita a governança aos processos organizacionais e aos aspectos de direção, execução e controle das ações de gestão. Dentro desta mesma visão Pollitt e Huppe (2011) corroboram com essa visão e de que a governança corporativa está direcionada para os processos Intra organizacionais de direção e responsabilidade fiscal (*accountability*).

Observa-se, nesse sentido, a existência de perspectivas de governança que não são antagônicas, mas que consideram diferentes fatores e interações, influenciando a forma como cada uma dessas perspectivas é avaliada. Essas divergências na compreensão do significado da governança têm impacto não apenas no planejamento estratégico, mas também na obtenção dos resultados e no acompanhamento do processo. Ou seja, a visão da governança prescritivo formal não considera fatores importantes como os fatores políticos, e da integração da empresa estatal com o ambiente em que ela está inserida e seus arranjos. São fatores mais complexos, de difícil mensuração, mas que também influem no resultado da governança de TI.

Essas duas abordagens da governança estão em destaque neste trabalho: uma delas considera a capacidade de avaliar a governança com base em uma perspectiva formal e prescritiva, na qual os indicadores refletem a qualidade dos processos que estabelecem uma governança adequada. Nessa abordagem, a governança se destaca por sua capacidade de se adaptar aos parâmetros adotados pelas organizações privadas, que são avaliadas pelos resultados obtidos.

Essa visão da governança é amplamente defendida pelo Banco Mundial, que sugere a utilização de indicadores prescritivos para avaliar a chamada "boa governança" dos governos. O Tribunal de Contas da União (TCU) adotou essa perspectiva de governança e incluiu ações relacionadas à governança pública em seu planejamento estratégico de 2011-2015 (TCU, 2013).

Em uma outra abordagem, é apresentada uma visão da governança, onde ela pode ser influenciada pelo contexto em que a organização está inserida. Além disso, diferentes organizações, que

buscam atender à mesma política pública, podem adotar estratégias e arranjos distintos. Essas organizações também podem ser impactadas de maneiras diversas por interferências políticas, econômicas, sociais, bem como por relações multissetoriais e temporais. Em resumo, essas organizações podem apresentar respostas diversas dependendo das influências mencionadas.

A partir da experiência prática de gestores de TI, busca-se identificar quais são os fatores que influenciam a governança de TI. Dessa forma, pretende-se contribuir para o debate sobre a governança pública, e identificar fatores que os questionários do TCU não identificam e por esta razão prejudicam a avaliação da governança da TI. Para este trabalho, utilizou-se como referência os questionários de levantamento de indicadores de governança de TI adotados pelo TCU.

1.1. CONTEXTUALIZAÇÃO

A fim de estabelecer a compreensão do debate acadêmico em torno da governança pública, este estudo parte de um caso específico de análise da governança de TI em uma empresa pública. Com base nessa redução, busca-se retornar ao caso mais geral, trazendo o assunto de volta à origem da discussão e, assim, contribuir para o debate sobre as perspectivas da governança analítica e da governança prescritiva formal, tomando como referência a avaliação dos indicadores de governança adotados pelo TCU para empresas públicas no Brasil.

Para compreender a origem do debate, é necessário analisar o processo de importação do termo "governança" para o setor público, que foi introduzido no Brasil a partir de países de língua inglesa e ganhou ainda mais destaque em 2017, com o pedido formal do Brasil para se tornar membro da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) (MELLO, 2020). Conforme afirmam Caldeira et al. (2022, online, tradução nossa):

> De acordo com a política de governança brasileira, governança pública é um "conjunto de mecanismos de liderança, estratégia e controle implementados para avaliar, dirigir e monitorar a gestão, conduzir políticas públicas e prestar serviços de interesse da sociedade. (2017, art. 2º, I)".

Para Rhodes (1996), o conceito utilizado foi incorporado da definição da governança corporativa e tem escopo limitado, por estar

relacionado aos processos organizacionais e aos aspectos de direção, execução e controle das ações de gestão. É importante ressaltar, como citado por Caldeira (2021), que o conceito de governança pública, publicado em 2017 no art. 2º, I, durante o Governo Temer (2016-2018), não contemplou a participação social, nem no desenho, nem nas decisões sobre as políticas públicas. Isso resultou na exclusão da ação das redes nas implementações e acompanhamento dos serviços públicos, bem como na ausência das parcerias público-privadas (PPPs), entre outros aspectos.

Seguindo a linha de argumentação de que a governança pública brasileira teve uma compreensão limitada, afirmou-se (KOOIMAN, 1993; RICHARDS & SMITH, 2002, segundo CALDEIRA):

> A política de governança pública brasileira tem utilizado, portanto uma compreensão limitada do conceito de governança pública ao combinar elementos de 'governança corporativa' com 'boa governança'. Para fins analíticos, tomamos o conceito de governança pública como paradigma de gestão pública, caracterizado pela relação horizontal entre atores públicos e privados na concepção e gestão de políticas públicas (KOOIMAN, 1993; RICHARDS & SMITH, 2002, APUD CALDEIRA).

Portanto, no cerne do debate está o conceito de uma governança pública limitada aos processos organizacionais, caracterizada pela direção, execução e controle das ações de gestão. A esta perspectiva é atribuída a visão de uma governança prescritiva e normativa. Por outro lado, encontra-se a governança analítica, mencionada anteriormente por Kooiman, Richards e Smith, conforme citação de Caldeira (2022):

> Tem como elementos derivados desse paradigma a participação social no processo decisório de políticas públicas e as redes de implementação e prestação de serviços públicos, nas parcerias público-privadas, na transparência e responsabilidade social na coprodução de bens públicos. (CALDEIRA,2022).

Essa governança mencionada anteriormente utiliza indicadores prescritivos tanto para avaliar sua situação atual quanto para estabelecer os objetivos a serem alcançados pelas empresas. Os índices de desempenho, formados por indicadores, são recursos utilizados para comparar a evolução dos resultados, auxiliando na tomada de decisões e previsões. Um indicador é composto por uma ou mais variáveis e desempenha um papel importante na representação de algo real. Quando bem ajustados, os indicadores são valiosos aliados dos gestores, pois auxiliam nas tomadas de decisões.

A governança de TI em uma empresa desempenha um papel importante em seus resultados. No entanto, o termo "governança" não possui uma única interpretação. Conforme destacado por Cavalcante & Pires (2018), há diferentes perspectivas em relação a ele. Uma delas é a abordagem prescritiva formal da "boa governança", que utiliza um modelo de referência com dependência do contexto e das variações presentes no ambiente empresarial. Nesse sentido, a governança é estruturada com base em conceitos de boas práticas, sendo o índice de governança composto por indicadores que capturam e mensuram os processos relacionados à "boa governança". Essa abordagem é fundamentada na universalidade das “boas práticas” e não depende do contexto específico da empresa.

Por outro lado, há a perspectiva que tem como referência os resultados da evolução da governança dependerem do ambiente e contexto em que ela está inserida, bem como das interações da gestão, em resposta à dinâmica deste ambiente em sua relação com a organização.

O Tribunal de Contas da União (TCU) tem assumido a responsabilidade de contribuir para aprimorar a governança das Administrações Públicas Federais (APF). Para tanto, realiza levantamentos, apresenta conceitos e avalia a governança dessas entidades públicas, com um mesmo questionário.

Conforme se pode observar, o Decreto 9.203 de 22/11/2017 estabelece em seu artigo 2º que "governança pública é o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade." Neste sentido, o decreto expressa a necessidade de avaliar e monitorar a gestão.

O TCU criou, tomando como referência informações de várias instituições renomadas (conforme mencionado no item 1.3 deste trabalho), uma estrutura para avaliar a governança das Administrações Públicas Federais (APF), utilizando-se de índices gerais que têm, como um de seus componentes, o índice de governança de TI, o qual será tratado neste trabalho.

Acompanhar e entender a evolução da governança das empresas, com um recorte específico na governança de TI, é importante para a melhoria dos serviços prestados pelo Estado e para a gestão da governança pública.

Segundo Cavalcanti (2008), o fraco desempenho do setor público decorre, em parte, da falta de governança de TI. No documento "Levantamento de governança de TI (2014)", disponível no site do TCU, é afirmado que:

> O cenário apresentado pelo levantamento de governança de TI 2014 confirma a tendência de evolução identificada em pesquisas anteriores. Não obstante, o nível de adoção das práticas, no geral, ainda está distante de um cenário satisfatório para a Administração Pública Federal-APF. (TCU, 2014)

Ainda neste mesmo documento, no item “Benefícios esperados”, é afirmado que o maior benefício da avaliação da TI é a “a manutenção do processo de indução de melhoria da governança e da gestão de TI na APF o que tende a resultar em melhor desempenho das organizações na prestação dos serviços públicos à sociedade” (CAVALCANTE, 2014, acórdão 3.117). Neste item, é ratificada a relação cada vez mais forte entre a TI e os resultados do negócio.

O objetivo de otimizar recursos e alcançar melhores resultados é compartilhado não apenas pelo TCU, mas também pelos contribuintes, pelo poder executivo e pela sociedade em geral. Iniciativas para aprimorar a qualidade das organizações públicas são essenciais para o país, pois promovem um debate mais aprofundado em busca do que é melhor para a prestação dos serviços públicos. Ao considerar a importância do alinhamento da TI com o negócio, identifica-se que esse também é o pensamento de outros autores.

Em relação à importância do alinhamento da TI com o negócio, Weill & Ross realizaram uma avaliação da governança da TI em mais de 250 empresas em 33 países, com o objetivo de compreender o valor da TI para as organizações (WEILL; ROSS, 2006, p. 3).

Nesse contexto, constataram que empresas que alinham a governança de TI à governança da organização obtêm melhores resultados financeiros. Em um estudo realizado pela MIT Sloan School - CISR (Center for Information System Research) (2003, apud WEILLI & ROSS), os ativos de TI são apontados como um dos seis principais a serem monitorados pela governança corporativa, juntamente com os ativos humanos, financeiros, físicos, de propriedade intelectual e de relacionamento.

Nesse mesmo estudo, os autores constataram que as áreas de TI de grandes organizações adotam estratégias e arranjos distintos, sendo que o arranjo é uma consequência da estratégia adotada (WEILL; ROSS, 2006, p. 2 e 14). Além disso, destacam que, mesmo com arranjos diferentes, uma empresa pode obter bons resultados quando devidamente adaptada ao contexto em que está inserida. Em outras palavras, as empresas utilizam estratégias e arranjos diversos para alcançar bons resultados.

O Tribunal de Contas da União adota como conceito para governança uma visão que toma como referência a da governança corporativa, e é a partir deste modelo que calcula os índices de governança da empresa e o índice de governança da TI, conforme o Glossário Integrado 2021 portal v4. Estes índices apresentam um viés “prescritivo formal “da boa governança”, quando considerada a classificação apresentada por Cavalcante & Pires no trabalho “Variedades da governança pública” (2018). Em seu relatório de auditoria (iGovTI, 2014), o TCU evidencia ainda mais o indicador como indutor da melhoria da governança de TI. Nele o TCU afirma:

> Objetivando induzir a melhoria da governança de TI na administração pública federal, o TCU criou, no âmbito do levantamento de 2010, um índice que busca refletir, de forma geral, a situação de governança de TI de cada organização avaliada, denominado de índice de governança de TI (iGovTI, 2014).

Ainda em relação ao uso de indicadores, um outro desafio é identificar em quais bases eles devem ser definidos e como devem ser ponderados para representar e mensurar com precisão os processos da governança de TI. Isso ocorre devido à composição de diferentes

variáveis e à influência da subjetividade e do entendimento de quem os avalia.

Embora esses fatores sejam importantes na medição dos índices de governança, este trabalho não tem como objetivo avaliar os indicadores sob essa perspectiva, o que por si só justifica uma pesquisa específica. Aqui, pretende-se explorar quais fatores, na visão dos gestores de TI, impactam a governança de sua área de atuação e verificar se os indicadores de governança utilizados pelo TCU, são capazes de mensurá-los, como também identificar quais os fatores os questionários do TCU não capturam e que causam impacto na governança de TI de empresas estatais. Em uma forma secundária se pretende buscar identificar a qual das perspectivas da governança de TI estão associados esses fatores.

O paradoxo deste estudo se manifesta em duas questões. Por um lado, espera-se que indicadores prescritivos formais "da boa governança" sejam capazes de representar os processos institucionais e, assim, contribuir para a melhoria da governança, independentemente da organização ou área avaliada. Por outro lado, é importante considerar que a governança também é influenciada por fatores internos, externos e temporais, com suas inter-relações. Além disso, os resultados da governança dependem de estratégias e arranjos, e nem sempre esses fatores podem ser facilmente capturados ou mensurados devido à subjetividade, complexidade e influências envolvidas, como por exemplo as variáveis organizacionais que podem ser dependentes das variáveis do ambiente (LAURENCE; LORSH, apud MORESI, 2001).

Com o objetivo de contribuir para esse debate e compreender como os gestores de TI percebem a governança, foi escolhida como referência uma empresa do Governo Federal que é reconhecida por sua excelência em governança e é frequentemente elogiada por seus excelentes resultados e possui uma das mais bem estruturadas áreas de TI, dentro de sua área de atuação, no mundo. Essa empresa está classificada entre os maiores ROE (Retorno sobre o Patrimônio) do mundo em seu setor de atuação, o que demonstra sua capacidade de obter bons resultados e ao mesmo tempo desempenhar um papel importante na implementação das políticas públicas do Governo Federal.

Por meio da pesquisa realizada por questionário eletrônico e análise, conforme descrito na metodologia, o objetivo deste estudo foi

explorar, com base na avaliação dos gestores, quais fatores impactam a governança de TI e se os questionários do TCU são capazes de capturar os processos de governança de TI. A análise também usou como complemento um comparativo entre o que é avaliado pelos indicadores prescritivos formais e como os gestores de TI percebem a influência desses resultados na chamada "boa governança de TI", utilizando o levantamento realizado pelo TCU como referência. Além disso, buscou-se identificar descobertas nos resultados da pesquisa que possam revelar elementos relevantes, tanto em termos de conteúdo manifesto quanto de conteúdo latente.

1.2. O CARÁTER INVESTIGATIVO DA PESQUISA

Avaliar os resultados da "boa governança de TI" é um fator importante tanto para diagnosticar a qualidade dos processos executados na área quanto para definir e implementar ações de melhoria nos serviços prestados pela TI.

Neste estudo, buscou-se explorar os fatores que podem influenciar a governança e verificar se essas descobertas podem contribuir para o debate das perspectivas da governança, tendo como ponto de partida o caso específico da governança de TI em uma empresa estatal da área financeira. Essa empresa é reconhecida pelo mercado por sua excelência em governança, tanto na organização como na área de TI, assim como pelos resultados apresentados.

Devido à natureza investigativa, este estudo é caracterizado como técnico descritivo e exploratório, adotando a estratégia de estudo de caso. Os gestores de TI da empresa estatal da área financeira foram envolvidos neste trabalho, e a partir de suas respostas aos questionários elaborados para esta pesquisa, utilizando análise de frequência e de conteúdo, buscou-se identificar quais fatores influenciam essa governança.

Dessa forma, por meio de um estudo exploratório, busca-se identificar, além dos resultados das respostas de conteúdo manifesto sobre o uso de indicadores, quais fatores impactam a avaliação da governança de TI. Assim, a expectativa foi explorar as respostas para encontrar possíveis relacionamentos com as expectativas da governança de TI, contribuindo assim para o debate. Por essa razão, o

questionário utilizado como referência foi o do TCU, que é um exemplo com o qual os gestores se deparam ao longo de suas carreiras.

1.3. O MODELO ADOTADO PELO TCU

O Tribunal de Contas da União (TCU) acompanha as estruturas das organizações e realiza pesquisas para verificar a adoção das melhores práticas de TI, utilizando questionários estruturados com base em diversos modelos de referência. Esses modelos incluem as seguintes fontes: IBGC (Instituto Brasileiro de Governança Corporativa); o guia *Good Governance Standard for Public Service* - CIPFA (2004); o documento da *International Federation of Accountants* – IFAC (2001); o *Government Audit Directorate* – DAR (2000); o documento sobre governança elaborado pelo Ministério das Finanças da Holanda intitulado *Government Governance Corporate: governance in the public sector, why and how?*; o modelo *Institute of Internal Auditors* – IIA (2001), publicado pelo Departamento de Finanças Irlandês em 1992; o documento *Princípios de Governança Corporativa*, publicado pela Organização para a Cooperação e Desenvolvimento Econômico - OCDE (2004) e o guia *Control Objectives for Information and Related Technology - COBIT*.

O COBIT é uma framework amplamente utilizada no mercado. Essa framework (COBIT 5.0) é dividida em 4 grandes domínios, que por sua vez estão agrupados em 34 processos que alinham a TI ao negócio. Esses 34 processos possuem objetivos de controle e são avaliados por meio de um formulário padrão com perguntas previamente tabuladas. A pontuação obtida nessas respostas, que varia de 1 a 5, determina o grau de maturidade dos processos, do domínio e, por consequência, da organização que está sendo avaliada.

De maneira semelhante, o formulário apresentado pelo TCU também possui pontuações para as diversas questões. Essas questões são respondidas pelos gestores da estatal avaliada e compõem diferentes indicadores de governança, de acordo com os agrupamentos identificados. Assim, existem indicadores para governança de compras, governança de pessoas, governança de TI, entre outros. Todos esses indicadores compõem o indicador geral da governança da empresa.

Embora seja reconhecido que a composição dos indicadores, bem como o significado de cada componente e a quantificação de sua valorização para avaliar a governança, sejam importantes na definição dos indicadores, entende-se que esse é um assunto bastante abrangente que exigiria um estudo específico e, portanto, deve ser considerado em um trabalho separado.

No entanto, caso sejam identificadas observações relevantes ao longo deste estudo, à luz das teorias envolvidas, serão consideradas as informações e os alertas que indiquem a necessidade de estudos complementares.

1.4. OBJETIVOS GERAIS

Este trabalho teve como objetivo principal realizar um estudo exploratório dos fatores que influenciam a governança de TI, com base na opinião dos gestores que utilizam os questionários contendo os indicadores de governança de TI do TCU. Em outras palavras se busca analisar a percepção dos gestores de uma importante estatal brasileira acerca dos indicadores de governança que eles respondem constantemente em um questionário do TCU e que têm impacto sobre a imagem da gestão interna da organização, pela qual estes gestores respondem.

