TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

SECEX
SECRETARIA DE CONTROLE EXTERNO

Relatório de Levantamento

GOVERNANÇA DE TI

NA ADMINISTRAÇÃO PÚBLICA ESTADUAL

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

SECEX
SECRETARIA DE CONTROLE EXTERNO

AUDITORIA DE TI

RELATÓRIO DE LEVANTAMENTO

Governança de Tecnologia da Informação no âmbito da administração pública estadual

Natal/RN
2024

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

SECEX
SECRETARIA DE CONTROLE EXTERNO

AUDITORIA DE TI

RELATÓRIO DE LEVANTAMENTO - Governança de Tecnologia da Informação no âmbito da administração pública estadual

ATO ORIGINÁRIO	Plano de Fiscalização Anual 2023-2024; Decisão n. 478/2023-TC; Processo 000736/2023-TC; ID 4.00.2023.089.000.
ATO DE DESIGNAÇÃO	Portaria nº 093/2023 – SECEX/TCE/RN, publicada no Diário Eletrônico do dia 13 de novembro de 2023.
UNIDADE JURISDICIONADA	Unidades Gestoras da Administração direta e indireta da esfera estadual.
OBJETO DA FISCALIZAÇÃO	Situação da Governança de Tecnologia da Informação
OBJETIVO DA FISCALIZAÇÃO	Conhecer a situação atual da Governança de TI no âmbito das unidades gestoras da Administração direta e indireta da esfera estadual, bem como identificar os Sistemas de Informação em funcionamento considerados de maior relevância pelos jurisdicionados. As informações obtidas neste levantamento serão utilizadas como fonte de consulta no processo de planejamento de Auditorias de TI a serem realizadas pelo Tribunal, com intuito de aumentar a eficiência e eficácia de suas ações. Além disso, espera-se que a aplicação do questionário sirva como ferramenta de indução de melhorias na governança de TI na Administração Pública Estadual, consequentemente, sua modernização e aperfeiçoamento.
ÁREA	Tecnologia da Informação

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

SECEX
SECRETARIA DE CONTROLE EXTERNO

AUDITORIA DE TI

PERÍODO DE ABRANGÊNCIA	2023
EQUIPE	
Membros	Alexandre Luiz Galvão Damasceno, Auditor de Controle Externo, Matrícula nº 9.988-0. Eduardo Pereira Lima, Auditor de Controle Externo, Matrícula nº 9.874-4.
Coordenador	Marcelo Santos de Araújo, Auditor de Controle Externo, Matrícula nº 9.908-2.
Supervisor	Evandro Nunes Franco, Auditor de Controle Externo, Matrícula nº 9.917-1.
Gestor da Unidade Técnica	Cleyton Marcelo Medeiros Barbosa, Auditor de Controle Externo – Matrícula nº 9.983-0.

RESUMO

A adoção de boas práticas de Governança de Tecnologia de Informação (TI) é imprescindível para controlar e dirigir o uso da TI para que os seus resultados agreguem valor ao negócio da instituição, assegurando a correta aplicação dos recursos, gerenciando riscos e contribuindo para que a organização alcance os objetivos institucionais estabelecidos.

Levando em consideração a elevada importância do tema, o TCE/RN inseriu em seu Plano Anual de Fiscalização (PFA 2023-2024) uma ação fiscalizatória com o objetivo de conhecer a atual situação da Governança de TI no âmbito da Administração Pública Estadual (APE), bem como identificar os sistemas eletrônicos informacionais considerados de maior relevância ou essenciais para a APE.

Para tanto, fazendo uso do instrumento de fiscalização do tipo Levantamento, a equipe de auditoria disponibilizou, no período compreendido entre os dias 9 e 24 de novembro de 2023, por meio da ferramenta *LimeSurvey,* um questionário eletrônico aos 67 (sessenta e sete) jurisdicionados da esfera estadual, incluindo todos os poderes e órgãos autônomos. O aludido questionário foi desenvolvido utilizando como referências o Levantamento de Governança de TI e o Levantamento de Sistemas Críticos, ambos realizados pelo Tribunal de Contas da União no âmbito da esfera Federal, e o Índice Municipal de Governança de Tecnologia da Informação (i-Gov TI), componente do IEGM e concebido pela Rede Nacional de Indicadores Públicos (Rede INDICON).

Assim, para identificar a situação da Governança de TI, a equipe de auditoria buscou obter informações detalhadas associadas a nove macrotemas: Infraestrutura e Pessoal de TI; Planejamento de TI; Gestão de Serviços de TI; Gestão dos Níveis de Serviços Prestados de TI; Gestão dos Riscos de TI; Definição de políticas, processos e responsabilidades para a gestão da Segurança da Informação; Gestão de continuidade de serviços de tecnologia da informação; Processo de Software; e Gestão de Projetos de TI.

Além disso, foi solicitado aos gestores públicos que identificassem, no âmbito da respectiva pasta de atuação, os cinco sistemas eletrônicos informacionais considerados mais relevantes ou essenciais, assinalando as vulnerabilidades desses sistemas e os impactos que eles podem ocasionar em casos de falhas.

Dos 67 jurisdicionados envolvidos no levantamento, apenas 4 se mantiveram omissos e não submeteram as respostas requisitadas, quais sejam: Secretaria de Estado da Saúde Pública - SESAP, Companhia de Águas e Esgotos do RN - CAERN, Fundação Djalma Marinho - FDM e Hospital Regional Tarcísio Maia - HRTM.

Apesar dessas omissões, o levantamento alcançou o objetivo esperado e as informações obtidas a partir deste levantamento possibilitaram:

- A identificação da fragilidade da Governança de TI na grande maioria dos órgãos da APE, como também os pontos fortes a serem disseminados;
- A autoavaliação dos jurisdicionados sobre o tema, induzindo a implementação das boas práticas de Governança de TI na APE;
- A identificação e a classificação dos sistemas eletrônicos informacionais de maior importância e em funcionamento na APE;

Ademais, as informações coletadas passarão a compor o banco de dados do TCE/RN e serão utilizadas no processo de planejamento das ações fiscalizatórias a serem realizadas em PFAs futuros, aprimorando a estratégia de atuação da Corte de Contas na fiscalização dos recursos públicos empregados na área da Tecnologia da Informação.

SUMÁRIO

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ANSI	American National Standards Institute
ANSI/PMI	Instituto Nacional Americano de Padrões / Instituto de Gerenciamento de Projetos
APO	Alinhar, Planejar e Organizar
BI	Inteligência de Negócios
BIA	Business Impact Analysis
COBIT	Control Objectives for Information and related Technology
iGovTIC-JUD	Diagnóstico feito anualmente pelo Conselho Nacional de Justiça para mensurar o nível de maturidade dos órgãos submetidos ao seu controle administrativo e financeiro em iniciativas de tecnologia da informação e comunicação.
INTOSAI	Organização Internacional de Entidades Fiscalizadoras Superiores
ISO/PC	Padrão da Organização Internacional de Normalização preparada pelo “Project Committee”.
ISSAI	Normas Internacionais das Entidades Fiscalizadoras Superiores
ITIL	Information Technology Infrastructure Library
LGPD	Lei Geral de Proteção de Dados Pessoais Lei n° 13.709/2018
MCTI	Ministério da Ciência, Tecnologia e Inovações
MPSBR	Melhoria do Processo de Software Brasileiro - programa da Softex com apoio do Ministério da Ciência, Tecnologia e Inovações (MCTI).
NBASP	Normas Brasileiras de Auditoria do Setor Público
NBR ISO/IEC	Norma Brasileira baseada na Organização Internacional de Normalização junto com a International Electrotechnical Commission - organização que lidera a área eletrotécnica normativa.
PMBOK	Project Management Body of Knowledge - Guia de conceitos e ferramentas para descrever e fazer a gestão do “ciclo de vida” de um projeto.
SEFAZ/MT	Secretaria de Estado da Fazenda de Mato Grosso
SGSTI	Sistema de Gestão de Serviços de TI
SLA	Acordo de Nível de Serviço
TI	Tecnologia da Informação