1.5. OBJETIVOS ESPECÍFICOS

- Identificar se, na visão dos gestores de TI entrevistados, o questionário do TCU, por meio de seus indicadores, é adequado e abrange os fatores que influenciam os processos que refletem os resultados da governança de TI;
- Realizar uma revisão da literatura, abordando estudos teóricos e metodológicos sobre os conceitos utilizados, as definições adotadas e os dados coletados;

1.6. ESTRUTURA PRELIMINAR DA DISSERTAÇÃO

Este trabalho está organizado em 4 capítulos. O Capítulo 1 fornece uma introdução e uma contextualização do tema em estudo.

O Capítulo 2 apresenta a fundamentação teórica que abrange os assuntos a serem abordados no trabalho, buscando situar o leitor no contexto do debate sobre as perspectivas existentes, de modo geral, da governança em empresas públicas e, mais especificamente, trazendo essa abordagem para a governança de TI nesse tipo de organização.

No Capítulo 3, é apresentada a metodologia e a natureza dos dados utilizados, com descrição dos resultados da pesquisa, como foram construídos e o que eles representam. Também são apresentados os formulários da pesquisa e a metodologia utilizada para sua elaboração. Descreve-se a pré-análise dos dados, a construção do corpus e os objetivos de cada questão formulada, bem como os resultados obtidos, a análise realizada e seus achados.

O Capítulo 4 apresenta as conclusões do trabalho, suas contribuições, as limitações encontradas e propõe possíveis desdobramentos para pesquisas futuras.


2

2 FUNDAMENTAÇÃO TEÓRICA

A criação de indicadores e metas são itens herdados da governança corporativa, e, segundo Peters (2012), "por esta razão, tem seu foco em obtenção de resultados." No caso de empresas públicas sem fins lucrativos, esses resultados estão voltados para a melhoria do serviço público, como resultado de políticas públicas aplicadas.

A averiguação do indicador, em termos de uma boa representação dos processos ocorridos nas organizações, bem como o sentido da explicação sobre os fatores que contribuíram para esses resultados, é objeto de divergências no meio acadêmico.

Dentro dessa visão, busca-se a apropriação de alguns conceitos do que são políticas públicas e como elas podem influenciar uma empresa de administração direta ou indireta. Em uma abordagem sobre política pública, Dye afirma que ela seria "tudo o que os governos escolhem fazer ou deixar de fazer" (2013, p.3). Ressalte-se que é dado ao executor das ações as atribuições do papel e responsabilidade. Quando expressa que é o governo quem escolhe o que deve ou não ser feito, ele atribui ao governo o papel e responsabilidade pelas definições das políticas públicas.

Outra consideração a ser feita é que Dye esclarece que políticas públicas não são representadas exclusivamente pelas ações que o governo decide tomar, mas também pelas que decide não fazer. Como

terceiro ponto relevante, deve-se destacar que aquilo que é consequência de uma ação, de forma não consciente, não deve ser considerado, neste conceito, como política pública. Portanto, cabe observar que o governo pode influenciar tanto pelo que decidir fazer quanto pelo que decidir não fazer. Dentro dessa conjuntura, é possível compreender que a empresa pública, responsável pela implementação das políticas de governo, tem sua governança atrelada a fatores externos que podem nem estar explicitados pelo governo, e muitos deles só podem ser observados por um olhar mais cuidadoso.

Segundo William Jenkins, a política pública é:

> um conjunto de decisões inter-relacionadas - tomadas por um ator ou grupo de atores políticos - que se referem à seleção de objetivos e dos meios necessários para alcançá-los, no âmbito de uma situação especificada em que o alvo dessas decisões estaria, em princípio, ao alcance dos mesmos atores" (JENKINS apud HOWLETT et al., 2014, p. 3).

Nessa definição, Jenkins inclui os atores como responsáveis por decisões, tanto no que diz respeito à seleção de objetivos quanto aos meios necessários para alcançá-los, destacando assim a importância do agente público na implantação da política pública.

Outro ator importante são os clientes da empresa pública, que percebem, de forma distinta, a qualidade como a melhoria do serviço entregue, não sendo o foco principal os custos envolvidos. Nesse sentido, Peters, em seu artigo "O que é Governança?", afirma que "a ênfase em governança reflete de muitas formas as preocupações públicas com relação à capacidade de seus sistemas políticos de agirem de forma efetiva e decisiva no sentido de resolver problemas públicos" (2013, p. 127). Com essa visão, ao abordar a governança, ele trata da preocupação de que a qualidade da governança pública esteja atrelada à resolução de problemas públicos, cujos clientes são os cidadãos.

Segundo Capano, Howlett e Ramesh (2015), é necessário avaliar indicadores quantitativos e qualitativos para verificar o desempenho da política e os problemas políticos. O debate sobre governança também apresenta outro componente, que é a diversidade de entendimentos sobre o que é governança.

Pollitt afirma, em relação à definição do termo governança, que "Desde o final da década de 1990 'governança' se tornou um termo imensamente popular entre acadêmicos e profissionais" (2009, p. 20). Segundo o autor, o termo se popularizou tanto que existem muitos significados atribuídos a ele.

A dificuldade do uso de indicadores para medir a governança é abordada por Rose-Ackerman, conforme citado por Buta & Teixeira (2020), em seu artigo "Governança pública em três dimensões: conceitual, mensural e democrática". Na citação, Rose-Ackerman esclarece que o conceito de governança é "polissêmico, multidimensional e carregado de ambiguidade" (2020, p. 327). Nesse sentido, há um debate no meio acadêmico sobre os fatores que influenciam a governança pública e se eles são independentes do contexto onde a organização está inserida, ou se é possível utilizar indicadores padronizados, simplificando assim a um modelo baseado em boas práticas para se obter uma boa governança de TI.

Ainda nesse contexto, Apaza argumenta que a confiabilidade dos indicadores não é completamente garantida: "A precisão na comparação da governança ao longo do tempo e entre países por meio dos indicadores agregados continua sendo de certa forma pouco confiável..." (2009, p. 142).

Cavalcante & Pires (2018), em seu artigo sobre governança pública, contribuem com essa análise, alertando para a diversidade do uso do termo "governança pública" e o risco da simplificação conceitual. Eles também ressaltam a dificuldade da utilização de um padrão que prescreva as ações públicas, com normativos, padrões e indicadores a serem publicados para a melhoria e adoção de novas políticas.

No sentido de valorizar o uso de indicadores, outros posicionamentos podem ser encontrados, como o de Merry, conforme citado por Buta & Teixeira (2020), que entende os indicadores como incentivo para uma busca pela melhoria do desempenho.

Da mesma forma, os predicados atribuídos à governança e utilizados por Marini & Martins são os de que a governança "é para resultados, porque se orienta para o desempenho e para o valor público; é colaborativa, porque requer interações multi-institucionais e entre múltiplas instituições e a sociedade. A governança é a capacidade institucional para resultados" (2014, p. 50). Portanto, é considerada, pelos autores, em uma perspectiva de ordem prática e

transformacional como um processo. Nesse sentido, deve-se destacar que, apesar de considerar que a governança é para resultados, os autores alertam para o fato de que a governança é colaborativa, por manter interações multi-institucionais, e, dessa forma, pode sofrer influência de fatores externos.

Nesta linha de discussão, o debate acerca do uso de indicadores na área de TI não poderia ser diferente. Weill & Ross atribuem à "Governança de TI: a especificação dos direitos decisórios e da framework de responsabilidades para estimular comportamentos desejáveis na utilização da TI" (2006, p. 8). Esta framework é formada por alguns fatores que são usados com o objetivo de identificar padrões de comportamentos e que são tratados como o reflexo da melhoria da governança de TI. Ainda segundo Weill & Ross (2006, p. 121), para avaliar o desempenho da governança de TI de uma empresa, deve-se avaliar o quão bem ela atinge os níveis previstos na framework de governança de TI.

Para Carvalho, "A governança de TI traz para a empresa uma nova cultura de gestão baseada em medições, que considera características não financeiras, mas que controla fatores que apontem para o futuro, através de indicadores" (2004, p. 142). Nessa visão, é criada a framework COBIT, que tem como objetivo o gerenciamento e aprimoramento dos processos de TI, por meio da medição de indicadores. Para Fernandes e Abreu (2006), a melhoria da governança de TI pode ser obtida com o acompanhamento de indicadores de processos de TI, baseados na framework COBIT, que podem ser usados para atingir metas e, por sua vez, alinham a área de TI aos requisitos de negócio. Esse parece ser o norteador utilizado pelo TCU para considerar que a busca pelo atingimento dos indicadores funciona como indutora da melhoria da governança, o que também é sugerido pelo Banco Mundial como diretriz a ser seguida para a melhoria da governança pública.

Neste sentido, percebe-se que a perspectiva prescricional é direcionada, assim como na governança corporativa, para resultados, desconsiderando-se a influência de outras variáveis além daquelas presentes nesse contexto. Essa abordagem não leva em conta elementos importantes, como tradições, culturas administrativas, dependência de caminhos, capacidades institucionais e particularidades dos arranjos e políticas públicas, reduzindo a governança pública a apenas uma parte do todo (BIANCHI et al., apud CALDEIRA, 2021).

Além disso, entende-se que, ao apresentar indicadores baseados em boas práticas universais, a ideia é simplesmente persegui-los, como se fosse uma prescrição na qual nenhuma outra variável pudesse impactar tais resultados.

Por outro lado, a perspectiva de uma visão analítica da governança, considerando sua constante interação com diversos fatores que influenciam seus resultados. É importante ressaltar que essas diferentes visões são percebidas por meio de modelos distintos para a captura dos resultados da governança. Enquanto no primeiro modelo basta um planejamento para alcançar um determinado resultado, no segundo modelo são essenciais o monitoramento e a capacidade de ajustar a direção da organização, incluindo seus arranjos e processos.

É evidente que existem várias abordagens ao mensurar e compreender a evolução da governança. É necessário compreender os arranjos que devem compor o monitoramento da evolução da governança e os contextos específicos nos quais estão inseridos. No caso de organizações públicas envolvidas na prestação de serviços e políticas públicas para a população, é crucial situar em qual contexto político-institucional os agentes públicos dessas organizações estão atuando. Para acompanhar a evolução ou retrocesso da governança pública, é fundamental entender quais fatores são determinantes para tais mudanças e se os indicadores são capazes de capturar os fatores externos e internos à organização.

Portanto, não é suficiente apenas definir indicadores e acompanhar seus resultados. É crucial que se possa mensurar e identificar se esses indicadores realmente representam as melhorias alcançadas e, em caso contrário, quais outros fatores contribuíram para essas discrepâncias. É necessário identificar até que ponto os fatores externos podem impactar essas avaliações e se os indicadores prescricionais formais conseguem capturar e explicar as mudanças ocorridas.

Por essa razão, é crucial compreender se os resultados dos indicadores de governança das empresas estatais refletem os esforços empreendidos para o aprimoramento de suas governanças. Logo, é necessário estar atento ao fato de que, nos casos em que os indicadores de governança pública não são representativos, seja por não capturarem essas variáveis ou por não fornecerem uma explicação adequada para os resultados observados, eles podem gerar

informações que não contribuirão para o acompanhamento e para a implementação de ações de melhoria pelos gestores. Deve-se considerar que outros fatores externos e até mesmo internos, decorrentes de decisões políticas, interações multi-institucionais, ações dos agentes públicos, entre outros, podem influenciar essas discrepâncias.


3

3 METODOLOGIA

Este capítulo tem como objetivo apresentar informações sobre a metodologia adotada, sendo subdividido em quatro seções. Na seção 3.1, será apresentada a metodologia considerando o tipo de pesquisa e os critérios utilizados, dentro de um contexto científico. Prosseguindo para a seção 3.2, será descrita a construção do corpus, a coleta dos dados e a pré-análise. A seção 3.3 fornecerá uma descrição da pré-análise dos dados.

3.1. SOBRE A METODOLOGIA ADOTADA

Por se tratar de pesquisa na área das ciências sociais, é considerada a interação sujeito-objeto, compartilhando a ideia de que a realidade social é resultado de uma construção social e, portanto, parte do paradigma interpretativista em uma realidade intersubjetiva (SACCOL, 2009). Segundo Saccol, na epistemologia construtivista, não há uma realidade a ser descoberta, as verdades e significados são construídos a partir da inter-relação, ou seja, a construção dessa realidade ocorre por meio do processo de interação social com os significados criados e adotados coletivamente.

Considerando as informações acima, esta pesquisa será de natureza qualitativa, focando principalmente na construção de significados a partir da perspectiva dos participantes. Será uma pesquisa exploratória, buscando compreender a construção feita pelos participantes em relação ao uso prescritivo de indicadores para mensurar e comparar a "boa governança de TI" (Tribunal de Contas da União, questionário utilizado para avaliação da governança de TI em empresas estatais). Quanto ao tipo, será também descritiva, pois aborda as percepções das pessoas sobre os fatores que influenciam a governança de TI. No final, será realizada uma análise de conteúdo categorial, utilizando a técnica de Bardin, que combina uma abordagem qualitativa com uma abordagem quantitativa, ao tratar as frequências de classe para as categorias selecionadas de todas as questões envolvidas, independentemente do objetivo aparente das perguntas elaboradas.

Segundo Vergara (1998), as pesquisas exploratórias são realizadas em áreas com pouco conhecimento acumulado e sistematizado. Por serem investigativas, essas pesquisas não possuem hipótese definida, embora hipóteses possam surgir ao longo do estudo ou até mesmo ao final.

Com o objetivo de contribuir para o debate sobre governança, abordando tanto a perspectiva prescritiva formal quanto a governança como uma perspectiva analítica, a estratégia adotada é identificar os fatores que influenciam a governança e que não compõem os indicadores de governança de TI, adotados pelo TCU, na visão dos gestores dessa área. Como fator secundário dos resultados da pesquisa se pretende identificar, nas narrativas dos gestores, os pontos que merecem destaque em relação à assertividade destes indicadores, definidos no questionário do TCU. É importante ressaltar que por esta razão a pesquisa não teve como objetivo identificar a qual perspectiva da governança pertenciam as categorizações e sim identificar, tendo como referência a epistemologia construtivista de que os conhecimentos dos gestores, apesar de não se pautarem no conhecimento teórico possuem uma verdade e significados advindos da inter-relação, onde a construção dessa realidade se dá por meio do processo de interação social com estes significados criados e usados coletivamente. Dessa forma não se busca entender se eles sabem distinguir as perspectivas e sim identificar em suas respostas, independente de seus conhecimentos teóricos, se os indicadores prescritivos formais, utilizados pelo TCU, são capazes de avaliar a “boa governança de TI”.

Esta pesquisa utiliza o estudo de caso de uma grande empresa estatal do setor financeiro, reconhecida como uma das maiores do Brasil, com estrutura e processos bem estabelecidos, sujeita a controles internos e auditorias internas e externas. Essa empresa é considerada um exemplo de qualidade nos serviços prestados e obteve resultados que a posicionaram entre as dez empresas mais rentáveis do mundo, em sua área de atuação, no ano de 2021.

Devido às características desse trabalho e à utilização de um estudo de caso, optou-se pela abordagem da pesquisa exploratória.

3.2. CONSTRUÇÃO DO CORPUS

O levantamento de informações foi realizado por meio da técnica de pesquisa da observação direta extensiva, utilizando um questionário conforme a classificação de Marconi e Lakatos (2021, p. 243). O questionário foi desenvolvido e respondido em um formulário online disponibilizado por link, visando facilitar o acesso e permitir respostas por meio de smartphones. O público-alvo selecionado para a pesquisa foram executivos e gestores de gerência média de TI (total de 14 gestores, de um universo de 133) da empresa pesquisada, devido à experiência em governança de TI que possuem e sua capacidade de análise crítica dos processos. Essa abordagem online foi adotada para minimizar as dificuldades de escassez de tempo decorrentes das funções ocupadas pelos executivos e gerentes de nível médio.

As questões foram distribuídas da seguinte forma: três questões iniciais com o objetivo de identificar a função exercida pelo participante da pesquisa, o tempo de ocupação dessa função e se já haviam tido contato com o formulário do TCU. As questões de 4 a 6 abordaram diretamente o uso dos indicadores, seguindo a técnica denominada por funil, proposta por Marconi e Lakatos (2021), onde a pergunta começa de forma mais abrangente e se torna mais específica. Já as questões de 7 a 9 apresentaram os indicadores do TCU com o intuito de provocar uma avaliação crítica por parte dos participantes em relação aos resultados desses indicadores e justificar os fatores que impactam a governança de TI. Na questão número 8, foi utilizada como referência outra empresa estatal do setor financeiro, com o objetivo de estimular a comparação dos indicadores e, principalmente, gerar justificativas que possam indicar os fatores que impactam a avaliação da governança de TI.

A pergunta 10 foi formulada de maneira aberta, solicitando quaisquer considerações por parte dos participantes da pesquisa, permitindo, dessa forma, o levantamento e a descrição de aspectos não identificados anteriormente.

Na elaboração do questionário (Apêndice B), foram consideradas as perspectivas de governança, adaptando-as ao contexto específico de TI, levando em conta a abordagem utilizada pelo TCU para avaliar a governança de TI em empresas estatais.

3.3. PRÉ-ANÁLISE

Em uma análise exploratória inicial da evolução dos índices de governança de TI, obtidos dos questionários do TCU, foi avaliado o comportamento de uma empresa estatal do setor financeiro no período de 2017 a 2021. Após identificar esse comportamento, conforme apresentado na Tabela 1 a seguir, observou-se uma descontinuidade na melhoria do indicador de governança da empresa "A" entre os anos de 2018 e 2021, com uma redução aproximadamente duas vezes maior do que o ganho obtido no período de 2017 a 2019.

Tabela 1 - Índices de governança de TI da empresa "A" entre 2017 e 2021

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	93	96	90,6

Fonte: elaborada pelo autor com base em dados do TCU (2021).

Ao avaliar tais comportamentos, verificou-se um crescimento do índice de governança de TI entre 2017 e 2018, mantendo a empresa "A" acima da média de governança das estatais da mesma área de atuação. No entanto, houve uma queda desse índice entre 2018 e 2021, levando-a a uma faixa abaixo da média. Com base nesses dados iniciais, a pesquisa se concentrou em um estudo de caso dessa empresa "A", uma vez que ela já apresentava valores consolidados na governança e teve sua curva de tendência modificada entre 2018 e 2021. Isso levou a supor a existência de alguma interferência no percurso da governança da empresa, o que motivou a utilização de técnicas exploratórias para compreender esse comportamento e identificar o que pode ter causado essa alteração de tendência e o que esse comportamento representa para a governança de TI.

Além disso, a queda do índice de governança chama a atenção em relação a esse padrão de comportamento, especialmente considerando que empresas do setor financeiro seguem recomendações de entidades reguladoras. Elas são acompanhadas por auditorias internas e externas, possuem processos de controles internos e são submetidas periodicamente a avaliações de certificações de entidades externas. Esses mecanismos fazem parte de um procedimento que visa estabelecer uma governança com maior controle, buscando melhorias contínuas nos processos e,

principalmente, focando em resultados para reduzir os riscos para a economia do país.

É importante destacar a peculiaridade do período avaliado, devido às mudanças na política pública no Brasil, resultantes da troca de poder em duas ocasiões, em curto espaço de tempo. A primeira mudança ocorreu devido ao impeachment sofrido por Dilma Rousseff, do PT (Partido dos Trabalhadores), que governou até o final de agosto de 2016. Em seguida, Michel Temer, membro do MDB (Movimento Democrático Brasileiro), assumiu o governo e cumpriu mandato até 2018, quando Jair Bolsonaro, então filiado ao PSL (Partido Social Liberal), foi eleito.

Outra característica singular é o surgimento dos primeiros casos de COVID-19, identificados internacionalmente em novembro de 2019, na China. A partir de 30 de janeiro de 2020, a situação foi considerada uma emergência pública internacional e, em 11 de março do mesmo ano, a Organização Mundial da Saúde (OMS) a declarou como uma pandemia. Isso resultou em diversas mudanças nos comportamentos das organizações.

Essas mudanças ocorreram sob forte influência global, uma vez que o fechamento de processos produtivos levou muitas equipes a trabalharem remotamente. Isso provocou uma grande alteração nos processos internos e externos das organizações, além de afetar seu relacionamento com a sociedade de maneira mais ampla. Como resultado, as organizações foram forçadas a revisar suas estruturas e controles de forma abrupta, sem a realização de análises de riscos ou estudos de impacto.

Dadas essas características, é de se esperar que a identificação da existência ou inexistência da influência desses fatores seja observada de maneira mais rápida, devido aos contrastes provocados por mudanças ocorrendo de forma isolada e ao longo de intervalos maiores de tempo.

Essas circunstâncias apresentam características "sui generis" para o estudo da influência de fatores externos na administração pública e, consequentemente, para o objeto deste trabalho, que se concentra na governança de TI de empresas estatais.

Diante desse fato, foram consideradas algumas abordagens em relação às perspectivas da governança, e foi elaborado um questionário (Apêndice B), utilizando a opinião dos gestores da empresa "A" como

referência. Quanto à forma, o questionário abrangeu perguntas abertas e fechadas, seguindo a técnica de pesquisa de observação direta extensiva por meio de questionário, conforme a classificação de Marconi & Lakatos (2021, p. 243).

O questionário foi desenvolvido e respondido na plataforma do Google, devido à sua facilidade de acesso e possibilidade de resposta por meio de smartphones. Esse ambiente foi escolhido para minimizar as dificuldades decorrentes da escassez de tempo enfrentada pelos executivos e gerentes.

Foram selecionadas algumas questões fechadas para identificar se os respondentes faziam parte do público-alvo e facilitar as respostas às questões abertas, servindo como um "aquecimento". Ao final, foi incluída uma pergunta que permitia aos gestores fazerem observações adicionais que considerassem importantes sobre o assunto.

Com o objetivo de compreender melhor quais fatores impactam a governança de TI das empresas estatais, também foram incluídas perguntas que, de acordo com Marconi & Lakatos (2021), caracterizam-se por serem abertas, diretas e de opinião.

Para essa sequência de perguntas abertas, foi utilizada a técnica conhecida como "funil", em que se começa com perguntas mais abrangentes e, aos poucos, avança-se para questões mais específicas, conforme descrito por Marconi & Lakatos (2021, p. 229-230).

3.4. METODOLOGIA PARA ANÁLISE DOS DADOS

A metodologia utilizada para a análise de dados neste trabalho é qualitativa, por empregar a análise de conteúdo de Bardin, por meio da técnica de análise temática ou categorial, a fim de identificar nas respostas dos questionários as categorias mencionadas e relacioná-las às perspectivas da governança. Além disso, a metodologia também possui uma abordagem quantitativa, pois utiliza recursos estatísticos para avaliar as frequências das respostas nas questões de quatro a seis, bem como o uso da frequência de classe na análise de conteúdo das questões de quatro a dez.

No estudo do corpus, foram adotados três tipos de abordagem para as perguntas de quatro a seis. A pergunta visa identificar como os sujeitos pesquisados se posicionam em relação à avaliação dos

questionários do TCU, concordando ou não com a afirmativa da questão, e também solicita uma justificativa para a resposta. Na primeira abordagem, o conteúdo foi lido com o objetivo exclusivo de identificar a manifestação de concordância ou discordância, atribuindo-se o resultado como "Sim" ou "Não". Mesmo quando o sujeito não expressou explicitamente o "Sim" ou o "Não", buscou-se inferir a partir de sua resposta. Os resultados dessa pergunta serão apresentados a seguir. No final do trabalho, serão realizadas comparações entre esses valores e os valores obtidos pela segunda abordagem, que consistiu na análise de conteúdo das respostas das questões de quatro a dez. A terceira abordagem diz respeito às descobertas relacionadas à perspectiva da governança de TI e às abordagens pretendidas para a conclusão do trabalho.

Para a categorização, realizou-se a análise do corpus, utilizando as duas perspectivas de governança como referência: a perspectiva analítica e a perspectiva prescritivo-formal, conforme o artigo *Governança Pública* de Cavalcante & Pires (2018, p. 11).

Para utilizar como referência das influências externas, foi adotada a caracterização nos ambientes das organizações, conforme descrito por Moresi (2001, p. 68), com algumas adaptações. As referências internas foram estabelecidas durante o processo de leitura, estruturação e análise dos dados. Foi criada uma categoria na qual são agrupados os casos em que não foi possível identificar a resposta em nenhuma das duas perspectivas da governança e em que a resposta não está diretamente relacionada às perspectivas da governança, mas sim às questões que podem gerar desvios nos fatores que influenciam o resultado dos questionários, independentemente da perspectiva de governança à qual estejam associados.

Dessa forma, busca-se identificar quais fatores podem impactar o resultado do questionário, mas que não se enquadram em nenhuma das duas perspectivas da governança. A categorização foi definida de acordo com o Quadro 1.

Quadro 1 - Categorias, unidades de registro e de contexto.

Categorização	Unidade de Registro	Unidade de contexto
	Influência Externa	*1
	Influência Interna	*2

Perspectiva analítica da governança	Influência Temporal	*3
Perspectiva prescritivo formal da "boa governança	Representação do processo	
	Prescritíva/Normativa	
	Mensurável	
Não Identificada		

Fonte: elaborado pelo autor

Após a categorização adotada se buscou relacioná-lo com as diferentes perspectivas da governança. Foi criada uma categoria "Não Identificada" que tem como objetivo classificar as marcações que não foram identificadas ou não se enquadram em nenhuma das duas perspectivas.

Quanto à unidade de registro, foram utilizados os fatores que caracterizam as perspectivas da governança. Para a governança na perspectiva analítica, as unidades de registro adotadas foram externa, interna e temporal. As unidades de contexto foram criadas de acordo com as referências apresentadas no Quadro 1.

3.5. DEFINIÇÃO DA CATEGORIZAÇÃO ADOTADA

Para definir a categorização, foi seguida a metodologia de Bardin (1977), que envolve as seguintes fases em ordem cronológica: pré-análise, exploração do material, tratamento dos resultados, inferência e interpretação. Durante a categorização, foram observadas as seguintes etapas e observações:

- Leitura flutuante de todo o material obtido como resultado da pesquisa junto aos gestores.
- Efetuada a codificação para os formulários de categorias de análise, à partir de do referencial teórico.
- Definição dos trechos que fazem sentido para o estudo e separados em segmentos, como unidades de registros.

- Estabelecimento de estrutura organizada onde os dados brutos são agrupados estabelecendo-se uma classificação.

- Agrupadas as unidades com o mesmo indicativo de fatores e relacionadas às perspectivas.

- Avaliados os dados em relação ao referencial teórico e efetuada a interpretação e inferências.

Como unidades de registro, foram adotados os elementos que caracterizam a perspectiva da governança, citados anteriormente, e associados a essas categorias. Essa escolha baseou-se em diversas referências teóricas, como Cavalcante & Pires (2018), Caldeira (2021) e Tarapanoff et al. (2001), além das escolhas e elaboração do próprio autor, a partir da análise de conteúdo.

Para definir as unidades de contexto, foram escolhidos os fatores ou variáveis associados à unidade de registro de cada categoria, principalmente com base na classificação dos textos recebidos como respostas dos questionários.

No caso de respostas que não puderam ser identificadas em nenhuma categoria, foi adotada a categoria "Não identificada ou não Informada". Para essa categoria específica, não foram definidas unidades de registro nem unidades de contexto.

A seguir, são apresentadas as unidades de registro e as unidades de contexto associadas, referenciadas no Quadro 1. Para a unidade de contexto abaixo, foi adotado o modelo de ambiente externo padrão apresentado por Moresi (2021), que inclui os fatores que influenciam uma organização em uma abordagem de inteligência organizacional e competitiva. Também foi verificado se os fatores desconsiderados na definição brasileira da governança pública, mencionados por Bianchi et al. (2021), estavam contemplados nas unidades de contexto.

Quadro 2 - Quadro com unidades de contextos de influência externa.

Influência Externa – Condições Legais, Condições Políticas, Condições Econômicas, Condições demográficas, Condições Sociais, Condições Culturais, Condições Ecológicas, Condições Tecnológicas, Concorrentes, Fornecedores, Clientes, Entidades Reguladoras, inter-relação com outros órgãos. *Pandemias consideradas aqui como condições ecológicas, uma vez que os demais itens

estão relacionados em outros itens, como condições econômicas, condições sociais, entre outras.

Fonte: elaborado pelo autor a partir de definição de Moresi (2001)

Como unidade de contexto, para influência interna, foram adotados alguns fatores que caracterizam elementos internos da organização, tomando como referência as informações passadas pelos gestores. Só foram considerados aqui fatores que ou não são mensuráveis por indicadores simples, há necessidade de uma avaliação analítica ou por intermédio de uma avaliação dinâmica.

Quadro 3 – Unidades de contexto de influências externas

Influência interna - cultura e comportamento organizacional, liderança e fatores psicossociais do trabalho, arranjos da organização, arranjos de TI.

Fonte: elaborado pelo autor tomando como referência a análise de conteúdo.

Devido à dificuldade de caracterizar todos os possíveis fatores que podem sofrer influência temporal, optou-se por descrevê-la de forma mais genérica, permitindo o entendimento e facilitando-se assim o que se pretende classificar como marcações do texto ou “tags”.


4

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS OBTIDOS

Os resultados são apresentados da seguinte maneira: dos itens "a" até o "f", foi realizada uma análise do conteúdo manifesto das questões 1 a 6 do formulário de pesquisa. No item "g", são apresentados os resultados estatísticos da análise de conteúdo. Os itens 4.1 e 4.2 apresentam a análise descritiva das respostas dos questionários e estabelecem uma conexão com a teoria. O item 4.3 traz considerações sobre os resultados, enquanto o item 4.4 traz as considerações finais, avaliando os objetivos definidos, as contribuições do trabalho, as limitações e as dificuldades encontradas, além de fornecer recomendações para trabalhos futuros.

Em relação às análises das questões apresentadas, foram obtidos os seguintes resultados:

a) Nas questões um a três, foram obtidas informações sobre as funções dos entrevistados e seu conhecimento em relação aos formulários. Neste levantamento, todos os sujeitos que responderam à pesquisa ocupam cargos gerenciais (Tabela 2), que são o público-alvo. Desses, apenas dois estão na função há menos de dois anos, ambos ocupando cargos executivos. Geralmente, esses cargos são ocupados no final da carreira, quando o funcionário já possui mais de 25 anos na empresa (Tabela 3). Não houve descarte de respostas ao questionário.

Tabela 2 - Distribuição dos susijeitos pesquisados por função (%)

Executivo	Gerência média
42.86%	57.14%

Fonte: elaborada pelo autor

Em relação ao tempo em que ocupa a função, a Tabela 3 apresenta a distribuição do sujeito pesquisados por tempo de função (%), a seguir:

Tabela 3 - Distribuição do tempo de exercício da função dos pesquisados

Menos de 2 anos	Entre 2 e 4 anos	acima de 4 anos
14.29%	14.29%	71.43%

Fonte: elaborado pelo autor

A questão 3 teve como objetivo identificar se os funcionários conheciam os questionários do TCU e que tipo de experiência haviam vivido em relação a eles. A estrutura de TI da empresa sujeita ao estudo de caso possui uma área específica de governança de TI, como é comum nas áreas financeiras. Por esse motivo, é muito comum que esse questionário seja respondido pela equipe de governança, enquanto as demais áreas estão envolvidas apenas nas questões relacionadas às suas áreas de atuação.

Nos dados avaliados, 7,14% afirmaram não conhecer e nunca ter respondido o questionário do TCU, enquanto 92,86% afirmaram conhecer e 50% afirmaram conhecer e já ter respondido ao questionário. Considerando que a empresa possui cerca de 4.000 colaboradores e que a grande maioria não tem contato com esse questionário, o número de entrevistados que já o responderam ou o conhecem foi considerado bastante positivo. Ao entregar a pesquisa para encaminhamento ao público alvo, foi observado como fator importante que as pessoas conhecessem o formulário do TCU ou o framework do COBIT, que são o foco da pesquisa. Essa provavelmente é a razão para o percentual expressivo de entrevistados que conhecem o formulário.

A inclusão do conhecimento do formulário do COBIT como alternativa foi feita porque ele é amplamente utilizado pelos controles internos e auditorias na área de TI, serviu como um dos documentos de referência para o desenvolvimento do framework do TCU e tem como base o uso de indicadores prescritivos formais da "boa governança de TI". Essa alternativa foi incluída para permitir a avaliação caso o número de entrevistados que conhecem o formulário fosse muito baixo. A Tabela 4 apresenta os resultados dessa questão.

Tabela 4 – Percentual de pesquisados que conhecem o questionário do TCU

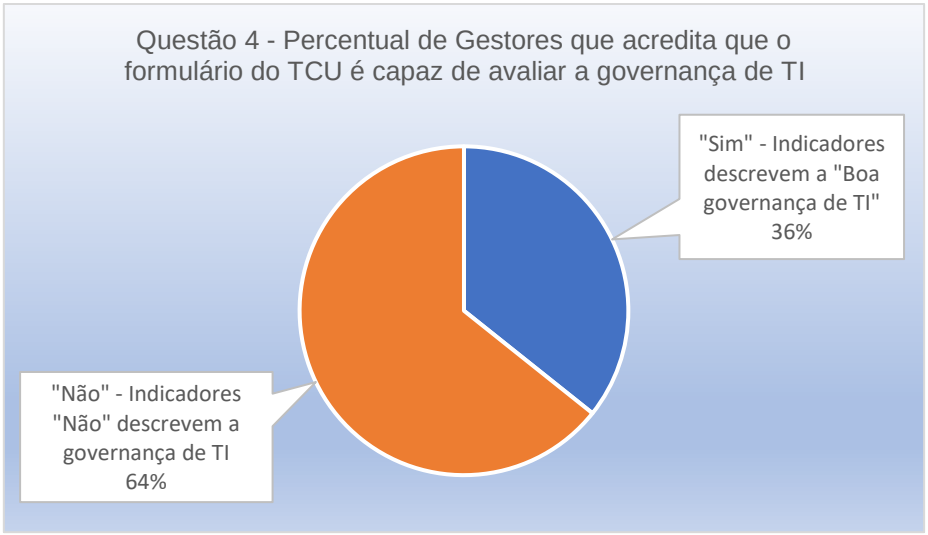
NR-Não respondeu	Conhece – NR	Conhece - Resp.

7.14%	42.86%	50,00%

Fonte: Elaborado pelo autor

A questão quatro teve como objetivo identificar a opinião dos sujeitos da pesquisa em relação ao questionário do TCU e verificar se eles consideram que o questionário é capaz de capturar os processos que representam a governança de TI. Essa pergunta foi feita de forma espontânea, sem fornecer informações ou sugestões sobre os fatores que podem influenciar os indicadores da governança de TI. O resultado mostrou que 64% dos gestores entendem que os indicadores não são suficientes para capturar os processos que representam a governança de TI.

Figura 1 - Percepção dos gestores em relação ao formulário do TCU avaliarem a governança de TI.



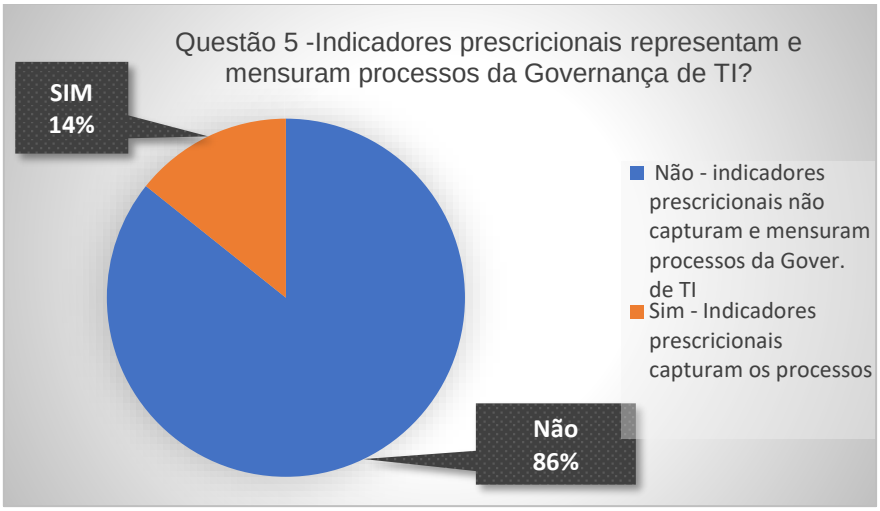
Fonte: elaborado pelo próprio autor.