1.INTRODUÇÃO

1.1.Deliberação que originou o trabalho

O Pleno do Tribunal de Contas do Estado do Rio Grande do Norte aprovou, nos termos prescritos na Resolução nº 017/2016–TCE, de 26 de julho de 2016, o Plano de Fiscalização Anual 2023-2024, por meio da Decisão n° 478/2023-TC, em sessão ordinária n° 00018, de 28 de março de 2023, fazendo constar ação fiscalizatória destinada à realização de Levantamento de Governança de Tecnologia da Informação no âmbito da administração pública estadual, identificada sob o n° ID 4.00.2023.089.000.

1.2.Objetivo e escopo

Busca-se por meio do instrumento de fiscalização Levantamento conhecer a situação atual da Governança de TI no âmbito das unidades gestoras da Administração direta e indireta da esfera estadual, bem como identificar os sistemas eletrônicos informacionais considerados de maior relevância pelos jurisdicionados envolvidos.

As informações obtidas neste levantamento serão utilizadas como fonte de consulta no processo de planejamento de Auditorias de TI a serem realizadas pelo Tribunal de Contas do Estado, com intuito de aumentar a eficiência e eficácia de suas ações. Além disso, espera-se que a aplicação do questionário sirva como ferramenta de indução de melhorias na Governança de TI na Administração Pública Estadual e, consequentemente, na sua modernização e aperfeiçoamento.

1.3.Metodologia e limitações

O presente levantamento foi conduzido com observância aos princípios e padrões estabelecidos pelo Tribunal de Contas do Estado do Rio Grande do Norte e em conformidade com as Normas de Auditoria do Setor Público – NBASP, adotadas por meio da Resolução nº 010/2020-TCE. O referido arcabouço normativo foi consolidado convergindo com as Normas Internacionais de Auditoria das Entidades Fiscalizadoras Superiores – ISSAI, emitidas pela Organização Internacional de Entidades Fiscalizadoras Superiores – INTOSAI.

A partir de estudos realizados sobre o tema da Governança de Tecnologia da Informação foram estabelecidas 9 questões na Matriz de Planejamento e Procedimentos. Para respondê-las foi desenvolvido um questionário eletrônico composto por 181 perguntas agrupadas em 17 grupos temáticos. O questionário foi elaborado utilizando a ferramenta eletrônica *LimeSurvey* e disponibilizado aos gestores de 67 órgãos da administração direta e indireta da esfera estadual, incluindo todos os poderes e órgãos autônomos, por meio de endereço eletrônico (*link*) acessível no Portal do Gestor, no período compreendido entre os dias 9 e 24 de novembro de 2023.

O referido questionário foi desenvolvido utilizando como referências o Levantamento de Governança de TI e o Levantamento de Sistemas Críticos, ambos realizados pelo Tribunal de Contas da União no âmbito da esfera Federal, e o Índice Municipal de Governança de Tecnologia da Informação (i-Gov TI), componente do IEGM e concebido pela Rede INDICON.

A aplicação do questionário pela equipe de auditoria contou com o apoio da Coordenadoria de Soluções Tecnológicas para o Controle Externo - COEX no processo de esclarecimento de dúvidas dos jurisdicionados, bem como na busca ativa por meio de contato telefônico com a finalidade de obter as respostas de 100% dos envolvidos. Todavia, mesmo com todos os esforços, quatro jurisdicionados se mantiveram omissos e não submeteram as informações requisitadas, quais sejam: Secretaria de Estado da Saúde Pública - SESAP, Companhia de Águas e Esgotos do RN - CAERN, Fundação Djalma Marinho - FDM e Hospital Regional Tarcísio Maia - HRTM.

Dentre os 63 jurisdicionados que responderam o questionário, 13[1] submeteram informações inconsistentes ou incompletas acerca dos sistemas informacionais relevantes, comprometendo, em parte, a identificação desses sistemas.

Importante se faz destacar que o tempo previsto para realização do trabalho, o volume de informações coletadas, e o tamanho da equipe constituída configuram limitações que impossibilitaram a validação das respostas submetidas pelos jurisdicionados, de modo que os dados possuem natureza declaratória. De todo modo, em questões específicas, foram solicitadas as documentações comprobatórias na busca pela informação fidedigna.

2. GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA ESTADUAL

2.1. Contextualização

A Governança de Tecnologia da Informação é um componente essencial em organizações de natureza pública ou privada. Há várias definições para o termo: a norma ABNT NBR ISO/IEC 38500 a define como o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Para a metodologia COBIT, Governança de TI é um conjunto de boas práticas e gestão de tecnologia da informação, em nível internacional, que tem como objetivo principal criar valor para a organização com base nas necessidades das partes interessadas em torno de três eixos: gestão de riscos, uso otimizado de recursos e entrega de benefícios. O Instituto de Governança de TI (IGTI) define o conceito como a responsabilidade da alta

[1] Agência Reguladora de Serviços Públicos do RN (ARSEP); Controladoria Geral do Estado (CONTROL); Diretoria de Saúde da Policia Militar (DSPM); Empresa Gestora de Ativos do RN (EMGERN); Hospital Regional Doutor Cleodon Carlos de Andrade (HCCA); Hospital Regional Nelson Inácio dos Santos (HRNIS); Instituto de Desenvolvimento Sustentável e Meio Ambiente do RN (IDEMA); Instituto de Pesos E Medidas do RN (IPEM); Procuradoria Geral de Justiça (PGJ); Secretaria de Estado da Agricultura, da Pecuária e da Pesca (SAPE); Secretaria de Estado do desenvolvimento Econômico (SEDEC); Secretaria de Estado das Mulheres, da Juventude, da Igualdade Racial e dos Direitos Humanos (SEMJIDH); Vice Governadoria (VICEGOV).

gestão de assegurar que os objetivos e estratégias de uma organização sejam alcançadas por meio de seus processos e estruturas concernentes à Tecnologia da Informação.

No âmbito do Controle Externo, o Ministro Aroldo Cedraz do Tribunal de Contas da União, em seu voto constante no Acórdão 2.308/2010 – Plenário, explica que a governança de tecnologia da informação:

> [...] é o conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de tecnologia da informação, de modo a assegurar, a um nível aceitável de risco, eficiente utilização de recursos, apoio aos processos da organização e alinhamento estratégico com objetivos desta última. Seu objetivo, pois, é garantir que o uso da TI agregue valor ao negócio da organização.