Como primeiro resultado, obtivemos que 36% dos participantes afirmaram que o questionário do TCU é capaz de capturar o resultado da governança de TI, enquanto 64% responderam que o questionário não é capaz de capturar os resultados da governança de TI. Essa pergunta foi formulada como uma escolha espontânea, não mencionando quais influências os indicadores poderiam sofrer, permitindo que os participantes informassem, caso identificassem, quais fatores não eram capturados pelos formulários do TCU e que impactavam a governança de TI. Nas respostas dessa questão, surgiram os primeiros achados, mencionando fatores externos e internos que

influenciam a governança pública e que não são capturados pelos indicadores prescritivos, tais como: impactos causados por mudanças de tecnologia, fatores psicossociais do trabalho, cultura organizacional (*Path dependent*) e conhecimento.

Com o objetivo de identificar se, na opinião dos participantes, existem fatores que influenciam o resultado da governança de TI e que não podem ser representados ou capturados por indicadores, foi feita a pergunta a seguir. Foi observado um aumento no número de participantes que entendem que existem outros fatores que os indicadores prescritivos não representam (Figura 2).

Figura 2- Respostas dos gestores em relação aos indicadores prescricionais



Fonte: elaborado pelo próprio autor

Esta questão provocou uma mudança na distribuição das respostas dos gestores pesquisados. Quatorze por cento (14%) respondeu "Não", como exemplificado por um participante: "Penso que tudo é possível de ser mensurado apesar da dificuldade com coisas não tangíveis". Os outros 86% dos entrevistados responderam que existem fatores capazes de influenciar o resultado da governança de TI e que não podem ser representados. Dentre os fatores citados, destacam-se "questões como estratégia, arquitetura, segurança, conformidade, entre outros aspectos". Neste ponto, é importante ressaltar o que afirmam Weill & Ross em relação à governança de TI: "A estratégia e organização da empresa definem os comportamentos desejáveis que motivam a governança" (Weill & Ross, 2006, p. 152). Os autores também enfatizam que a eficácia das estratégias, juntamente com os arranjos

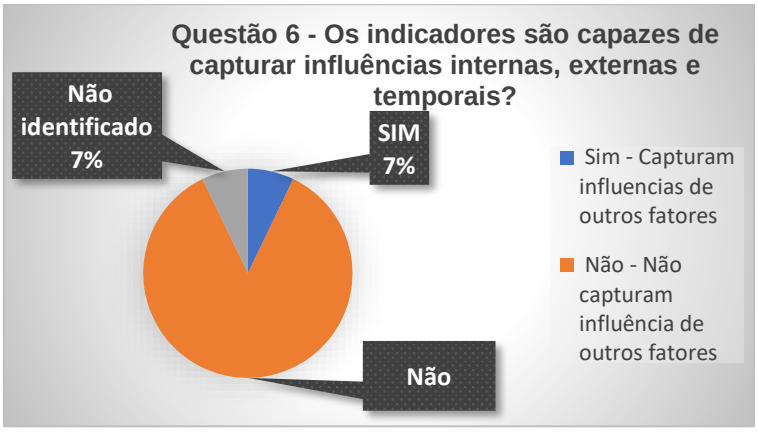
de governança definidos para a empresa, reflete na capacidade de atingir as metas de desempenho de negócio declaradas (Weill & Ross, 2006). Arquitetura, estratégia e segurança são alguns dos fatores que fazem parte do arranjo da TI. Assim, estratégias e arranjos de TI diferentes geram motivações diferentes para a governança.

Neste caso, se processos passados influenciam nos novos, que provocam estratégias, arranjos e metas diferentes, gerando diferentes motivações para a governança, faz sentido utilizar um questionário padrão para capturar a boa governança em diferentes empresas? Neste sentido, não corremos o risco de cometer um erro ao comparar unidades de análise que são diferentes? Como alertam Pollitt & Bouckaert (2006, p. 7-8), países diferentes possuem pontos de partida e histórias diferentes.

Adotando essa visão para a área de TI, é necessário questionar se a governança de TI, com estratégias, arranjos e pontos de partida diferentes, inserida em políticas e contextos distintos, pode ser avaliada por um mesmo questionário.

Com o objetivo de verificar, em uma pergunta com resposta estimulada, se os indicadores são capazes de capturar a influência de fatores externos, internos e temporais, não houve uma mudança considerável nas respostas. Verificou-se que 7% dos participantes da pesquisa acreditam que os indicadores prescritivos capturam a influência dos fatores externos, internos e temporais, e 7% tiveram respostas não identificadas em nenhuma das duas classificações. Por outro lado, o percentual dos participantes que entendem que os indicadores prescritivos não são capazes de capturar fatores externos, internos ou temporais permaneceu em 86% (Figura 3).

Figura 3 - Capacidade dos formulários do TCU capturarem influências externas, internas e temporais



Fonte: elaborado pelo próprio

Novamente, a resposta teve 7% dos pesquisados que entendem que os indicadores do TCU capturam a influência de fatores internos, externos ou temporais, e um sujeito da pesquisa cujo conteúdo não ficou muito claro, considerado não identificado. Os demais entendem que os indicadores do TCU não são capazes de capturar a influência de fatores externos, internos ou temporais, totalizando 86%.

Dos fatores citados que os indicadores não conseguem capturar, os principais fatores que impactam a governança de TI, tomando como referência o formulário do TCU, foram obtidos na seguinte ordem de citação: "condições políticas" - 34 vezes citados; "cultura e comportamento organizacional" - 15 vezes; "entidades reguladoras" - 09; "fator psicossocial do trabalho" e "conhecimento" - 07 vezes; "tecnologia" - 05 vezes; "fatores externos" (citados de forma genérica) e "clientes" - 04 vezes; "fator econômico", "legal", "arranjo de TI", "estratégia" e "liderança" - 03 vezes.

Outros fatores foram citados em menor número: "terceirização"; "turnover"; "fatores internos" (citados de forma genérica); "mudanças de governo"; "mudança de política financeira do governo (apetite por resultado e ao risco)"; "vinculados a aspectos temporais da coleta e da necessidade do acompanhamento das informações da governança de forma contínua", alertado por dois sujeitos da pesquisa; "mudanças internas com reorganização na estrutura de funcionamento" e "políticas de cargos e salários".

Outra questão levantada diz respeito ao direcionamento do questionário, segundo o sujeito pesquisado, atende apenas ao cenário que o TCU precisa capturar. Em relação a este item, há uma informação não explicitada que demonstra a insatisfação do gestor com o uso do questionário. Na percepção dele, o questionário atende às necessidades do TCU, mas não ajuda a avaliar nem a desenvolver a governança de TI em sua empresa, como afirmam os documentos do TCU. Com isso, o sujeito pesquisado demonstra que não utiliza o resultado para nenhum outro objetivo, exceto o de atender a uma necessidade do TCU.

É possível perceber a existência e citação de vários fatores externos e internos que não estão previstos nos indicadores prescritivos. Todos são fatores dinâmicos e que dependem das características específicas de cada empresa. Dessa forma, podemos

entender que é um achado importante, pois direciona o resultado para a perspectiva da governança analítica e dinâmica, como as condições políticas, que possivelmente ganharam um destaque ainda maior por causa das diferentes mudanças políticas pelas quais a empresa passou em um curto espaço de tempo, com três governos em apenas quatro anos.

Outro fator levantado, com grande ênfase, foi o da cultura e comportamento organizacional, que sofre influência do ambiente externo e se apresenta de forma dinâmica, com características específicas em cada organização.

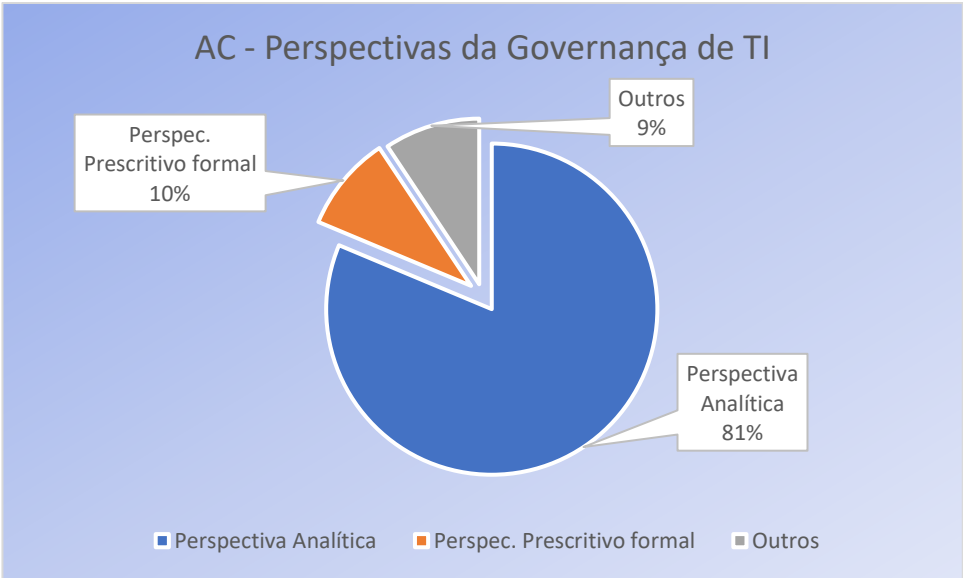
As questões de sete a dez foram elaboradas com o objetivo de contribuir para a análise de conteúdo. Por essa razão, não foram elaborados gráficos ou levantamentos estatísticos com base exclusivamente no relatório da análise de conteúdo. Essa análise foi feita em conjunto com todas as respostas analíticas obtidas, das questões quatro a dez. Para a análise de conteúdo, as frases foram subdivididas em "marcações (tags)" por conteúdos textuais, de acordo com o sentido e as unidades de contexto definidas. Foram identificadas 134 marcações (tags) e para cada resposta foram definidas tantas marcações quantas identificadas nas unidades de contexto ou unidade de registro. Assim, uma resposta pode ter várias marcações ou até mesmo nenhuma.

O resultado da análise de conteúdo apresentou a seguinte distribuição entre as categorias definidas, considerando as perspectivas da governança apresentadas por Cavalcante & Pires (2018): 81% das respostas estão alinhadas com a perspectiva da governança analítica, 10% com a perspectiva prescritiva formal e 9% em outras categorias. É importante destacar a aproximação dos valores obtidos pela avaliação do conteúdo manifesto quando comparados ao conteúdo latente. Mesmo quando a pergunta foi abordada em uma pesquisa espontânea, o resultado não apresentou uma diferença significativa, indicando que, na experiência dos gestores dessa empresa, os indicadores prescricionais não são suficientes para capturar os processos que representam a chamada "boa governança de TI". No item 4.1, serão apresentados os resultados da "Análise dos dados e Achados", onde uma avaliação mais detalhada de cada questão será feita.

Outro fator importante no resultado desta pesquisa diz respeito aos entrevistados. Como pode ser observado, os questionários foram respondidos por gestores experientes, sendo 42,86% de executivos e

57,14% de gerentes médios. O universo consiste em uma equipe de executivos de TI da empresa com cerca de 23 membros, enquanto a gerência média possui atualmente cerca de 113 membros, em uma área que deve abranger mais de 5.000 colaboradores. Dos gestores, 71,43% têm mais de quatro anos na função, 14,29% entre dois e quatro anos, e igual percentual abaixo de dois anos na função e dos pesquisados 92,86% conhece o questionário do TCU.

Figura 4 - Tendência da perspectiva investigada por análise de conteúdo.



Fonte: elaborado pelo próprio

As questões de sete a dez foram examinadas por meio da análise de conteúdo categorial, conforme proposto por Bardin, juntamente com as questões quatro a seis. Além disso, foram destacados trechos que reforçaram os achados desta pesquisa.

4.1. AS PERSPECTIVAS DA GOVERNANÇA PRESCRITIVO-FORMAL

Conforme abordado anteriormente, a perspectiva prescritivo-formal da governança é amplamente utilizada, encontrando respaldo principalmente em áreas de controle, como auditorias, órgãos de controle interno e entidades regulatórias (CAVALCANTE & PIRES, 2018). O Tribunal de Contas da União (TCU) adota um conjunto de indicadores

para avaliação da governança de TI nas APFs. Esses indicadores são padronizados, independentemente da área de atuação das organizações. Neste estudo, foram identificados alguns achados em que os participantes consideram que o uso desses indicadores representa os processos de TI. De acordo com os participantes 4, 6 e 8:

> O questionário aborda questões essenciais no dia a dia da produção em TI. A dificuldade que surge, em alguns pontos, é a de conectar a prática com os processos ali notificados. Os termos por vezes não são os mesmos do uso prático de cada empresa (SP4).

"Sim, é suficiente, uma vez que o questionário do TCU é bastante amplo e abrange de maneira bem completa todos os principais indicadores de governança de TI" (SP6).

"Sim. De forma geral, o questionário engloba os mecanismos de liderança, estratégia e controle para possibilitar o monitoramento e avaliação da gestão de TI" (SP8).

Pelos termos apresentados nas respostas, percebe-se uma visão de governança limitada aos controles. Pouco se observa, na pequena quantidade de respostas que concordaram com a visão prescritivo-formal da "boa governança", argumentos que não sejam relacionados à capacidade de mensurar e representar adequadamente os processos da governança pública.

4.2. A GOVERNANÇA EM UMA PERSPECTIVA ANALÍTICA

Em contraposição ao que foi exposto na seção anterior, a grande maioria dos participantes demonstrou entender que os indicadores usados pelo TCU – prescritivos formais da "boa governança", não conseguem capturar a influência dos ambientes externo, interno e temporal na governança de TI. Essa informação ficou evidente quando, no início desta pesquisa, 36% dos participantes entendem que o questionário do TCU é capaz de mensurar a governança de TI, enquanto 64% entendem que tais indicadores não capturam tais processos.

Ao longo das perguntas subsequentes e de suas respectivas justificativas, o número de participantes que acreditam que os indicadores prescritivos formais conseguem capturar os processos da governança de TI diminuiu para 7%, com mais 7% apresentando

respostas não claras. Mesmo que consideremos que as respostas não identificadas estivessem a favor do uso dos questionários do TCU para a avaliação da governança de TI, esse resultado não ultrapassaria 14%, em contraste com os 86% que entendem que os questionários do TCU não conseguem representar os processos da governança de TI. Estas informações serviram como uma análise secundária, uma vez que o foco principal do trabalho diz respeito a percepção de executivos e gestores de uma importante empresa estatal brasileira acerca da contribuição dos indicadores de governança de TI que eles respondem em questionários do TCU e que geram impacto sobre a imagem e gestão interna da organização pela qual eles respondem.

Ao longo da análise e com o aprofundamento do conteúdo das respostas, surgiram questões que evidenciam fatores não contemplados pelos indicadores prescritivos-formais, considerando o formulário do TCU. Durante a classificação dos conteúdos textuais, diversos achados foram identificados, destacando-se os principais conforme listados abaixo:

> Sim, existem fatores que podem afetar a governança de TI que não estão restritos à existência ou não de práticas ou processos instituídos. Em particular, em empresas que podem sofrer interferências políticas em suas administrações, alguns pontos podem não ser capturados. Um desses pontos é o nível de comprometimento dos funcionários e gestores (SP6).

"O grande fluxo de saída de funcionários decorrente de planos de demissão e aposentadoria demonstra como um fator externo pode interferir. A alta renovação nos quadros de gestores também é um fator importante" (SP6).

> Os indicadores nos ajudam a compreender diversos fatores, mas não podem prever todas as situações e influências (internas ou externas) no ambiente que está sendo analisado. Fatores como política, economia e mudanças administrativas tendem a influenciar as corporações como um todo, incluindo a governança de TI. Acredito que a política adotada pelo Governo Federal não priorizava a governança de forma geral. Isso refletiu em todos os níveis, resultando em um relaxamento em função de outras prioridades (SP7).

Políticas administrativas que não valorizam a governança nas instituições e as consideram como um processo oneroso tendem a provocar mudanças nos comportamentos em relação à manutenção dos processos e de seus controles. É evidente, segundo a opinião dos gestores, como as práticas políticas em mudanças de governo impactam diretamente as empresas estatais. Todos os casos mencionados acima demonstram os impactos da política pública. No caso do SP7, ele destaca o impacto causado pela decisão política de não priorizar a governança, podendo afetar o comportamento organizacional e os fatores psicossociais do trabalho. Isso evidencia a dificuldade de capturar, por meio do formulário prescritivo formal, o impacto de fatores externos sobre a governança da TI.

"[...] Acredito que tem relação com o envelhecimento do processo e não ocorreram atividades de revitalização com as novas realidades" (SP10). Essa resposta foi dada quando questionado se o gestor concordava com a redução do valor do índice de governança de TI apresentado no formulário. Os processos precisam ser readequados com o passar do tempo, inclusive devido às inovações, assim como os arranjos institucionais.

De acordo com Teng, Grover & Fiedler (1996), as variáveis devem ser atualizadas constantemente para melhorar seus resultados, o que corrobora com a afirmação do gestor de que o processo envelhece.

Em sua teoria da contingência, Lawrence & Lorsh (apud MORESI, 2001) ressaltam que não há uma única maneira de se organizar para obter os melhores resultados. Os arranjos institucionais são estabelecidos de acordo com o ambiente externo de uma organização. As organizações, portanto, sofrem mudanças culturais, tecnológicas, sociais, políticas, ecológicas, econômicas, entre outros elementos. Esses fatores são dinâmicos e, portanto, as organizações que trabalham nesses ambientes de incerteza se ajustam internamente ao longo do tempo para obterem os melhores resultados. Assim, tanto os processos quanto os arranjos institucionais precisam ser adaptados e até mesmo descartados para que a organização se mantenha atualizada. O setor financeiro é um bom exemplo de adaptação de processos às novas tecnologias e mudanças culturais.

> "[...] devido ao nível em que alguns itens são abordados no questionário do TCU, não é possível coletar de forma objetiva as possíveis características da empresa avaliada, uma vez que os questionamentos podem influenciar as respostas de forma

> padronizada devido a possíveis receios dos respondentes de estarem em desacordo com as premissas avaliadas pelo TCU" (SP11).

Nesse item supracitado, o sujeito da pesquisa apresenta uma importante questão em relação a papéis e responsabilidades. Ele não tem relação direta com a opção entre uma das duas perspectivas da governança de TI, mas põe em dúvida os resultados obtidos pelo índice de governança de TI. Isto porque o TCU é um órgão de assessoria do legislativo e parece assumir a função de direcionamento da governança, quando evoca para si que os questionários são indutores da governança, quando esta é uma atribuição do executivo que dispõe de um comitê com tais atribuições, o CGI (Comitê de Governança Institucional).

Esta ação pode gerar, para os agentes da burocracia, uma confusão sobre a verdadeira motivação dos levantamentos, como se apresenta no texto do sujeito pesquisado 11, acima.