A importância do tema na gestão pública enseja ações fiscalizatórias em vários órgãos. Desde o ano de 2007 o Tribunal de Contas da União desenvolve trabalho de levantamento da Governança de TI em seus órgãos jurisdicionados por meio de questionários. A partir de 2017, o TCU unificou quatro levantamentos de governança (pessoas, TI, contratações e governança pública) realizados com foco nas organizações públicas e tornou o trabalho anual, público e parte integrante do processo de prestação de contas anuais. De modo análogo, o Conselho Nacional de Justiça realiza um diagnóstico anual para aferir a evolução da governança, gestão e infraestrutura de Tecnologia da Informação do Poder Judiciário. O resultado desse diagnóstico compõe o iGovTIC-JUD.

Em nível estadual alguns Tribunais de Contas empreenderam esforços semelhantes, entre os quais se destacam o TCE/PR e o TCE/MT. Em 2016, a Corte de Contas paranaense realizou um levantamento da governança de TI nos 399 municípios do seu estado por meio de questionário eletrônico. Em 2017 o Tribunal de Contas de Mato Grosso realizou uma auditoria operacional no tema de governança de tecnologia da informação na Secretaria de Estado de Fazenda do Mato Grosso. O relatório identificou pontos de melhoria e dele originaram-se recomendações para a SEFAZ/MT.

Conclui-se dos trabalhos mencionados que nem sempre as estratégias adotadas para a tecnologia da informação apresentam resultados satisfatórios no setor público. A falta de um planejamento estratégico de TI alinhado ao planejamento estratégico institucional, muitas vezes, geram produtos que não entregam os resultados que a instituição almeja.

Diante do exposto, é de fundamental importância que o Tribunal de Contas do Estado do Rio Grande do Norte conheça a realidade da Governança de Tecnologia da Informação dos seus jurisdicionados, bem como identifique as principais soluções tecnológicas atualmente implantadas nas instituições públicas, para nortear e aprimorar a sua estratégia de atuação na fiscalização dos recursos públicos empregados na área da Tecnologia da Informação.

Além disso, espera-se que o levantamento de informações sobre a Governança de TI também provoque um exercício de autoconhecimento por parte dos jurisdicionados e sirva como ferramenta de indução de melhorias nessa área, consequentemente, trazendo modernização e aperfeiçoamento para a administração pública estadual.

2.2.Situação Encontrada

2.2.1.Estrutura e pessoal da área de Tecnologia da Informação

O uso da tecnologia da informação faz parte da rotina diária de funcionamento de qualquer unidade administrativa pública, sendo indispensável para o alcance eficiente dos seus objetivos e metas institucionais. Nesse cenário, torna-se fundamental e indispensável que a organização possua, preferencialmente em sua estrutura organizacional, um departamento ou um grupo de técnicos estruturado, com mão de obra especializada e continuamente capacitada, que desenvolva atividades para possibilitar o bom funcionamento dos serviços e produtos tecnológicos (computadores, impressoras, intranet, Internet, softwares, rede etc.), bem como para auxiliar a administração no processo cíclico de melhoria contínua institucional, atendendo as demandas de tecnologia da informação e participando diretamente ou indiretamente dos projetos de aperfeiçoamento organizacional.

De acordo com o item 1.6.9 da ABNT ISSO/IEC 38500, gestão é “o sistema de controles e processos necessário para alcançar os objetivos estratégicos estabelecidos pela direção da organização”. Para tanto, além de possuir mão de obra especializada, é importante que a organização defina os papéis e responsabilidades da área de gestão da tecnologia da informação.

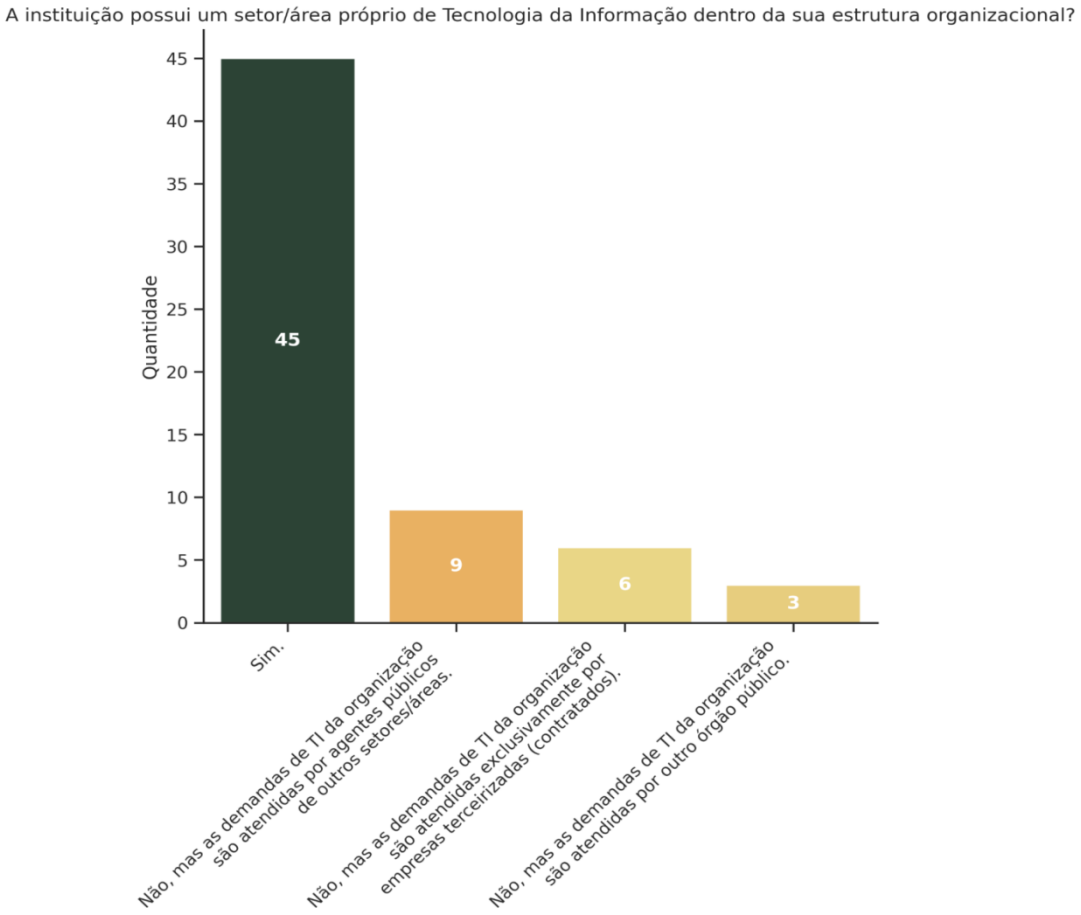
Considerando esses fatores, restou decidido pela equipe de auditoria que seria importante iniciar o levantamento buscando identificar se a organização possui estrutura e pessoal especializados em tecnologia da informação voltados para absorver as demandas de TI.

Sendo assim, foram requisitadas as seguintes informações:

- Departamento/Órgão que atende as demandas de Tecnologia da Informação da organização;
- Mão de obra especializada responsável pelas demandas de TI da organização;
- Definição das competências necessárias à execução das atividades de TI.

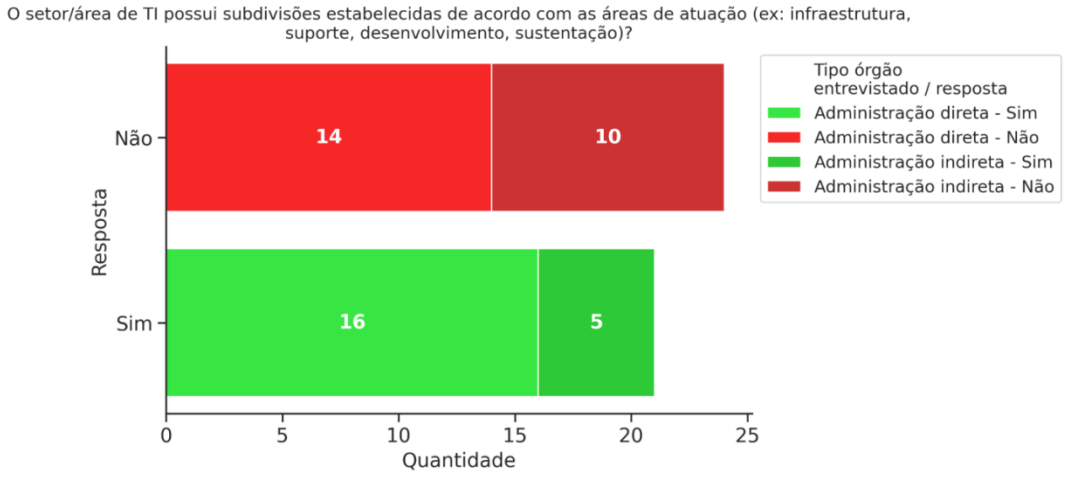
As respostas obtidas são apresentadas nas figuras 01, 02, 03 e 04.

Figura 1 - Departamento/Órgão que atende as demandas de TI da organização.



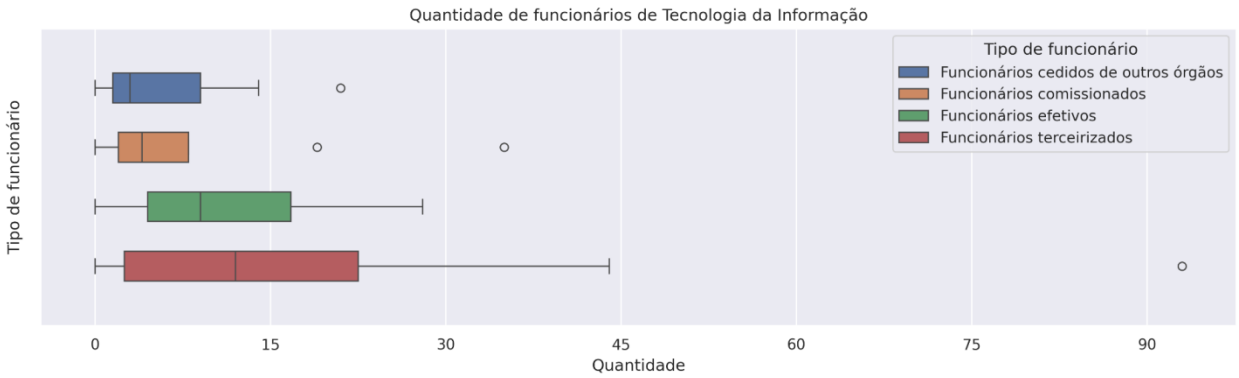
Na Figura 1 são apresentados os resultados de como os jurisdicionados estão estruturados para atender às suas próprias demandas de TI. A análise do referido gráfico permite identificar que 45 jurisdicionados (71% dos respondentes) declararam possuir um setor/departamento especializado em TI dentro de sua estrutura organizacional. No entanto, destaca-se o fato de 18 jurisdicionados (29%) não possuírem unidade setorial especializada em TI. Dentre estes, 9 utilizam agentes públicos lotados em outros setores para atender demandas de TI, 6 afirmaram que todas as demandas de TI são atendidas, exclusivamente, por prestadores de serviço terceirizados e 3 jurisdicionados informaram que as suas demandas de TI são atendidas por outro órgão da administração pública estadual.

Figura 2 - Subdivisões por área de atuação



Considerando apenas os jurisdicionados que possuem unidade setorial especializada em TI, observa-se no gráfico da Figura 2 que a maioria (24 jurisdicionados) não possui subdivisões estabelecidas de acordo com as áreas de atuação (ex: infraestrutura, suporte, desenvolvimento, sustentação). A falta de subdivisões por área de atuação não significa, necessariamente, ausência de segregação de atribuições na equipe que atua no departamento de TI, no entanto a direção e a coordenação de toda a equipe e de todas as atividades desenvolvidas pelo departamento ficam formalmente concentradas em uma única pessoa. Assim, a depender do tamanho da equipe e da quantidade de demandas existentes, essa concentração de responsabilidades pode dificultar a gestão e, consequentemente, o desempenho do setor.

Figura 3 - Mão de obra especializada

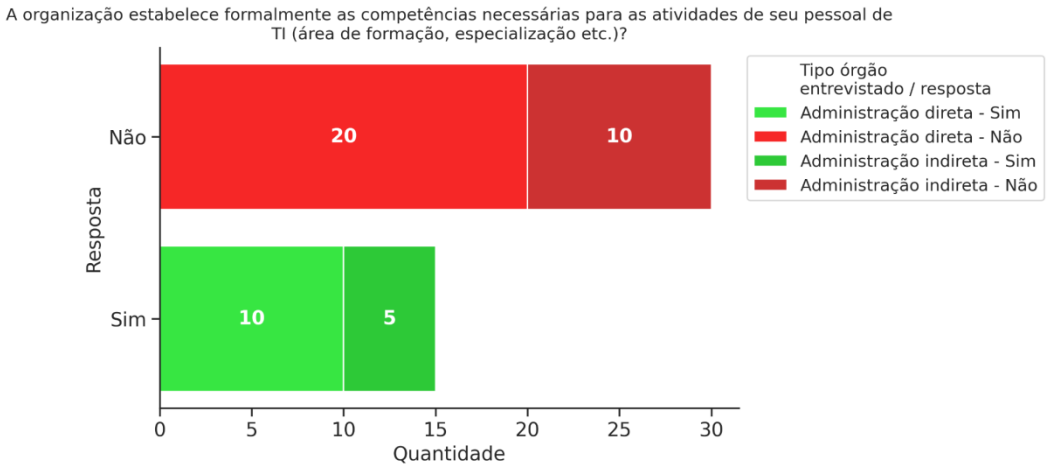


Uma vez identificados os jurisdicionados que possuem unidade setorial de TI em sua estrutura organizacional, foram solicitadas informações acerca do quantitativo de mão de obra existente, por tipo de vínculo profissional, no referido departamento.

O gráfico representado na Figura 3 demonstra, de forma consolidada, a distribuição de quantitativos de funcionários nos órgãos pesquisados. As informações, dispostas em forma de gráfico de caixa, destacam uma alta variância no tocante aos quantitativos de funcionários nos setores de Tecnologia da Informação. A média de terceirizados por setor é de 7,22 funcionários com um desvio padrão de 20,43 nessa distribuição de dados. À guisa de comparação, as mesmas estatísticas para funcionários efetivos são de 5,37 (média) e 7,96 (desvio padrão).

Fazendo-se uma análise conjunta da estrutura administrativa do setor de TI com o quantitativo de mão de obra alocada, o DETRAN e a PGE chamam a atenção por não possuírem subdivisões por área de atuação, ao mesmo tempo em que contam com um expressivo número de profissionais de TI (26 e 17 profissionais, respectivamente).