Em uma outra citação o sujeito da pesquisa 1 afirma que “O índice de terceirização empresa B (infra) é bem maior, o que ficou público nos escândalos envolvendo o ex-VP de TI (SP1). Este achado se refere a questão de número sete. Com o objetivo de capturar mais informações sobre os fatores que impactam a governança, a questão de número sete solicita para que o sujeito da pesquisa faça a comparação com outra empresa da mesma área e pergunta qual das duas empresas apresenta melhor governança e pede para justificar. Em relação à resposta, foi considerado como achado a questão envolvendo escândalo público, decorrente de assédio moral.

Alguns dos valores das boas práticas da governança pública dizem respeito à valorização e proteção contra o assédio moral nas empresas públicas. "O VP foi denunciado pela imprensa e pediu a demissão. Entretanto, a empresa apresentou grande crescimento do indicador de governança de TI no período. O indicador usado pelo TCU é sensibilizado pela existência da comissão de ética e não pela ocorrência de assédio."

> [...] adotar uma abordagem mais ampla e integrada para a governança de TI como estratégia, arquitetura, segurança,

conformidade, entre outros, devendo ser vista como um processo contínuo de melhoria (SP2).

Estes itens citados, arquitetura, segurança, estratégia etc., fazem parte dos arranjos de TI. Conforme descrito por Weill & Ross, os arranjos de TI das empresas que apresentam maiores lucros estão orientados aos seus resultados, mas geralmente são arranjos diferentes, pois estão inseridos em ambientes e contextos diferentes.

"Honestamente discordo. A empresa vem de um crescimento exponencial, gerando grandes resultados" (SP8).

A citação acima se refere a questão de número oito, na qual foi perguntado se o sujeito da pesquisa concorda com o resultado apresentado no Quadro 1, onde o indicador do TCU apresentou uma redução no indicador da governança de TI da empresa na qual ele trabalha, e solicita uma justificativa para a resposta apresentada. Para o sujeito SP8, a queda não faz sentido, pois os resultados da empresa vêm crescendo. "Honestamente discordo. A empresa vem de um crescimento exponencial, gerando grandes resultados" SP8. Este é um enfoque importante no que tange ao comportamento dos resultados da empresa em questão em relação aos indicadores da governança. A empresa "A" vem apresentando seguidos aumentos nos resultados financeiros, está entre os 10 maiores ROE (retorno sobre o patrimônio líquido) do mundo em sua área de atuação e recentemente alcançou papel de destaque no Brasil em decorrência do seu resultado, mas seus indicadores de governança de TI caíram.

Neste contexto, o que mais chama a atenção é que os indicadores são usados exatamente para medir os resultados financeiros em organizações corporativas e, neste caso, quando comparado ao resultado financeiro, o indicador não seguiu essa tendência, não sendo capaz de capturar aquilo que deveria ser sua característica mais forte, uma vez que sua origem nos remete a este objetivo em governança corporativa.

Em relação aos fatores que estão ligados a esta perspectiva, os que mais se destacaram foram: Política (34); Cultura e Comportamento Organizacional (15); Entidades Reguladoras (9); Conhecimento (7); Fatores psicossociais do trabalho (7) e Tecnologia (5), conforme Quadro 5.

Dessa forma, podemos concluir que os fatores políticos apresentaram forte influência, com inúmeras citações. As várias trocas

de governo, com consequente troca de gestão na administração da empresa, podem ter colaborado para evidenciar a relevância deste fator.

Avaliando os dados, podemos identificar que a empresa sofre impactos de condições políticas e que esse fator não é identificado pelos indicadores prescricionais. Além disso, conforme Dye (2013, p.3), políticas públicas não são representadas exclusivamente pelas ações que o governo decide tomar, mas também por aquelas ações que o governo decide não fazer. Retomando o que foi dito pelo sujeito de pesquisa SP7, "Penso que a política demonstrada pelo Governo Federal não priorizava a governança de um modo geral. Isso refletiu em todos os níveis com o consequente relaxamento em função de outras prioridades". Pode-se perceber que algumas políticas públicas não são facilmente identificáveis e provocam impacto nas organizações. Além disso, a política pública é "Um conjunto de decisões inter-relacionadas - tomadas por um ator ou grupo de atores políticos - que se referem à seleção de objetivos e dos meios necessários para alcançá-los [...]" (JENKINS apud HOWLLET et al.., 2014, p. 3). Nesse caso, os agentes públicos são parte integrante dos meios necessários e, como tal, podem se apropriar da implantação da política, o que é de difícil identificação.

Acerca desse assunto, pode-se observar o que foi respondido por um dos sujeitos pesquisados: "[...] existe uma diferença entre normatização de processos e a sua plena execução" (SP1). Desse achado, observa-se que o sujeito de pesquisa número um afirmou que, apesar de normatizado, o processo pode não ser executado. Para que isso ocorra, entende-se que o agente público se apropria do processo e o adapta, fazendo os ajustes que considera importantes para o processo. Pode-se também observar a influência de outros fatores, como Cultura e Comportamento Organizacional (15), Entidades Reguladoras (9), Conhecimento (7), Fatores psicossociais do trabalho (7) e Tecnologia (5), entre outros. Ressalte-se ainda que, pela teoria da contingência (MORESI, 2001), a estrutura e o comportamento organizacional são variáveis dependentes, e que as variáveis independentes são o ambiente e a tecnologia. Dessa forma, o comportamento organizacional pode ser impactado por outras variáveis, o que torna o modelo de captura ainda mais complexo.

4.3. CONSIDERAÇÕES SOBRE OS RESULTADOS

A questão norteadora deste estudo surge do entendimento das perspectivas de governança de TI, levando em consideração o trabalho do TCU para acompanhar a governança nas estatais. Se, por um lado, a perspectiva prescritiva formal da governança traz uma forma simples de acompanhamento, por outro lado não há evidências empíricas de que ela represente os processos que determinam a governança de TI e seja capaz de mensurá-los. Da mesma forma, não foram encontradas evidências sobre a validação empírica do questionário do TCU ou sua assertividade após algumas observações.

As análises numéricas dos dados obtidos fornecem uma visão inicial da tendência de como os gestores percebem a governança e a tratam de maneira prática e diária, como uma ferramenta para alcançar os resultados esperados. Por outro lado, durante a análise de conteúdo das justificativas dos gestores, as informações textuais convergem para o fato de que os questionários do TCU não são capazes de capturar o resultado da governança de TI, e elencam vários fatores que tais questionários não capturam e apontam a influência de diversas condições como: políticas, econômicas, aspectos temporais, comportamento organizacional, entidades reguladoras, relacionamento com os clientes, tecnologia, estratégia adotada e influência decorrente da pandemia, entre outros. Esses fatores podem ser influenciados a qualquer momento e passar por mudanças, tornando-os também de difícil mensuração. Ou seja, na visão dos gestores além de os indicadores existentes no formulário do TCU não apontarem fatores que dependem da dinâmica relacional de fatores externos, alguns dos indicadores apurados não são capazes de capturar aquilo a que o próprio indicador se propõe.

Dentro da teoria da contingência, em um contexto organizacional, os princípios de administração não são universais, e, portanto, não existe uma única maneira das empresas se organizarem (MORESI, 2001, p. 65), o que gera arranjos diferentes. Conforme essa teoria, a organização é um sistema aberto, sendo a estrutura e o comportamento organizacional variáveis dependentes, enquanto o ambiente e a tecnologia são variáveis independentes.

Fica claro, portanto, que essas variáveis, estrutura e comportamento, sofrem a influência do ambiente e da tecnologia. Assim, é de se supor que tanto as estruturas quanto os processos "envelheçam", como mencionado pelo sujeito da pesquisa SP10. Também se presume que as estruturas sofram mudanças, resultando em novos arranjos de TI, como observado e caracterizado na resposta

do sujeito SP2, que menciona as mudanças na arquitetura da segurança e nas estratégias como parte dos arranjos da governança de TI, conforme citado anteriormente por Weill & Ross.

Além disso, em um dos comentários dos gestores, fica evidente que se esperava que os índices de governança capturados pelos questionários do TCU, por terem sua origem no ambiente corporativo, apresentassem indicadores compatíveis com os resultados da empresa, o que não ocorreu. A empresa, cujos gestores foram alvo da pesquisa, registrou um crescimento de 3% em seu indicador entre 2017 e 2018, seguido de uma redução de 5,4% entre 2018 e 2021. No entanto, ao observar seu resultado em 2022, pode-se constatar que ela se destacou no mercado brasileiro e internacional, sendo classificada entre os 10 maiores ROE (retorno sobre o patrimônio) do mundo em seu setor de atuação.

É importante ressaltar, entretanto, que esse achado, embora relevante, requer estudos futuros mais específicos que possibilitem comparar como os índices de TI e o índice geral de governança da empresa se comportam em relação aos resultados financeiros apresentados, além disso a análise de conteúdo que se propõe a identificar e separar as perspectivas da governança da TI na visão dos gestores é uma primeira tentativa de fazer um estudo qualitativo e embora o resultado tenha se apresentado próximo dos valores obtidos do conteúdo manifesto, é importante aprimorar este debate no que tange a como separar tais indicadores em relação às perspectivas da governança, analítica e prescritivo-formal, o que pode ser alvo de novos trabalhos.

Este estudo está limitado a um estudo de caso em uma organização, e é necessário ter cautela em relação às conclusões apresentadas aqui. No entanto, segundo Yin, "Os estudos de caso não são generalizáveis para a população (generalização estatística); no entanto, eles podem ser utilizados para expandir e generalizar teorias (generalização analítica)" (2015, p. 22).

Das respostas dos questionários, por meio da análise de conteúdo, conclui-se que os indicadores prescritivos formais, usados pelo questionário do TCU, não são capazes de capturar características inerentes ao ambiente externo ou interno. As organizações sofrem influências externas, internas e temporais provenientes de diversos contextos, conforme a tabela de fatores levantados e definidos como unidade de contexto (Anexo 2). Esses fatores são difíceis de mensurar,

uma vez que estão relacionados ao comportamento e à natureza humana, possuem características temporais e apresentam variáveis dependentes, como no caso da estrutura e do comportamento organizacional, conforme a *Teoria de Contingência* de Lawrence & Lorsh (apud Moresi, 2001).

As estruturas das organizações sofrem mudanças, assim como seus arranjos, e seus processos "envelhecem" devido a fatores externos à organização, tornando-se impraticável acompanhá-los como é feito em uma governança corporativa. Além disso, uma vez que os indicadores prescritivos formais são definidos e acompanhados para compreender a evolução da empresa, não é possível realizar mudanças frequentes neles, caso contrário, estaríamos comparando informações diferentes. Por outro lado, como mencionado anteriormente, a organização está em um sistema aberto e é influenciada e se adapta aos fatores mencionados. Além disso, cada empresa possui uma história diferente, com estratégias e arranjos distintos. Conforme mencionado anteriormente, há um grande risco de medir conteúdos desiguais com a mesma ferramenta, o que pode levar a resultados inesperados e, na melhor das hipóteses, não permitir comparação, mesmo entre empresas do mesmo setor de atuação.

A governança, assim como os princípios de administração, não são tão simples de serem avaliados e definidos por modelos devido à subjetividade e às relações de interdependência que a envolve em um ambiente complexo. Dentro desse contexto, as áreas de TI, assim como as áreas de processos de negócio das APF, se organizam em arranjos que dependem de diversos fatores, como, por exemplo, as estratégias determinadas pelo ambiente em que a organização está inserida. Por essa razão, as empresas apresentam arranjos e processos diferentes, desenvolvidos para atender a essas características. Portanto, é de se esperar que os resultados de um formulário como o do TCU, elaborado com indicadores prescritivos formais, mesmo para empresas de TI do mesmo setor de atuação, apresentem resultados diferentes. De forma ainda mais complexa, as empresas de TI que atuam em áreas diferentes, como saúde e finanças, apresentam arranjos ainda mais diversos devido à natureza do negócio. É pouco provável que os mesmos questionários permitam uma avaliação com os mesmos indicadores, pois essas empresas possuem, como já mencionado, arranjos e processos distintos.

Um outro aspecto que chamou a atenção neste trabalho é o fato de o TCU, um órgão de assessoria ao legislativo com funções e

prerrogativas de fiscalização, estar envolvido na atividade de levantamento de informações e indução de melhorias na governança, conforme já apresentado anteriormente. Se, por um lado, observa-se a preocupação do TCU com a melhoria da governança, por outro lado verifica-se uma disfunção que pode influenciar as respostas e, consequentemente, aumentar o risco de desvio nos resultados dos índices de governança obtidos. Isso ocorre porque o papel do TCU é de assessoria ao legislativo, com foco na fiscalização, e não um órgão de gestão que faça parte do poder executivo.

Dessa forma, é possível notar que um dos resultados foi o questionamento, pelo sujeito pesquisado, do risco de as pessoas responderem ao questionário, entendendo que podem não estar de acordo com certas expectativas legais. Conforme trecho a seguir do SP11: "[...] tendo em vista que os questionamentos podem levar a respostas padronizadas devido a possíveis receios de que os respondentes não estejam em conformidade com as premissas avaliadas pelo TCU".

4.4. CONSIDERAÇÕES FINAIS

Esta dissertação tomou como referência a experiência de gestores de TI de uma empresa estatal considerada pelo mercado como exemplo de governança pública e que apresenta resultados compatíveis com essa visão de mercado. Este item de considerações finais completa a abordagem deste trabalho a partir dos objetivos apresentados e dos resultados alcançados, trazendo informações sobre as contribuições para a academia e para a APF, ao mesmo tempo em que aborda suas limitações e sugestões para estudos futuros.

O objetivo geral deste trabalho foi definido como fazer um estudo exploratório dos fatores que influenciam a governança de TI, tomando como referência a opinião dos gestores que utilizam os questionários com os indicadores de governança de TI do TCU, e explorar a relação desses fatores identificados com a perspectivas da governança de TI, como fator secundário.

Com base no estudo exploratório e nas respostas dos gestores de TI, foram identificados os fatores conforme constam no quadro 6. Para cada unidade de registro, pelo menos uma referência foi encontrada. Dentre as unidades de contexto, os fatores mais

mencionados estão listados no quadro 5. Com base nesses resultados, é possível concluir que, para os gestores, há uma grande interferência política que afeta a governança de TI em uma empresa pública e que não é capturada pelos indicadores prescritivos.

Matus (1997) alerta que os métodos de planejamento utilizados pelas empresas privadas não são adequados para o setor público, devido às suas diferentes vocações e valores. Ele destaca também a crença de alguns de que a solução consiste em transplantar o estilo de gestão do setor privado para o setor público, o que é difundido pelas escolas de planejamento tradicional de cunho "gerencialista". Matus argumenta que se o problema fosse de fácil solução, já teria sido resolvido, especialmente porque na América Latina as soluções de planejamento e gestão são imitadas com atraso. Para ele, os métodos de planejamento e gestão usados pelas organizações corporativas são inadequados para o setor público, pois possuem diferentes vocações e valores. Nesse caso, a cultura organizacional não evolui apenas com o uso de instrumentos que se baseiam em uma racionalidade instrumental (MATUS, apud SILVA et al., 2017).

Da mesma forma, ao analisarmos os resultados do levantamento de fatores que impactam a governança de TI em uma empresa pública, é possível argumentar que o raciocínio descrito por Matus para o Planejamento Estratégico Situacional (PES) e gestão se confirma, com base nos resultados, para a governança de TI em uma empresa pública. Isso se justifica, uma vez que o planejamento estratégico é dinâmico e dependente do contexto, sendo um componente da governança pública quando analisada sob a perspectiva analítica. A partir dos objetivos específicos estabelecidos no trabalho, segue-se a definição e conquista dos mesmos. "Identificar se, na visão dos gestores de TI entrevistados, o questionário do TCU, por meio de seus indicadores, é suficiente para capturar os processos que representam os resultados da governança de TI".

Com base nos resultados obtidos, a maioria dos gestores entrevistados indicou que o questionário do TCU não é suficiente para capturar os processos que representam os resultados da governança de TI. Para essa conclusão, foram obtidos três resultados da pesquisa. O primeiro resultado foi obtido a partir de uma pergunta de pesquisa espontânea, na qual questionou-se se o formulário é suficiente para capturar esses resultados. Nesse caso, 64% dos respondentes entendem que os indicadores utilizados pelo TCU não representam os processos da governança, enquanto 36% acreditam que os indicadores

prescritivos representam os processos da governança de TI. Em outros dois resultados, quando a pergunta foi feita de forma estimulada e quando foi realizada a análise de conteúdo das respostas dos gestores, obteve-se resultados ainda mais expressivos, com 86% no primeiro caso e 83% na análise de conteúdo.

No âmbito do seguinte objetivo: "Investigar quais outros fatores, na percepção dos sujeitos da pesquisa, os indicadores prescricionais utilizados pelo formulário do TCU não conseguem capturar", foram identificados 15 diferentes fatores, conforme apresentado no anexo 3, e duas respostas inespecíficas que mencionaram exclusivamente fatores externos e internos.

No item dedicado a "realizar revisão da literatura, seus estudos teóricos e metodológicos, sobre os conceitos utilizados, definições adotadas e dados coletados", essa revisão está presente no capítulo 2, embora esse objetivo tenha sido parcialmente prejudicado devido à escassez de trabalhos que abordem a governança de TI em uma perspectiva dinâmica. O objetivo era "investigar e tentar relacionar as descobertas encontradas na pesquisa com as perspectivas de governança de TI".

Em relação a esse objetivo, foram identificados vários achados, alguns dos quais relacionados especificamente à perspectiva da governança, conforme análise dos resultados das questões no capítulo 4, seções 4.1 e 4.2, classificados em relação às perspectivas da governança como perspectiva prescritiva e perspectiva analítica. Este trabalho apresenta algumas contribuições ao inserir a visão de administradores de TI de uma empresa de grande porte, altamente conceituada no mercado por sua excelência em governança, incluindo a governança de TI. Além disso, traz para o debate uma perspectiva diferente desses gestores em relação ao objeto da pesquisa.

Como resultado do estudo de caso, percebe-se que os indicadores prescritivos formais da "boa governança", adotados pelo TCU, não apresentam resultados satisfatórios na área de TI e alerta-se para o risco de os questionários obterem resultados enviesados, uma vez que são elaborados e acompanhados por uma área responsável pela fiscalização contábil. Se por um lado o desenho que define indicadores de TI do TCU em seus questionários não conseguem avaliar a governança de TI por outro lado também há fatores que impactam esta governança e cuja influência deve ser medida de forma analítica e estão vinculados a fatores externos como o ambiente e a interação da

empresa com este ambiente não sendo capturados por sua natureza por fatores prescritivos formais. Por ser um estudo de caso, seus resultados devem ser considerados com cautela, mas oferece, circunstancialmente, um elemento adicional para o debate acadêmico. Por outro lado, esse debate traz a APF para discussão, uma vez que ela é uma parte interessada no trabalho em prol da melhoria da governança pública do país.

Foram identificadas as seguintes limitações: (i) a escassez de documentos e estudos que debatam a governança de TI sob a ótica de uma governança analítica; (ii) dificuldades inerentes ao levantamento das informações dos questionários, por envolver gestores que fazem parte da cúpula decisória da TI da empresa e, por fim, (iii) o momento específico vivido pela gestão das APF, com a transição de um governo para outro. Isso resulta do processo democrático de alternância de governos e, principalmente, devido a uma troca de poder dentro da empresa onde os gestores pesquisados atuam.

Durante o período da pesquisa, foi possível observar as interferências sofridas por essas empresas decorrentes da instabilidade da alternância de poderes. Existe um momento de instabilidade resultante das mudanças de gestores, que gera incertezas e uma inércia natural, em consequência da mudança na alta administração e da nova direção dada à empresa pelo governo que assume o poder. Essa questão limitou o trabalho a um número menor de gestores, uma vez que alguns não estavam disponíveis para responder o questionário da pesquisa devido a reuniões com a nova administração e com suas próprias equipes, buscando reduzir o número de boatos que geralmente ocorrem durante essas mudanças, especialmente em Brasília, devido à sua proximidade com o governo central. Como resultado dessas dificuldades, houve um aumento no tempo previsto para receber as respostas, o que dificultou uma possível expansão da pesquisa.

Como é característico de estudos de caso, há uma limitação em relação à generalização estatística da pesquisa. Entretanto, de acordo com Yin, conforme mencionado anteriormente, “Os estudos de caso não são generalizáveis para a população (generalização estatística); no entanto, eles podem ser usados para expandir e generalizar teorias (generalização analítica)” (2015, p. 22).

A área de governança pública de TI apresenta escassez de trabalhos que discutam a governança da TI em empresas públicas sob

a perspectiva de uma governança analítica. Essa perspectiva busca identificar, de forma dinâmica, os fatores ambientais que requerem monitoramento contínuo e suas influências na governança, permitindo que os gestores obtenham informações para acompanhar e tomar decisões visando melhorar a governança em suas respectivas áreas de atuação, incluindo a governança de TI.

Para trabalhos futuros que abordem o mesmo tema e visem uma ampliação estatística dos resultados, sugere-se expandir o levantamento para outras empresas estatais, ampliando assim o escopo da pesquisa. Além disso, propõe-se um estudo comparativo entre os índices de governança de empresas estatais com fins lucrativos e os resultados financeiros por elas apresentados, a fim de verificar se os comportamentos dos indicadores estão relacionados aos resultados alcançados.

Também seria possível realizar comparações com outras empresas estatais com fins lucrativos para avaliar a precisão da ferramenta definida pelo TCU e se o formulário pode ser utilizado para comparação e promoção da governança nas empresas estatais. Nesse sentido, não é necessário comparar empresas do mesmo setor, uma vez que os questionários são os mesmos, independentemente da área de atuação. Portanto, é possível comparar o índice de uma empresa de geração de energia com o de uma instituição financeira ou uma empresa de exploração e distribuição de combustível.

Por fim, entende-se que este trabalho representa uma pequena contribuição para o debate e para a Administração Pública Federal em um tema cujos estudos são relativamente novos, os conceitos ainda não estão consolidados e há uma grande carência e importância de pesquisa nessa área.

REFERÊNCIAS

REFERÊNCIAS

REFERÊNCIAS

ALTOUNIAN, Cláudio S.; DE SOUZA, Daniel L.; LAPA, Leonard Renne G. **Gestão e governança pública para resultados: uma visão prática**. Belo Horizonte: Fórum, 2020.

APAZA, Carmen R. Measuring Governance and Corruption through the Worldwide Governance Indicators: Critiques, Responses, and Ongoing Scholarly Discussion. **PS: Political Science & Politics**, v. 42, n. 1, p. 139-143, 2009.

CAVALCANTE, Pedro Luiz C.; PIRES, Roberto R. C. Apresentação: Variedades de governança pública**. Boletim de Análise Político-Institucional (BAPI),** n. 19, dez. 2018.

CARROLL, Toby et al. **Studies in the Political Economy of Public Policy.** London: Palgrave Macmillan, 2014.

CONTI, José Mauricio. **Levando o direito financeiro a sério**. São Paulo: Editora Blucher, 2016.

DYE, Thomas R. **Understanding public policy.** New Jersey: Prentice Hall, 2013.

FUKUYAMA, Francis. What is governance? *Governance* - **An International Journal of Policy, Administration, and Institutions**, v. 26, n. 3, p. 347-368, 2013.

HARDY, G. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. **Information Security technical report,** p. 55-61, March 2006.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. Um estudo empírico do impacto da governança de TI no desempenho organizacional. **Produção,** 22 (3), 612-624. 2012.

MAGALHÃES, Marcos Thadeu Queiroz. "Metodologia para desenvolvimento de sistemas de indicadores: uma aplicação no planejamento e gestão da política nacional de transportes." *Publicação T. DM-015A/2004*, **Dissertação de Mestrado, Departamento de Engenharia Civil e Ambiental, Faculdade de Tecnologia, Universidade de Brasília (2004).**

MARTINS, Humberto Falcão; MARINI, Caio. Governança pública contemporânea: uma tentativa de dissecação conceitual. **Revista do TCU**, n. 130, p. 42-53, 2014.

PETERSON, R. Integration strategies and tactics for information technology governance. *In*: VAN GREMBERGEN, W. **Strategies for information technology governance**. Hershey: Idea group publishing, 2004.

POLLITT, Christopher; BOUCKAERT, Geert. La reforma de la gestión pública: Un análisis comparado. Madrid: Instituto Nacional de Admnistración Pública, 2010.

SALVADOR, Evilasio; TEIXEIRA, Sandra O. Orçamento e políticas sociais: metodologia de análise na perspectiva crítica. **Revista de Políticas Públicas**, v. 18, n. 1, p. 15-32, 2014.

SILVA, Mauro Santos; SCHMIDT, Flávia de Holanda; KLIASS, Paulo (Orgs.). **Empresas estatais: políticas públicas, governança e desempenho**. Brasília: Ipea, 2019.

VERGARA, Sylvia Constant. **Projetos e Relatórios de Pesquisa em Administração**. São Paulo: Editora Atlas, 2ª. Edição, 1998.

WEILL, Peter; ROSS, Jeanne W**. Governança de TI-tecnologia da informação**. São Paulo: M. Books, 2020.

HOWLETT, M. et al. **Política pública: seus ciclos e subsistemas.** Rio de Janeiro, 2013. Elsevier.

SACCOL, Amarolinda Zanela. Um retorno ao básico: compreendendo os paradigmas de pesquisa e sua aplicação na pesquisa em administração. **Revista de Administração da UFSM**, v. 2, n. 2, p. 250-269, 2009.

YIN, Robert K. **Estudo de caso: planejamento e métodos**. Porto Alegre: Bookman editora, 2015.

Sites:

VALOR ONLINE. Dos dez mais rentáveis bancos do mundo, 4 são brasileiros. Valor online, 18 abr. 2022. Disponível em:

<https://g1.globo.com/economia/noticia/2022/04/18/dos-10-bancos-mais-rentaveis-do-mundo-4-sao-brasileiros.ghtml>. Acesso em: 20 abr. 2023.

TRIBUNAL DE CONTAS DA UNIÃO. Governança de TI. Disponível em: <https://portal.tcu.gov.br/governanca/governanca-de-ti/>. Acesso em: 11 dez. 2022.

TRIBUNAL DE CONTAS DA UNIÃO. Levantamento de governança. Disponível em: <https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento>. Acesso em: 20 ago. 2021.

OECD. Diretrizes da OCDE sobre governança corporativa de empresas estatais (Edição 2015). Disponível em:

<https://read.oecd-ilibrary.org/governance/diretrizes-da-ocde-sobre-governanca-corporativa-de-empresas-estatais-edicao-2015_9789264181106-pt>. Acesso em: 24 abr. 2023.

TRIBUNAL DE CONTAS DA UNIÃO. Referencial básico governança, 1ª edição [Arquivo PDF]. Disponível em:

<https://portal.tcu.gov.br/data/files/6A/B6/39/85/1CD4671023455957E18818A8/Referencial_basico_governanca_1_edicao.PDF>. Acesso em: 02 mai. 2023.

APÊNDICES

APÊNDICES

APÊNDICE

APÊNDICE A – Análise exploratória dos dados

UMA ANÁLISE EXPLORATÓRIA DOS DADOS DO TCU

Durante o levantamento inicial dos dados, foram abordados os primeiros estudos exploratórios. Foram elaborados quadros resumos dos resultados dos indicadores e de análise de evolução dos mesmos que estão apresentados nos quadros: Quadro-1 e Quadro-2, para a empresa “B” e nos quadros: Quadro-3 e Quadro 4 para a Empresa “A”. Em uma análise inicial pode-se observar que a Empresa “B” apresentou uma redução no indicador da “boa governança” de TI de aproximadamente 9,4%, pelos indicadores do TCU, entre os anos de 2017 a 2018 e um forte crescimento de aproximadamente 22,6% na “boa governança” de TI no período compreendido entre 2018 e 2021. Em outra medida a empresa “A”, que apresentou entre os períodos de 2017 e 2018 valores de crescimento de aproximadamente 3,225%, no indicador da “boa governança” de TI, valor consideravelmente alto quando se observa que ele já ocupava índice de governança acima de 93%, tendo atingido o patamar de 96% em 2018. No entanto, a variação entre os períodos de 2018 e 2021 de “A”, nos apresenta um alerta, pois o mesmo apresentou um recrudescimento de aproximadamente 5,63%, baixando seu indicador de “boa governança” de TI para o patamar de 90,6%.

Durante o levantamento inicial dos dados, foram abordados os primeiros estudos exploratórios. Foram elaborados quadros resumos dos resultados dos indicadores e de análise de evolução dos mesmos que estão apresentados nos quadros: Quadro-1 e Quadro-2, para “B” e nos quadros: Quadro-3 e Quadro 4 para o Banco do Brasil. Em uma análise inicial pode-se observar que “B” apresentou uma redução no indicador da “boa governança” de TI de aproximadamente 9,4%, pelos indicadores do TCU, entre os anos de 2017 a 2018 e um forte crescimento de aproximadamente 22,6% na “boa governança” de TI no período compreendido entre 2018 e 2021. Em outra medida “A”, que apresentou entre os períodos de 2017 e 2018 valores de crescimento de aproximadamente 3,225%, no indicador da “boa governança” de TI, valor consideravelmente alto quando se observa que ele já ocupava índice de governança acima de 93%, tendo atingido o patamar de 96% em 2018. No entanto, a variação entre os períodos de 2018 e 2021 de ”A”, nos apresenta um alerta, pois o mesmo mostrou um recrudescimento de

aproximadamente 5,63%, baixando seu indicador de “boa governança” de TI para o patamar de 90,6%

APÊNDICE B – Formulário da pesquisa

FORMULÁRIO DE PESQUISA. QUESTÕES ELABORADAS

Este formulário se destina a pesquisa acadêmica para composição de dissertação de mestrado em Governança Pública. Tem como objetivo contribuir com os trabalhos de Governança em TI e colaborar para o debate, conhecimentos sobre o assunto e ajudar na evolução da Governança das empresas estatais do Brasil. Todo o desenvolvimento primará por respeitar questões éticas envolvidas em pesquisas científicas, portanto, o sigilo será mantido de forma a preservar a identificação dos colaboradores. Agradeço por sua participação, ela será de grande contribuição para a evolução deste debate. Caso tenha interesse pelo resultado final da pesquisa ou necessitar contatar com o pesquisador, por favor encaminhe e-mail para Fernando H. S. Santos: fernandohs_santos@hotmail.com.

Instruções para as respostas:

O tempo médio previsto para responder esta pesquisa é de 15 minutos. (10 Questões + informação do e-mail).

Preencha todo o formulário exclusivamente embasado em sua experiência, procurando ser fiel à realidade e sempre que possível exemplifique situações identificadas em sua prática.

Não existe resposta certa ou errada o importante para a pesquisa é a experiência vivenciada pelos gestores.

O formulário está dividido em 3 seções. Antes de passar para a seção 2 assegure-se de haver fechado as questões da seção 1 e da mesma forma proceda para a seção 3. Apesar do retorno entre seções estar liberado não se deve retornar a seções anteriores.

Governança de TI - Pesquisa Empresa A

Seção: indicadores prescricionais e a "boa governança de TI"

Questão 1 – Cargo ocupado pelo entrevistado na TI:

Múltipla escolha: 3 opções

Questão 2 – Tempo no cargo/função. Múltipla escolha: 3 opções

Questão 3 – Em relação ao questionário do TCU sobre governança de TI

Múltipla escolha: 3 opções

Questão 4 – Você entende que o questionário do TCU, por intermédio dos seus indicadores, é suficiente para capturar os processos que representam os resultados da governança de TI? Caso você não conheça o questionário do TCU use como referência um modelo de avaliação de governança TI conhecido, informando a referência para esta questão e para a questão 6.

Explique em que se baseia esta sua concordância ou discordância.

Questão 5 – Em sua avaliação existem fatores que são capazes de influenciar o resultado da boa governança de TI, de forma positiva ou negativa e que não podem ser representados ou mensurados por indicadores?

Explique em que está embasada sua resposta e se for o caso indique quais fatores, na sua visão, impactam a Governança de TI que dificilmente poderão ser identificados por indicadores.

Questão 6 – Na sua opinião os indicadores de governança de TI do TCU capturam a influência de fatores internos ou mesmo externos vinculados a: Troca de governo? Da administração da gestão da própria empresa, inclusive TI? Mudanças de políticas públicas, inclusive políticas salariais e de privatizações? Fatores temporais ou outros fatores não citados?

Explique em que se baseia sua opinião e dê exemplos.

Questão 07 – Esta pesquisa contempla as empresas A e B. Pautado em sua experiência, considerando-se um contexto de colaboração entre as duas empresas, qual delas, de um modo geral, possui a Governança de TI mais evoluída? Explique em que se baseia sua opinião e se possível cite exemplos.

Seção: Seção 2 - Quadro do TCU em relação a sua empresa. (A)

Questão 08 – Observe o quadro 1 abaixo (Empresa A):

Considere a variação do índice de governança de TI entre 2017 e 2018 e entre 2018 e 2021. Você concorda que os resultados acima refletem as mudanças da governança de TI de sua empresa? Explique, tomando como base sua experiência, porque e quais os fatores que refletiram nas variações entre os períodos apresentados.

Quadro 1 – Empresa A

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	93	96	90,6

Fonte: elaborado pelo autor com base em dados do TCU (2021).

Seção: Seção 3 - Quadro do TCU - Resultado de Governança - Comparativo A e B.

Questão 09 – Considere os quadros abaixo:

Na sua opinião quais fatores explicam melhor os diferentes comportamentos (Queda no índice de governança da empresa B e aumento do índice de Governança da empresa" A" - entre 2017 e 2018 e aumento do índice de Governança da B e queda do índice de governança da empresa "A" no período compreendido entre 2018 e 2021). Você concorda que os índices acima, quadro 1 e 2, refletem a variação da melhoria da governança de TI das empresas. Justifique.

Quadro 1 – Indicadores de governança de TI da empresa "A" entre 2017-2021

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	93	96	90,6

Fonte: elaborado pelo autor com base em dados do TCU (2021).

Quadro 2 - Indicadores de governança de TI empresa "B" entre 2017 e 2021

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	85	77	94.4

Fonte: elaborado pelo autor com base em dados do TCU (2021).

Questão 10 - Há mais algum item, sobre o assunto, que gostaria de comentar, incluir ou complementar?

Texto de resposta longa

APÊNDICE C – Quadro Análise de conteúdo categorial – Uma proposta inicial para classificação.

Quadro 5 – Fatores utilizados para classificar a perspectiva da governança

Perspectiva da Governança Analítica			Perspectiva prescritivo formal "boa governança"		
Fatores externos	Fatores internos	Fatores temporais	Representa o processo	Prescritiva/ Normativa	Mensurável
Ambiente	Cultura organizacional	Decorre da passagem do tempo	Variáveis estão representadas	Independe da empresa	Pode ser medida
Condições Legal	Comportamento organizacional	Mudam com o tempo	permite comparar	Controle do desempenho	consegue quantificar
Condições Políticas	conhecimento	Necessário acompanhamento permanente	processo captura todos os fatores		consegue avaliar.
Condições Econômicas	liderança	desatualizam-se com o tempo			consegue avaliar
Condições demográficas	Psicossociais do trabalho	influenciado pela história da empresa			
Condições Sociais	Arranjo da organização				
Condições Culturais	Arranjo da TI				
Condições Ecológicas,					
Condições Tecnológicas					
Concorrentes					
Fornecedores					
Cliente					
Entidades Reguladoras					

Inter-relação com outros órgãos					
*Pandemias consideradas como condições ecológicas.					

APÊNDICE D – Os 15 principais fatores apontados pelos gestores

Detalhamento dos fatores apontados pelos gestores que em sua suas opiniões os indicadores prescritivos não conseguem capturar.

Relação dos 15 principais fatores apontados pelos Gestores que não são capturados por indicadores prescricionais da "Boa governança"
Políticos
Cultura e comportamento Organizacional
Influência de entidades reguladoras
Conhecimento
Fatores psicossociais do trabalho
Tecnologia
Comportamento organizacional
Relação com os Clientes
Arranjos de TI
Fatores Econômicos
Questões legais
Estratégia
Liderança
Temporalidade
Pandemia (considerada como Ecologia)

ANEXO A – Questionário de "iGovTI" – TCU (2021)

4200. Gestão de tecnologia da informação e da segurança da informação

4210. Realizar planejamento de tecnologia da informação

4211. A organização executa processo de planejamento de tecnologia da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) as áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação
- ☐ b) o processo de planejamento de TI integra-se e harmoniza-se com o processo de planejamento institucional

- c) a organização estabeleceu critérios para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) e os mantêm atualizados

- d) análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações)

- e) o processo de planejamento de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de planejamento de TI e promove eventuais ajustes necessários

- Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Planejamento de Tecnologia da

Informação; Plano de Tecnologia da Informação; Projeto; Risco; TI (Tecnologia da Informação).