Figura 4 - Competências necessárias formalmente definidas



Por fim, buscou-se conhecer quais jurisdicionados definem formalmente as competências necessárias à execução das atividades TI. Assim, a partir da análise da Figura 4, conclui-se que, dentre os 45 jurisdicionados que possuem unidade organizacional especializada em TI, apenas 15 afirmaram definir formalmente essas competências. A ausência dessa definição por parte dos demais jurisdicionados figura como um ponto de atenção a ser observado, pois é requisito básico para elaboração de plano de capacitação voltado para o pessoal de TI.

2.2.2.Planejamento de Tecnologia da Informação

O planejamento de Tecnologia da Informação (TI) desempenha um papel crucial no funcionamento eficiente de organizações públicas, sendo um componente estratégico que impacta diretamente a capacidade do setor público em atender às demandas da sociedade de maneira eficaz e transparente. A importância do planejamento de TI para uma organização pública é evidenciada por vários fatores, elencados a seguir:

- Eficiência Operacional: o planejamento de TI permite a automação de processos e a implementação de sistemas integrados, resultando em uma melhoria significativa na

eficiência operacional. Isso reduz a burocracia, otimiza fluxos de trabalho e agiliza a prestação de serviços à população.

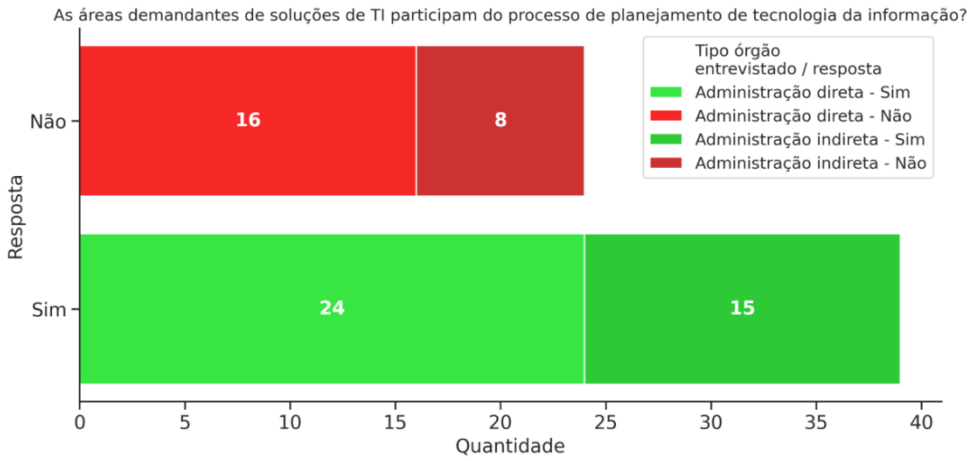
- Transparência e Prestação de Contas: sistemas de TI bem planejados facilitam a coleta, análise e relato de dados. Isso contribui para a transparência, pois informações sobre gastos, desempenho e resultados podem ser facilmente acessadas pelo público. Além disso, promove a prestação de contas, um princípio fundamental em organizações governamentais.
- Tomada de Decisão Embasada em Dados: o planejamento de TI fornece as ferramentas necessárias para coletar e analisar dados relevantes. Isso permite que os gestores tomem decisões informadas, baseadas em evidências, contribuindo para a eficácia das políticas públicas e alocando recursos de forma mais estratégica.
- Segurança da Informação: com ameaças digitais em constante evolução, a segurança da informação é vital. O planejamento de TI inclui estratégias para proteger dados sensíveis, garantindo a confidencialidade, integridade e disponibilidade das informações, essenciais para o bom funcionamento de órgãos governamentais.
- Integração e Colaboração: sistemas integrados de TI facilitam a colaboração entre diferentes setores e órgãos governamentais. Isso reduz a redundância, evita a duplicação de esforços e promove uma abordagem mais holística na prestação de serviços públicos.
- Adoção de Inovações Tecnológicas: o planejamento de TI permite que organizações públicas adotem inovações tecnológicas, como inteligência artificial, análise de big data e automação. Essas tecnologias podem revolucionar a forma como os serviços públicos são entregues, melhorando a experiência do cidadão e a eficácia das operações.
- Economia de Recursos: um planejamento eficiente de TI também contribui para a economia de recursos, garantindo que investimentos sejam feitos de forma estratégica e que os recursos disponíveis sejam utilizados da melhor maneira possível.

Em resumo, o planejamento de TI é essencial para o sucesso das organizações públicas, capacitando-as a enfrentar os desafios do mundo moderno, promovendo a transparência, eficiência operacional e a entrega eficaz de serviços públicos. O investimento contínuo nesse planejamento é crucial para garantir que as organizações estejam alinhadas com as demandas em constante evolução da sociedade.

Assim, o questionário elaborado busca também avaliar se as organizações envolvidas realizam planejamento de TI. Para iniciar essa análise, foram requisitadas informações dos jurisdicionados acerca: do processo de planejamento de Tecnologia da Informação, do Plano de TI vigente, e do orçamento da área de TI executado em 2023 e planejado para 2024.

As Figuras 5, 6 e 7 a seguir apresentam os resultados das questões exploratórias elaboradas para identificar o processo de Tecnologia da Informação existente nos jurisdicionados envolvidos.

Figura 5 - Áreas demandantes participam do planejamento de TI.

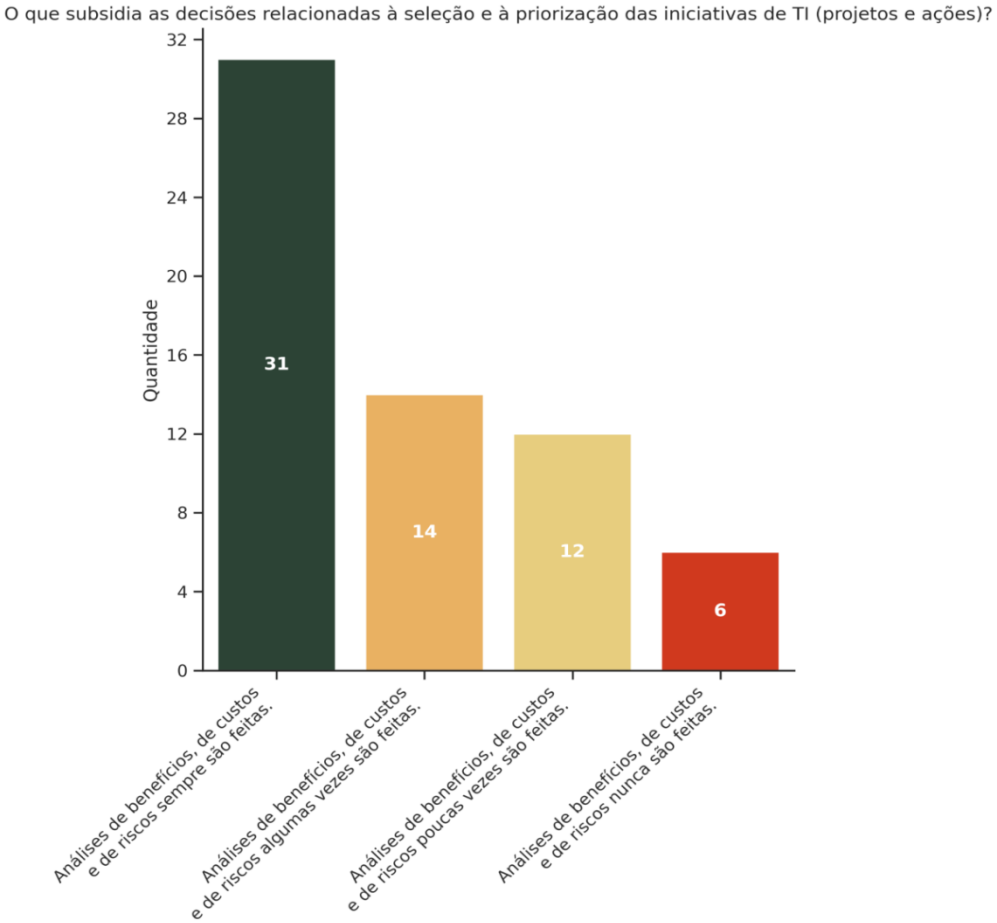


Iniciando a análise, verifica-se por meio da Figura 5 que 39 instituições (62%) informaram que as áreas demandantes de soluções de TI participam do planejamento de TI, e 24 (38%) declararam que as áreas demandantes não participam.