4212. A organização possui plano de tecnologia da informação vigente

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o plano de tecnologia da informação (plano de TI) é aprovado pelo dirigente máximo da organização ou por dirigente ou colegiado que integra a alta administração
- ☐ b) o plano de TI é publicado na internet, para fácil acesso de partes interessadas e da sociedade

- c) o plano de TI fundamenta a proposta orçamentária da área de TI e o plano de contratações

- d) as iniciativas de TI (projetos e ações) constantes do plano de TI alinham-se aos objetivos e iniciativas definidos no plano estratégico e demais planos institucionais, assim como, quando aplicável, às estratégias e objetivos estabelecidos por instâncias de governança superiores (p. ex. Estratégia de Governança Digital - EGD, Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD)

- e) a seleção de iniciativas de TI (projetos e ações) para compor o plano de TI considera estimativas fundamentadas em dados históricos ou em estudos técnicos sobre a capacidade e a disponibilidade dos recursos de TI da organização (financeiros, humanos, materiais, equipamentos etc.)

- f) ao elaborar o Plano de TI, a organização avalia iniciativas estratégicas que têm por objetivo ampliar ou melhorar o uso de TI como instrumento de transformação do negócio em benefício da sociedade (transformação digital), especialmente quanto aos riscos de adoção, adoção tardia ou não adoção de tais iniciativas

- g) é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Conselho ou Colegiado Superior / instância superior; Dirigente máximo; Partes interessadas; Planejamento de Tecnologia da Informação; Plano de Tecnologia da

Informação; Projeto; TI (Tecnologia da Informação); Transformação Digital.

4220. Gerir serviços de tecnologia da informação

4221. A organização elabora um catálogo de serviços de tecnologia da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o catálogo contém as metas definidas para cada serviço (p. ex. prazos de entrega, horários de serviço e de suporte,

bem como pontos de contato para solicitação do serviço, envio de sugestões, esclarecimento de dúvidas e reporte de incidentes)

- b) o catálogo está atualizado e as informações que nele constam são compatíveis com os Acordos de Níveis de

Serviço (ANS) estabelecidos pela área de tecnologia da informação e as áreas de negócio da organização

- c) o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Serviço de TI; TI (Tecnologia da Informação); Usuário.

4222. A organização executa processo de gestão de mudanças

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) a organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais)

- b) mudanças são previamente comunicadas a todas as partes que possam ser afetadas

- c) identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados

- d) a realização de cada mudança é precedida de planejamento e testes

- e) mudanças executadas são rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes

- f) lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki)

- g) o processo de gestão de mudanças está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- h) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Efetividade;

Gestão de serviços de tecnologia da informação; Processo de gestão de mudanças.

4223. A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles
- ☐ b) a base de dados de configurações permite à organização conhecer o histórico da situação dos serviços e ativos de TI e do relacionamento entre eles ao longo do tempo

- c) a base de dados de configurações é mantida atualizada
- d) a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças
- e) o processo de gestão de configuração e ativos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação;

Processo de gerenciamento de configuração e ativos; Serviço de TI; TI (Tecnologia da Informação).

4224. A organização executa processo de gestão de incidentes de serviços de tecnologia da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização definiu regras para a priorização e o escalamento de incidentes
- ☐ b) a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes

- c) bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes

- d) o processo de gestão de incidentes está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de

incidentes de serviços de tecnologia da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação; Serviço de TI; TI (Tecnologia da Informação).

4230. Gerir nível de serviço de tecnologia da informação

4231. A área de gestão de tecnologia da informação acorda os níveis de serviço com as demais áreas de negócio internas à organização (Acordo de Nível de Serviço - ANS)

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) os ANS estabelecem metas de nível de serviço acordadas com representantes das áreas de negócio clientes
- b) os ANS são submetidos a revisões regulares, para assegurar que estejam atualizados e sejam efetivos
- c) os ANS estabelecidos na organização são formalizados
- d) a área de gestão de tecnologia da informação monitora continuamente o alcance dos níveis de serviço que foram definidos com as áreas de negócio clientes
- e) a área de gestão de tecnologia da informação comunica às áreas de negócio o resultado do monitoramento do alcance dos níveis de serviço
- f) a organização comunica aos usuários o resultado do monitoramento do alcance dos níveis de serviço

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Área de gestão de

tecnologia da informação; Área de negócio; Meta; TI (Tecnologia da Informação); Usuário.

4240. Gerir riscos de tecnologia da informação

4241. A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização identifica e avalia os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio

- b) a organização trata os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio, com base em um plano de tratamento de risco

- c) a organização atribuiu a responsabilidade por coordenar a gestão de riscos de tecnologia da informação

- d) o processo de gestão dos riscos de tecnologia da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de tecnologia da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Estabelecer; Gestão de riscos;

Gestão do desempenho; Identificação de riscos; Risco de Tecnologia da Informação; TI (Tecnologia da Informação); Tratamento de risco.

4242. A organização executa processo de gestão de continuidade de serviços de tecnologia da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização elabora um plano de continuidade de serviços de TI

☐ b) as ações e os prazos definidos no plano de continuidade de serviços de TI fundamentam-se em análises de

impacto no negócio realizadas sobre os processos organizacionais críticos

- c) o plano de continuidade de serviços de TI é testado e revisado periodicamente

- d) o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio

- e) o processo de gestão de continuidade de serviços de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de continuidade de serviços de TI e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de impacto no negócio; Gestão de

continuidade do negócio; Gestão do desempenho; Plano de continuidade do negócio; Serviço de TI.

4250. Definir políticas de responsabilidades para a gestão da segurança da informação

4251. A organização dispõe de uma política de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos,

estruturas e responsabilidades relativos à segurança da informação

- b) a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação

- c) a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação

- d) a política é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes

- e) a política é mantida atualizada, por meio de revisões periódicas

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Colaboradores; Diretriz; Gestão

de riscos; Informação; Política; Política de segurança da informação; Risco de Segurança da Informação; Segurança da Informação.

4252. A organização dispõe de comitê de segurança da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo

☐ b) o comitê formula diretrizes para a segurança da informação

- c) o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação

- d) o comitê é composto por representantes de áreas relevantes da organização

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Comitê de segurança da informação; Diretriz; Informação; Segurança da Informação.

4253. A organização possui um gestor institucional de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) o gestor institucional de segurança da informação foi designado formalmente pela alta administração
- b) o gestor institucional de segurança da informação reporta-se diretamente à alta administração
- c) o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional
- d) o gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional
- e) o gestor institucional de segurança da informação fomenta e coordena ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores
- f) o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Competências; Gestão de riscos; Gestor institucional de segurança da informação; Informação;

Partes interessadas; Risco de Segurança da Informação; Segurança da Informação.

4260. Estabelecer processos e atividades para a gestão da segurança da informação

4261. A organização executa processo de gestão de riscos de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização identifica e avalia riscos de segurança da informação
- ☐ b) a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos

- c) a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação

- d) o processo de gestão de riscos de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Gestão de riscos; Gestão do desempenho; Gestor; Identificação de riscos; Informação; Risco de

Segurança da Informação; Segurança da Informação; Serviço de TI; Tratamento de risco.

4262. A organização executa processo de controle de acesso à informação e aos ativos associados à informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização implementa controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das

informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio

- b) os controles de acesso implementados na organização aplicam o princípio “necessidade de conhecer”, o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio “privilégio mínimo”, o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades

- c) há controles de acesso lógicos na organização que utilizam autenticação com certificado digital ICP-Brasil, a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais

- d) a organização analisa criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos

- e) a organização instituiu uma Política de Controle de Acesso (PCA), a qual estabelece princípios, objetivos, diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de controle de acesso e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Certificado digital;

Controle; Diretriz; Gestão do desempenho; Informação; Política; Serviço de TI.

4263. A organização executa processo de gestão de ativos associados à informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização mantém um inventário dos ativos associados à informação
- ☐ b) a organização definiu responsabilidades pelos ativos associados à informação
- ☐ c) o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem

- d) o processo de gestão de ativos associados à informação subsidia a implantação de controles e ações com vistas a assegurar a adequada proteção dos ativos e das informações que armazenam, processam ou transmitem

- e) o processo de gestão de ativos associados à informação subsidia a implantação de ações mitigatórias aplicáveis no caso de ocorrência de evento catastrófico que inviabilize a utilização de ativos

- f) o processo de gestão de ativos associados à informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- g) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos

associados à informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Gestão do desempenho; Informação; Processo de gestão de ativos.

4264. A organização executa processo para classificação e tratamento de informações

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- b) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “a” em conformidade com os requisitos legais e de negócio

- c) informações sigilosas em razão de sua imprescindibilidade à segurança da sociedade ou do Estado são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- d) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “c” em conformidade com os requisitos legais e de negócio

- e) informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- f) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “e” em conformidade com os requisitos legais e de negócio

- g) informações críticas para a organização em razão de necessidades do negócio (p. ex. requisitos associados à integridade, disponibilidade, autenticidade ou a outros atributos da informação) são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- h) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “g” em conformidade com os requisitos legais e de negócio

- i) o processo de classificação e tratamento de informações está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- j) a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e

tratamento de informações e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão do desempenho; Informação; Processo para classificação e tratamento de informações.

4265. A organização executa processo de gestão de incidentes de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização definiu e comunica amplamente o ponto de contato a ser notificado no caso de ocorrência de

incidente de segurança da informação, bem como os canais de comunicação apropriados

- b) a organização definiu procedimentos e responsabilidades quanto ao tratamento das notificações de incidentes de segurança da informação, adoção de ações emergenciais e diretrizes para escalamento e comunicação interna e externa

- c) a organização definiu procedimentos e responsabilidades quanto à análise de incidentes de segurança da informação, identificação de causas raízes e planejamento e implementação de ações corretivas

- d) a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente

- e) o processo de gestão de incidentes de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de

incidentes de segurança da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão do desempenho; Informação; Processo de gestão de incidentes; Segurança da Informação.

4266. A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização gerencia (inventaria e controla) os dispositivos conectados em sua rede

- b) a organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conectados em sua rede

- c) a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio

- d) a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio

- e) a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio

- f) a organização aplica controles compensatórios para o uso de privilégios administrativos em seus ativos de software, de hardware e de rede críticos para o negócio

- g) a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing)

- h) a organização limita e controla o uso de portas, protocolos e serviços de rede nas conexões de sua rede interna com a internet e outras redes externas

- i) a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas

- j) a organização implementa cópias regulares de segurança (backup) das informações em meio digital, conforme

as melhores práticas e as necessidades de negócio, incluindo a realização periódica de testes de recuperação das informações

- k) a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração)

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Informação; Segurança dos recursos de processamento da informação.

4270. Executar processo de software

4271. A organização executa um processo de software

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) a organização possui pessoal próprio capacitado para gerir o processo de software

- b) a organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo “construir ou adquirir”)

- c) na etapa de planejamento das contratações de soluções de software, a organização realiza estudos para identificar e mitigar o risco de dependência tecnológica, com vistas a viabilizar a substituição de fabricante/fornecedor quando tecnicamente viável e economicamente vantajoso

- d) a organização utiliza prioritariamente arquiteturas de software que promovem o desacoplamento de soluções, sistemas e componentes, inclusive nos casos de software adquirido e desenvolvimento realizado mediante contratação, com vistas a facilitar a realização de manutenções e otimizar custos

- e) o processo de software utilizado pela organização promove a participação de representante da área de negócio como integrante da equipe de desenvolvimento ou aquisição de software, desde sua concepção até a aceitação final

- f) o processo de software da organização promove a identificação precoce de requisitos de segurança da informação e a gestão permanente desses requisitos durante todo o ciclo de vida do software

- g) o processo de software da organização promove a identificação precoce de requisitos de interoperabilidade e a gestão permanente desses requisitos durante todo o ciclo de vida do software

- h) o processo de software da organização promove a identificação precoce de requisitos de acessibilidade e de

usabilidade, bem como a gestão permanente desses requisitos durante todo o ciclo de vida do software

- i) a organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação

- j) organização avalia, por meio de mensurações, indicadores e metas, a qualidade do software desenvolvido ou adquirido

- k) o processo de software está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- l) a organização avalia periodicamente o desempenho e a conformidade do processo de software e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área de negócio; Gestão do desempenho;

Identificação de riscos; Indicador; Meta; Mitigar risco; Processo de software; Segurança da Informação.

4280. Gerir projetos de tecnologia da informação

4281. A organização executa processo de gestão de projetos de tecnologia da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização possui base de dados consolidada (portfólio) de projetos de tecnologia da informação

☐ b) escopo, custos, uso de recursos e cumprimento de prazos são gerenciados em cada projeto

- c) é realizada a gestão de riscos de cada um dos projetos de alta materialidade ou alta relevância

- d) o processo de gestão de projetos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de projetos de tecnologia da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de riscos; Gestão do desempenho; Portfólio de projetos de tecnologia da informação; Proj

UMA ANÁLISE EXPLORATÓRIA DOS DADOS DO TCU

Durante o levantamento inicial dos dados, foram abordados os primeiros estudos exploratórios. Foram elaborados quadros resumos dos resultados dos indicadores e de análise de evolução dos mesmos que estão apresentados nos quadros: Quadro-1 e Quadro-2, para a empresa “B” e nos quadros: Quadro-3 e Quadro 4 para a Empresa “A”. Em uma análise inicial pode-se observar que a Empresa “B” apresentou uma redução no indicador da “boa governança” de TI de aproximadamente 9,4%, pelos indicadores do TCU, entre os anos de 2017 a 2018 e um forte crescimento de aproximadamente 22,6% na “boa governança” de TI no período compreendido entre 2018 e 2021. Em outra medida a empresa “A”, que apresentou entre os períodos de 2017 e 2018 valores de crescimento de aproximadamente 3,225%, no indicador da “boa governança” de TI, valor consideravelmente alto quando se observa que ele já ocupava índice de governança acima de 93%, tendo atingido o patamar de 96% em 2018. No entanto, a variação entre os períodos de 2018 e 2021 de “A”, nos apresenta um alerta, pois o mesmo apresentou um recrudescimento de aproximadamente 5,63%, baixando seu indicador de “boa governança” de TI para o patamar de 90,6%.

Durante o levantamento inicial dos dados, foram abordados os primeiros estudos exploratórios. Foram elaborados quadros resumos dos resultados dos indicadores e de análise de evolução dos mesmos que estão apresentados nos quadros: Quadro-1 e Quadro-2, para “B” e nos quadros: Quadro-3 e Quadro 4 para o Banco do Brasil. Em uma análise inicial pode-se observar que “B” apresentou uma redução no indicador da “boa governança” de TI de aproximadamente 9,4%, pelos indicadores do TCU, entre os anos de 2017 a 2018 e um forte crescimento de aproximadamente 22,6% na “boa governança” de TI no período compreendido entre 2018 e 2021. Em outra medida “A”, que apresentou entre os períodos de 2017 e 2018 valores de crescimento de aproximadamente 3,225%, no indicador da “boa governança” de TI, valor consideravelmente alto quando se observa que ele já ocupava índice de governança acima de 93%, tendo atingido o patamar de 96% em 2018. No entanto, a variação entre os períodos de 2018 e 2021 de ”A”, nos apresenta um alerta, pois o mesmo mostrou um recrudescimento de

aproximadamente 5,63%, baixando seu indicador de “boa governança” de TI para o patamar de 90,6%

APÊNDICE B – Formulário da pesquisa

FORMULÁRIO DE PESQUISA. QUESTÕES ELABORADAS

Este formulário se destina a pesquisa acadêmica para composição de dissertação de mestrado em Governança Pública. Tem como objetivo contribuir com os trabalhos de Governança em TI e colaborar para o debate, conhecimentos sobre o assunto e ajudar na evolução da Governança das empresas estatais do Brasil. Todo o desenvolvimento primará por respeitar questões éticas envolvidas em pesquisas científicas, portanto, o sigilo será mantido de forma a preservar a identificação dos colaboradores. Agradeço por sua participação, ela será de grande contribuição para a evolução deste debate. Caso tenha interesse pelo resultado final da pesquisa ou necessitar contatar com o pesquisador, por favor encaminhe e-mail para Fernando H. S. Santos: fernandohs_santos@hotmail.com.

Instruções para as respostas:

O tempo médio previsto para responder esta pesquisa é de 15 minutos. (10 Questões + informação do e-mail).

Preencha todo o formulário exclusivamente embasado em sua experiência, procurando ser fiel à realidade e sempre que possível exemplifique situações identificadas em sua prática.

Não existe resposta certa ou errada o importante para a pesquisa é a experiência vivenciada pelos gestores.

O formulário está dividido em 3 seções. Antes de passar para a seção 2 assegure-se de haver fechado as questões da seção 1 e da mesma forma proceda para a seção 3. Apesar do retorno entre seções estar liberado não se deve retornar a seções anteriores.

Governança de TI - Pesquisa Empresa A

Seção: indicadores prescricionais e a "boa governança de TI"

Questão 1 – Cargo ocupado pelo entrevistado na TI:

Múltipla escolha: 3 opções

Questão 2 – Tempo no cargo/função. Múltipla escolha: 3 opções

Questão 3 – Em relação ao questionário do TCU sobre governança de TI

Múltipla escolha: 3 opções

Questão 4 – Você entende que o questionário do TCU, por intermédio dos seus indicadores, é suficiente para capturar os processos que representam os resultados da governança de TI? Caso você não conheça o questionário do TCU use como referência um modelo de avaliação de governança TI conhecido, informando a referência para esta questão e para a questão 6.

Explique em que se baseia esta sua concordância ou discordância.

Questão 5 – Em sua avaliação existem fatores que são capazes de influenciar o resultado da boa governança de TI, de forma positiva ou negativa e que não podem ser representados ou mensurados por indicadores?

Explique em que está embasada sua resposta e se for o caso indique quais fatores, na sua visão, impactam a Governança de TI que dificilmente poderão ser identificados por indicadores.

Questão 6 – Na sua opinião os indicadores de governança de TI do TCU capturam a influência de fatores internos ou mesmo externos vinculados a: Troca de governo? Da administração da gestão da própria empresa, inclusive TI? Mudanças de políticas públicas, inclusive políticas salariais e de privatizações? Fatores temporais ou outros fatores não citados?