Figura 6 - Estabelece critérios para orientar e priorizar as iniciativas de TI.

A Figura 6 retrata que apenas 8 instituições (13%) afirmaram estabelecer critérios para orientar a seleção e a priorização das iniciativas de TI, mantendo-os atualizados, e 55 (87%) não estabelecem esses critérios.

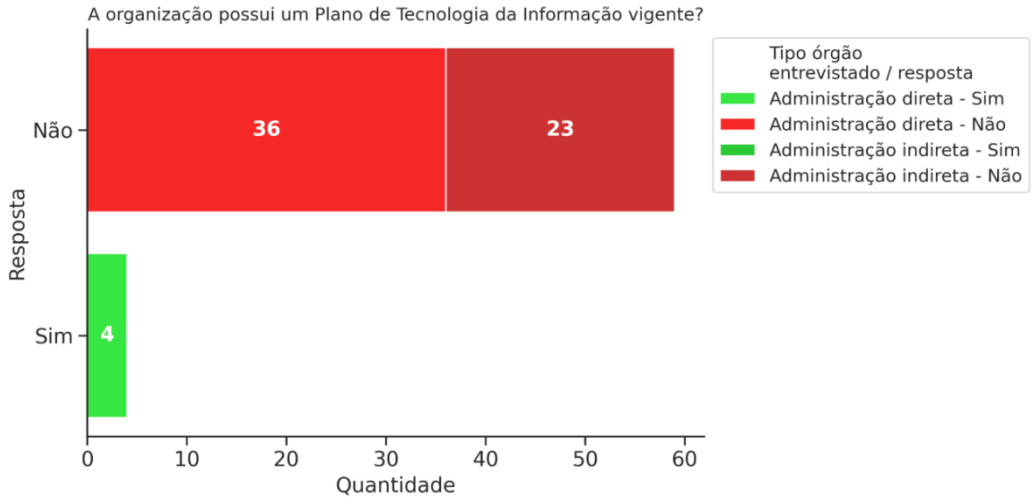
Figura 7 - O que subsidia as decisões relacionadas à priorização das iniciativas de TI



Ainda analisando o processo de planejamento de TI, a Figura 7 mostra que 31 instituições (49%) afirmaram que análises de benefícios, de custos e de riscos sempre são feitas para subsidiar as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações), 14 instituições (22%) declararam que algumas vezes essas análises são feitas, 12 instituições (19%) fazem poucas vezes essas análises e 6 (10%) nunca fazem essas análises.

A Figura 8 a seguir apresenta o resultado da questão exploratória elaborada para identificar a existência de Plano de Tecnologia da Informação vigente nos jurisdicionados.

Figura 8 - A organização possui um plano de TI vigente



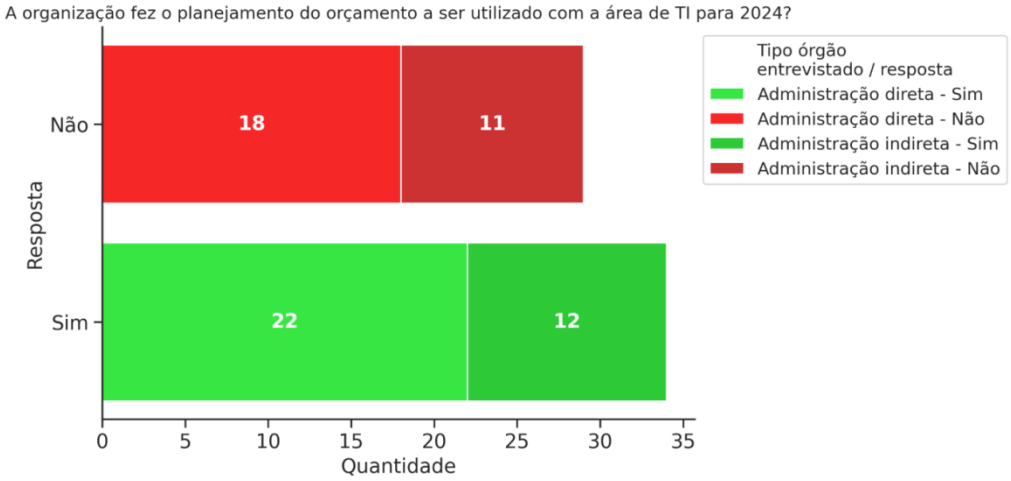
Como resultado, apenas 4 instituições (6%) se destacaram ao afirmar possuir plano de TI vigente, quais sejam: Procuradoria Geral de Justiça, Defensoria Pública Geral do Estado, Tribunal de Justiça, Escola da Magistratura do RN.

Para conhecer com mais detalhes os Planos de TI existentes, foram realizadas as seguintes perguntas exploratórias:

- Quais itens são contemplados pelo Plano de TI?
- Os projetos e ações do Plano de TI alinham-se aos objetivos e iniciativas definidas no Plano Estratégico e demais planos institucionais?
- O Plano de TI é aprovado pelo dirigente máximo da organização ou por dirigente ou colegiado que integra a alta administração?
- O Plano de TI é publicado na Internet?
- É feito acompanhamento concomitante à execução do Plano de TI é acompanhado de forma concomitante, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessários?
- Qual foi o orçamento da área de TI executado em 2023 e planejado para 2024?

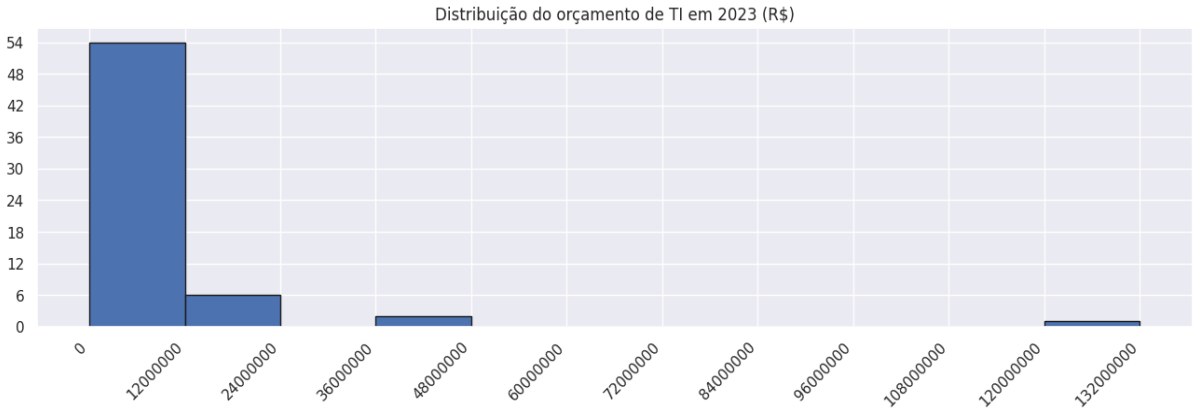
Das 4 instituições que informaram possuir um plano de TI vigente, apenas 2 informaram ter esse Plano alinhado ao Plano Estratégico (ou institucional) e possuir o plano aprovado pela alta gestão da instituição. Além disso, todas informaram publicar o Plano de TI pela Internet, deixando acessível a qualquer cidadão e 3 afirmaram fazer o acompanhamento concomitante à execução do Plano.