Explique em que se baseia sua opinião e dê exemplos.

Questão 07 – Esta pesquisa contempla as empresas A e B. Pautado em sua experiência, considerando-se um contexto de colaboração entre as duas empresas, qual delas, de um modo geral, possui a Governança de TI mais evoluída? Explique em que se baseia sua opinião e se possível cite exemplos.

Seção: Seção 2 - Quadro do TCU em relação a sua empresa. (A)

Questão 08 – Observe o quadro 1 abaixo (Empresa A):

Considere a variação do índice de governança de TI entre 2017 e 2018 e entre 2018 e 2021. Você concorda que os resultados acima

refletem as mudanças da governança de TI de sua empresa? Explique, tomando como base sua experiência, porque e quais os fatores que refletiram nas variações entre os períodos apresentados.

Quadro 1 – Empresa A

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	93	96	90,6

Fonte: elaborado pelo autor com base em dados do TCU (2021).

Seção: Seção 3 - Quadro do TCU - Resultado de Governança - Comparativo A e B.

Questão 09 – Considere os quadros abaixo:

Na sua opinião quais fatores explicam melhor os diferentes comportamentos (Queda no índice de governança da empresa B e aumento do índice de Governança da empresa" A" - entre 2017 e 2018 e aumento do índice de Governança da B e queda do índice de governança da empresa "A" no período compreendido entre 2018 e 2021). Você concorda que os índices acima, quadro 1 e 2, refletem a variação da melhoria da governança de TI das empresas. Justifique.

Quadro 1 – Indicadores de governança de TI da empresa "A" entre 2017-2021

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	93	96	90,6

Fonte: elaborado pelo autor com base em dados do TCU (2021).

Quadro 2 - Indicadores de governança de TI empresa "B" entre 2017 e 2021

Ano	2017	2018	2021
iGovTI (índice de governança e gestão de TI)	85	77	94.4

Fonte: elaborado pelo autor com base em dados do TCU (2021).

Questão 10 - Há mais algum item, sobre o assunto, que gostaria de comentar, incluir ou complementar?

Texto de resposta longa

APÊNDICE C – Quadro Análise de conteúdo categorial – Uma proposta inicial para classificação.

Quadro 5 – Fatores utilizados para classificar a perspectiva da governança

Perspectiva da Governança Analítica			**Perspectiva prescritivo formal "boa governança"**		
Fatores externos	Fatores internos	Fatores temporais	Representa o processo	Prescritiva/ Normativa	Mensurável
Ambiente	Cultura organizacional	Decorre da passagem do tempo	Variáveis estão representadas	Independe da empresa	Pode ser medida
Condições Legal	Comportamento organizacional	Mudam com o tempo	permite comparar	Controle do desempenho	consegue quantificar
Condições Políticas	conhecimento	Necessário acompanhamento permanente	processo captura todos os fatores		consegue avaliar.
Condições Econômicas	liderança	desatualizam-se com o tempo			consegue avaliar
Condições demográficas	Psicossociais do trabalho	influenciado pela história da empresa			
Condições Sociais	Arranjo da organização				
Condições Culturais	Arranjo da TI				
Condições Ecológicas,					
Condições Tecnológicas					
Concorrentes					
Fornecedores					
Cliente					
Entidades Reguladoras					
Inter-relação com outros órgãos					
*Pandemias consideradas como					

condições ecológicas.					

APÊNDICE D – OS 15 principais fatores apontados pelos gestores

Detalhamento dos fatores apontados pelos gestores que em sua suas opiniões os indicadores prescritivos não conseguem capturar.

Relação dos 15 principais fatores apontados pelos Gestores que não são capturados por indicadores prescricionais da "Boa governança"
Políticos
Cultura e comportamento Organizacional
Influência de entidades reguladoras
Conhecimento
Fatores psicossociais do trabalho
Tecnologia
Comportamento organizacional
Relação com os Clientes
Arranjos de TI
Fatores Econômicos
Questões legais
Estratégia
Liderança
Temporalidade
Pandemia (considerada como Ecologia)

ANEXO A – Questionário de “iGovTI” – TCU (2021)

4200. Gestão de tecnologia da informação e da segurança da informação

4210. Realizar planejamento de tecnologia da informação

4211. A organização executa processo de planejamento de tecnologia da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) as áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação
- ☐ b) o processo de planejamento de TI integra-se e harmoniza-se com o processo de planejamento institucional

- c) a organização estabeleceu critérios para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) e os mantêm atualizados

- d) análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações)

- e) o processo de planejamento de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de planejamento de TI e promove eventuais ajustes necessários

- Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Planejamento de Tecnologia da

Informação; Plano de Tecnologia da Informação; Projeto; Risco; TI (Tecnologia da Informação).

4212. A organização possui plano de tecnologia da informação vigente

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o plano de tecnologia da informação (plano de TI) é aprovado pelo dirigente máximo da organização ou por dirigente ou colegiado que integra a alta administração
- ☐ b) o plano de TI é publicado na internet, para fácil acesso de partes interessadas e da sociedade

- c) o plano de TI fundamenta a proposta orçamentária da área de TI e o plano de contratações

- d) as iniciativas de TI (projetos e ações) constantes do plano de TI alinham-se aos objetivos e iniciativas definidos no plano estratégico e demais planos institucionais, assim como, quando aplicável, às estratégias e objetivos estabelecidos por instâncias de governança superiores (p. ex. Estratégia de Governança Digital - EGD, Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD)

- e) a seleção de iniciativas de TI (projetos e ações) para compor o plano de TI considera estimativas fundamentadas em dados históricos ou em estudos técnicos sobre a capacidade e a disponibilidade dos recursos de TI da organização (financeiros, humanos, materiais, equipamentos etc.)

- f) ao elaborar o Plano de TI, a organização avalia iniciativas estratégicas que têm por objetivo ampliar ou melhorar o uso de TI como instrumento de transformação do negócio em benefício da sociedade (transformação digital), especialmente quanto aos riscos de adoção, adoção tardia ou não adoção de tais iniciativas

- g) é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Conselho ou Colegiado Superior / instância superior; Dirigente máximo; Partes interessadas; Planejamento de Tecnologia da Informação; Plano de Tecnologia da

Informação; Projeto; TI (Tecnologia da Informação); Transformação Digital.

4220. Gerir serviços de tecnologia da informação

4221. A organização elabora um catálogo de serviços de tecnologia da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) o catálogo contém as metas definidas para cada serviço (p. ex. prazos de entrega, horários de serviço e de suporte,

bem como pontos de contato para solicitação do serviço, envio de sugestões, esclarecimento de dúvidas e reporte de incidentes)

- b) o catálogo está atualizado e as informações que nele constam são compatíveis com os Acordos de Níveis de

Serviço (ANS) estabelecidos pela área de tecnologia da informação e as áreas de negócio da organização

- c) o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Serviço de TI; TI (Tecnologia da Informação); Usuário.

4222. A organização executa processo de gestão de mudanças

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) a organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais)

- b) mudanças são previamente comunicadas a todas as partes que possam ser afetadas

- c) identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados

- d) a realização de cada mudança é precedida de planejamento e testes

- e) mudanças executadas são rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes

- f) lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki)

- g) o processo de gestão de mudanças está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- h) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Efetividade;

Gestão de serviços de tecnologia da informação; Processo de gestão de mudanças.

4223. A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles
- ☐ b) a base de dados de configurações permite à organização conhecer o histórico da situação dos serviços e ativos de TI e do relacionamento entre eles ao longo do tempo

- c) a base de dados de configurações é mantida atualizada

- d) a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças

- e) o processo de gestão de configuração e ativos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação;

Processo de gerenciamento de configuração e ativos; Serviço de TI; TI (Tecnologia da Informação).

4224. A organização executa processo de gestão de incidentes de serviços de tecnologia da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização definiu regras para a priorização e o escalamento de incidentes

☐ b) a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes

- c) bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes

- d) o processo de gestão de incidentes está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de

incidentes de serviços de tecnologia da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação; Serviço de TI; TI (Tecnologia da Informação).

4230. Gerir nível de serviço de tecnologia da informação

4231. A área de gestão de tecnologia da informação acorda os níveis de serviço com as demais áreas de negócio internas à organização (Acordo de Nível de Serviço - ANS)

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) os ANS estabelecem metas de nível de serviço acordadas com representantes das áreas de negócio clientes
- b) os ANS são submetidos a revisões regulares, para assegurar que estejam atualizados e sejam efetivos
- c) os ANS estabelecidos na organização são formalizados
- d) a área de gestão de tecnologia da informação monitora continuamente o alcance dos níveis de serviço que foram definidos com as áreas de negócio clientes
- e) a área de gestão de tecnologia da informação comunica às áreas de negócio o resultado do monitoramento do alcance dos níveis de serviço
- f) a organização comunica aos usuários o resultado do monitoramento do alcance dos níveis de serviço

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Área de gestão de

tecnologia da informação; Área de negócio; Meta; TI (Tecnologia da Informação); Usuário.

4240. Gerir riscos de tecnologia da informação

4241. A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização identifica e avalia os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio

- b) a organização trata os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio, com base em um plano de tratamento de risco

- c) a organização atribuiu a responsabilidade por coordenar a gestão de riscos de tecnologia da informação

- d) o processo de gestão dos riscos de tecnologia da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de tecnologia da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Estabelecer; Gestão de riscos;

Gestão do desempenho; Identificação de riscos; Risco de Tecnologia da Informação; TI (Tecnologia da Informação); Tratamento de risco.

4242. A organização executa processo de gestão de continuidade de serviços de tecnologia da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização elabora um plano de continuidade de serviços de TI

☐ b) as ações e os prazos definidos no plano de continuidade de serviços de TI fundamentam-se em análises de

impacto no negócio realizadas sobre os processos organizacionais críticos

- c) o plano de continuidade de serviços de TI é testado e revisado periodicamente

- d) o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio

- e) o processo de gestão de continuidade de serviços de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de continuidade de serviços de TI e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de impacto no negócio; Gestão de

continuidade do negócio; Gestão do desempenho; Plano de continuidade do negócio; Serviço de TI.

4250. Definir políticas de responsabilidades para a gestão da segurança da informação

4251. A organização dispõe de uma política de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos,

estruturas e responsabilidades relativos à segurança da informação

- b) a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação

- c) a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação

- d) a política é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes

- e) a política é mantida atualizada, por meio de revisões periódicas

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Colaboradores; Diretriz; Gestão

de riscos; Informação; Política; Política de segurança da informação; Risco de Segurança da Informação; Segurança da Informação.

4252. A organização dispõe de comitê de segurança da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo

☐ b) o comitê formula diretrizes para a segurança da informação

- c) o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação
- d) o comitê é composto por representantes de áreas relevantes da organização

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Comitê de segurança da informação; Diretriz; Informação; Segurança da Informação.

4253. A organização possui um gestor institucional de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) o gestor institucional de segurança da informação foi designado formalmente pela alta administração
- b) o gestor institucional de segurança da informação reporta-se diretamente à alta administração
- c) o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional
- d) o gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional
- e) o gestor institucional de segurança da informação fomenta e coordena ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores
- f) o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Competências; Gestão de riscos; Gestor institucional de segurança da informação; Informação;

Partes interessadas; Risco de Segurança da Informação; Segurança da Informação.

4260. Estabelecer processos e atividades para a gestão da segurança da informação

4261. A organização executa processo de gestão de riscos de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização identifica e avalia riscos de segurança da informação
- ☐ b) a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos

- c) a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação

- d) o processo de gestão de riscos de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Gestão de riscos; Gestão do desempenho; Gestor; Identificação de riscos; Informação; Risco de

Segurança da Informação; Segurança da Informação; Serviço de TI; Tratamento de risco.

4262. A organização executa processo de controle de acesso à informação e aos ativos associados à informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização implementa controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das

informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio

- b) os controles de acesso implementados na organização aplicam o princípio “necessidade de conhecer”, o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio “privilégio mínimo”, o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades

- c) há controles de acesso lógicos na organização que utilizam autenticação com certificado digital ICP-Brasil, a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais

- d) a organização analisa criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos

- e) a organização instituiu uma Política de Controle de Acesso (PCA), a qual estabelece princípios, objetivos, diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de controle de acesso e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Certificado digital;

Controle; Diretriz; Gestão do desempenho; Informação; Política; Serviço de TI.

4263. A organização executa processo de gestão de ativos associados à informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização mantém um inventário dos ativos associados à informação
- ☐ b) a organização definiu responsabilidades pelos ativos associados à informação
- ☐ c) o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem

- d) o processo de gestão de ativos associados à informação subsidia a implantação de controles e ações com vistas a assegurar a adequada proteção dos ativos e das informações que armazenam, processam ou transmitem

- e) o processo de gestão de ativos associados à informação subsidia a implantação de ações mitigatórias aplicáveis no caso de ocorrência de evento catastrófico que inviabilize a utilização de ativos

- f) o processo de gestão de ativos associados à informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- g) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos

associados à informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Gestão do desempenho; Informação; Processo de gestão de ativos.

4264. A organização executa processo para classificação e tratamento de informações

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- b) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “a” em conformidade com os requisitos legais e de negócio

- c) informações sigilosas em razão de sua imprescindibilidade à segurança da sociedade ou do Estado são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- d) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “c” em conformidade com os requisitos legais e de negócio

- e) informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- f) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “e” em conformidade com os requisitos legais e de negócio

- g) informações críticas para a organização em razão de necessidades do negócio (p. ex. requisitos associados à integridade, disponibilidade, autenticidade ou a outros atributos da informação) são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção

- h) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “g” em conformidade com os requisitos legais e de negócio

- i) o processo de classificação e tratamento de informações está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- j) a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e

tratamento de informações e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão do desempenho; Informação; Processo para classificação e tratamento de informações.

4265. A organização executa processo de gestão de incidentes de segurança da informação

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização definiu e comunica amplamente o ponto de contato a ser notificado no caso de ocorrência de

incidente de segurança da informação, bem como os canais de comunicação apropriados

- b) a organização definiu procedimentos e responsabilidades quanto ao tratamento das notificações de incidentes de segurança da informação, adoção de ações emergenciais e diretrizes para escalamento e comunicação interna e externa

- c) a organização definiu procedimentos e responsabilidades quanto à análise de incidentes de segurança da informação, identificação de causas raízes e planejamento e implementação de ações corretivas

- d) a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente

- e) o processo de gestão de incidentes de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de

incidentes de segurança da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão do desempenho; Informação; Processo de gestão de incidentes; Segurança da Informação.

4266. A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização gerencia (inventaria e controla) os dispositivos conectados em sua rede

- b) a organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conectados em sua rede

- c) a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio

- d) a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio

- e) a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio

- f) a organização aplica controles compensatórios para o uso de privilégios administrativos em seus ativos de software, de hardware e de rede críticos para o negócio

- g) a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing)

- h) a organização limita e controla o uso de portas, protocolos e serviços de rede nas conexões de sua rede interna com a internet e outras redes externas

- i) a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas

- j) a organização implementa cópias regulares de segurança (backup) das informações em meio digital, conforme

as melhores práticas e as necessidades de negócio, incluindo a realização periódica de testes de recuperação das informações

- k) a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração)

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Informação; Segurança dos recursos de processamento da informação.

4270. Executar processo de software

4271. A organização executa um processo de software

- ◯ Não adota
- ◯ Há decisão formal ou plano aprovado para adotá-lo
- ◯ Adota em menor parte
- ◯ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ◯ Não se aplica
- ◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
  - ➥ Indique que leis e/ou normas são essas:
- ◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
  - ➥ Identifique esses estudos:
- ◯ Não se aplica por outras razões.
  - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- a) a organização possui pessoal próprio capacitado para gerir o processo de software

- b) a organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo “construir ou adquirir”)

- c) na etapa de planejamento das contratações de soluções de software, a organização realiza estudos para identificar e mitigar o risco de dependência tecnológica, com vistas a viabilizar a substituição de fabricante/fornecedor quando tecnicamente viável e economicamente vantajoso

- d) a organização utiliza prioritariamente arquiteturas de software que promovem o desacoplamento de soluções, sistemas e componentes, inclusive nos casos de software adquirido e desenvolvimento realizado mediante contratação, com vistas a facilitar a realização de manutenções e otimizar custos

- e) o processo de software utilizado pela organização promove a participação de representante da área de negócio como integrante da equipe de desenvolvimento ou aquisição de software, desde sua concepção até a aceitação final

- f) o processo de software da organização promove a identificação precoce de requisitos de segurança da informação e a gestão permanente desses requisitos durante todo o ciclo de vida do software

- g) o processo de software da organização promove a identificação precoce de requisitos de interoperabilidade e a gestão permanente desses requisitos durante todo o ciclo de vida do software

- h) o processo de software da organização promove a identificação precoce de requisitos de acessibilidade e de

usabilidade, bem como a gestão permanente desses requisitos durante todo o ciclo de vida do software

- i) a organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação

- j) organização avalia, por meio de mensurações, indicadores e metas, a qualidade do software desenvolvido ou adquirido

- k) o processo de software está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- l) a organização avalia periodicamente o desempenho e a conformidade do processo de software e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área de negócio; Gestão do desempenho;

Identificação de riscos; Indicador; Meta; Mitigar risco; Processo de software; Segurança da Informação.

4280. Gerir projetos de tecnologia da informação

4281. A organização executa processo de gestão de projetos de tecnologia da informação

◯ Não adota

◯ Há decisão formal ou plano aprovado para adotá-lo

◯ Adota em menor parte

◯ Adota parcialmente

➥ Indique quais as evidências dessa adoção:

◯ Adota em maior parte ou totalmente

➥ Indique quais as evidências dessa adoção:

◯ Não se aplica

◯ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.

➥ Indique que leis e/ou normas são essas:

◯ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.

➥ Identifique esses estudos:

◯ Não se aplica por outras razões.

➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

☐ a) a organização possui base de dados consolidada (portfólio) de projetos de tecnologia da informação

☐ b) escopo, custos, uso de recursos e cumprimento de prazos são gerenciados em cada projeto

- c) é realizada a gestão de riscos de cada um dos projetos de alta materialidade ou alta relevância

- d) o processo de gestão de projetos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)

- e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de projetos de tecnologia da informação e promove eventuais ajustes necessários

Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de riscos; Gestão do desempenho; Portfólio de projetos de tecnologia da informação; Projeto; Risco; TI (Tecnologia da Informação).


idp
A ESCOLHA QUE
TRANSFORMA
O SEU CONHECIMENTO