Figura 9 - Fez planejamento do orçamento de TI para 2024



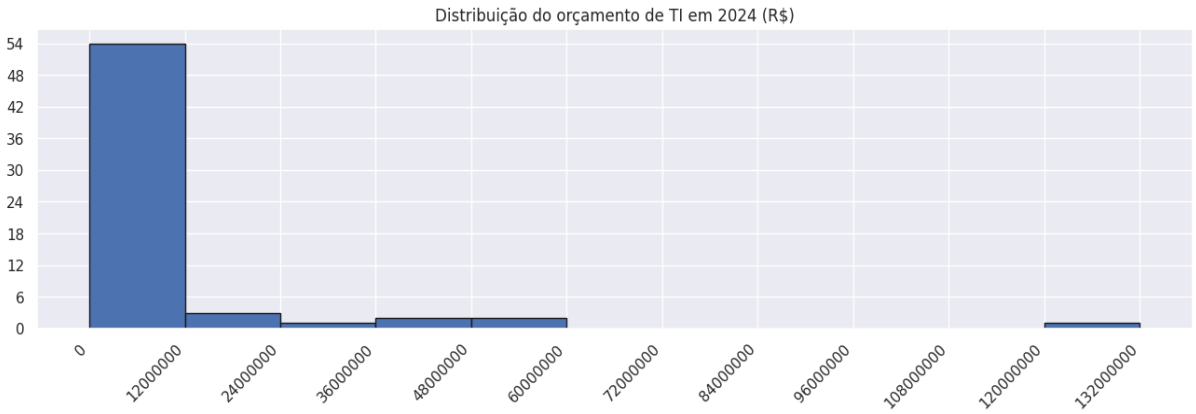
Considerando os dados sobre os orçamentos para a TI em 2023 e 2024, uma das questões levantadas refere-se ao planejamento de orçamento para a TI para o ano de 2024. A figura 9 mostra que 34 instituições informaram que fizeram o planejamento do orçamento de TI para 2024.

Figura 10 - Distribuição do Orçamento de Tecnologia da Informação executado em 2023



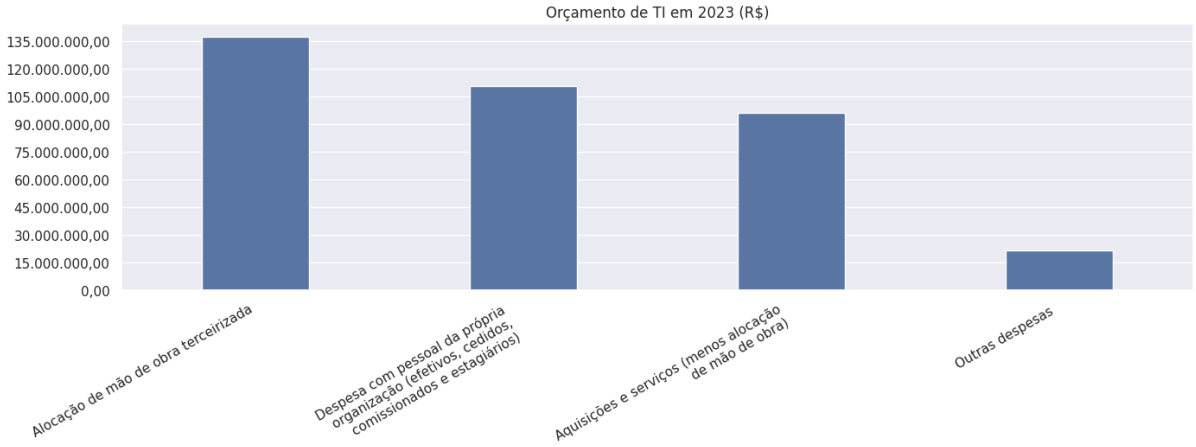
No tocante aos valores informados sobre os orçamentos dos anos 2023, a Figura 10 apresenta os dados informados pelos órgãos. É possível verificar que a maior parte dos órgãos (54 respostas ou 86% do total de órgãos) encontra-se na faixa de até 12 milhões de reais em orçamento para tecnologia da informação. Entre 12 e 24 milhões estão 6 órgãos. Nas outras faixas encontram-se 2 órgãos, no intervalo entre 36 e 48 milhões, e apenas 1 órgão no maior agrupamento definido, com R$ 123.124.600,00 de orçamento.

Figura 11 - Distribuição do Orçamento de Tecnologia da Informação planejado para 2024



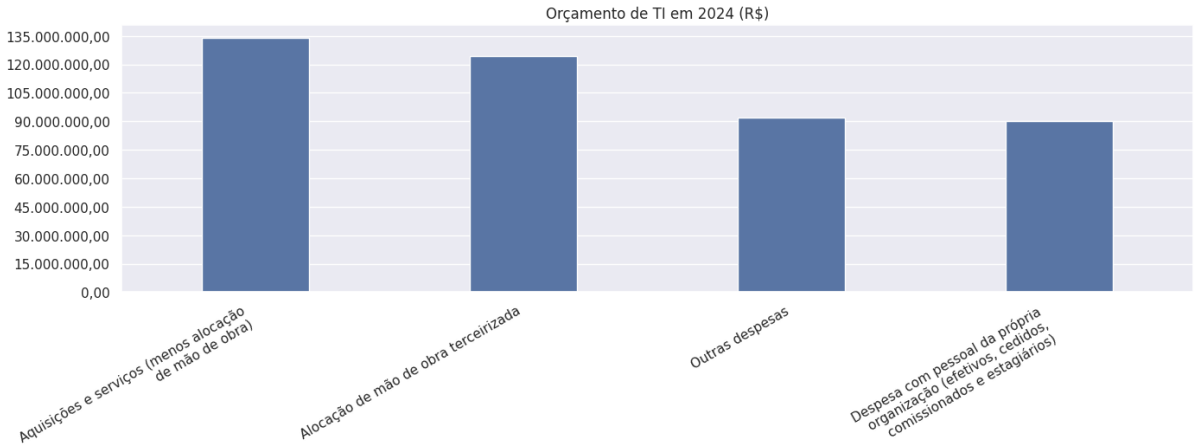
Ao analisar os dados apresentados na Figura 11 referentes ao orçamento de TI previsto para o ano de 2024, percebe-se que a mesma tendência persiste no ano subsequente. Por outra vez a maior parte dos órgãos estão contidos no primeiro grupo (até R$ 12.000.000,00 de orçamento total). Há uma distribuição mais esparsa nas outras faixas, porém o padrão se mantém.

Figura 12 - Total do Orçamento de Tecnologia da Informação executado em 2023



Quando analisado o valor total dos orçamentos aplicados em 2023, conforme declaração dos órgãos respondentes, verifica-se que sua maior parte foi alocada em despesa com alocação de mão de obra terceirizada, seguido de despesa com pessoal da própria organização, aquisições e serviços, e outras despesas (ver Figura 12).

Figura 13 - Total do Orçamento de Tecnologia da Informação planejado para 2024



Observando a Figura 13, percebe-se que os entes participantes deste levantamento informaram que a maior parte do orçamento previsto para uso em TI em 2024 será alocado em aquisições e serviços, seguido de despesas com alocação de mão de obra terceirizada, outras despesas, e por fim, despesas com pessoal da própria organização.

Comparando os orçamentos dos anos 2023 e 2024, percebe-se um aumento expressivo nos valores destinados à aquisição de serviços (menos alocação de mão de obra). Está previsto um aumento aproximado de 40 milhões nessa área. Além disso, um aumento de 70 milhões em outras despesas de TI evidencia um acréscimo notável no orçamento dessa natureza para esse ano. Há também um aumento aproximado de 13 milhões nos gastos destinados à locação de mão de obra terceirizada. Por fim, o orçamento previsto para gasto com pessoal da própria organização permaneceu sem alteração expressiva.

Alguns pontos de destaque valem ser apresentados. Considerando os dados informados sobre o orçamento de 2023, a Secretaria de Estado da Administração apresenta-se como o órgão que mais gastou com TI dentre os participantes deste trabalho: 123,12 milhões. Em seguida, o Tribunal de Justiça/Escola da Magistratura se apresentam com 39,14 milhões e o Instituto de Assistência Técnica e Extensão Rural com 22,94 milhões. Quando avaliamos a previsão de orçamento com a TI para 2024, a Secretaria de Estado da Administração se mantém em destaque com 131,12 milhões, o Tribunal de Justiça/Escola de Magistratura com 59,38 milhões e a Secretaria de Estado da Educação, da Cultura e do Esporte e do Lazer com 40,46 milhões.

2.2.3.Gestão de serviços de Tecnologia da Informação

A gestão dos serviços de Tecnologia da Informação revela-se crucial no contexto da administração pública, desempenhando um papel fundamental na eficiência operacional, na qualidade dos serviços prestados e na satisfação dos cidadãos. A relevância dessa gestão na esfera pública pode ser respaldada pelos princípios da ISO/IEC 20000 e do ITIL (Information Technology Infrastructure Library).

A ISO/IEC 20000, como norma internacional, estabelece requisitos para a implementação de um Sistema de Gestão de Serviços de TI (SGSTI) adaptado às peculiaridades governamentais. Essa norma destaca a importância de práticas consistentes e alinhadas com as necessidades específicas da administração pública, promovendo a entrega eficaz de serviços de TI que atendam às demandas dos cidadãos. A ISO/IEC 20000 não apenas preconiza a melhoria contínua dos processos de gestão de serviços, mas também enfatiza a necessidade de alinhamento com os objetivos estratégicos da organização governamental.

O ITIL, por sua vez, oferece uma abordagem estruturada e abrangente para a gestão de serviços de TI que pode ser especialmente benéfica no âmbito da administração pública. Alguns pontos destacam a importância do ITIL neste contexto, conforme lista a seguir:

- Alinhamento com Objetivos Governamentais: ambos os frameworks, ISO/IEC 20000 e ITIL, ressaltam a importância de alinhar os serviços de TI com os objetivos específicos da administração pública. Garantir que a TI esteja direcionada para contribuir efetivamente para o sucesso das iniciativas governamentais é essencial.
- Melhoria Contínua Adaptada ao Setor Público: tanto a ISO/IEC 20000 quanto o ITIL destacam a necessidade de melhoria contínua, adaptada às peculiaridades do setor público. A avaliação constante dos processos, a identificação de oportunidades de aprimoramento e a implementação de mudanças são vitais para atender às demandas dos cidadãos.
- Padronização para Consistência em Serviços Públicos: o ITIL, ao preconizar a padronização de processos, contribui para a consistência na entrega de serviços. Isso é crucial para a administração pública, reduzindo variabilidades, minimizando erros e promovendo a previsibilidade na prestação de serviços de TI.
- Foco na Satisfação do Cidadão: ambos os frameworks reconhecem a importância da satisfação do cliente. No contexto público, isso se traduz na satisfação dos cidadãos. O ITIL destaca a necessidade de gerenciar as expectativas dos cidadãos e fornecer serviços que atendam ou superem essas expectativas, promovendo a confiança e a credibilidade.
- Gestão de Riscos Adaptada ao Setor Público: a gestão de riscos é um aspecto central tanto na ISO/IEC 20000 quanto no ITIL, adaptada às peculiaridades do setor público. A identificação, avaliação e mitigação de riscos são práticas essenciais para garantir a continuidade dos serviços de TI e a resiliência diante de eventos adversos.

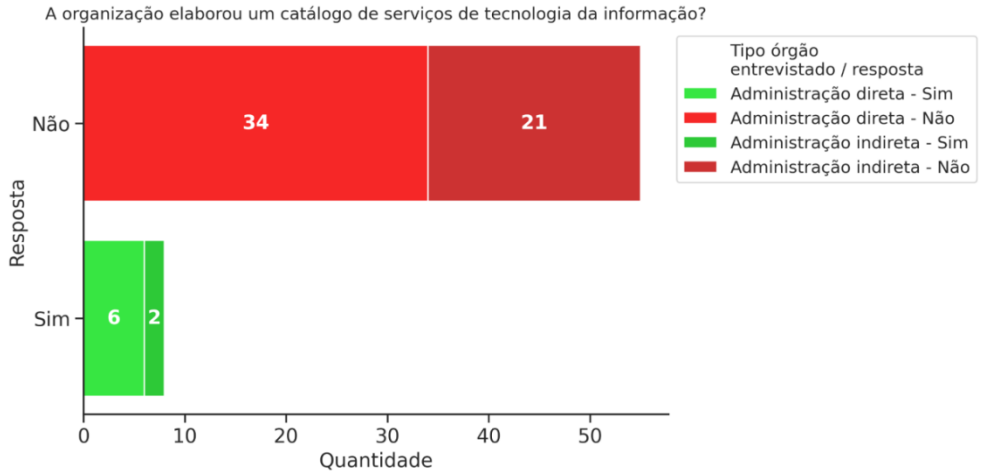
Em resumo, a gestão de serviços de TI, respaldada pelos princípios da ISO/IEC 20000 e do ITIL, desempenha um papel vital na administração pública. A aplicação desses frameworks não apenas eleva a eficiência operacional, mas também contribui para a prestação de serviços públicos de alta qualidade, alinhados com os objetivos governamentais e capazes de se adaptar às necessidades em constante evolução dos cidadãos.

Considerando os aspectos apresentados, ficou claro que uma das questões a serem trabalhadas nesse levantamento seria verificar se as **organizações gerenciam serviços de Tecnologia da Informação.** Assim, a equipe de auditoria considerou importante requerer informações acerca do catálogo de serviços de TI, do processo de gestão de

mudanças, do processo de gestão de configuração e ativos e do Processo de gestão de incidentes de serviços de Tecnologia da Informação.

As figuras 14 e 15 apresentam o resultado das respostas das instituições sobre seus catálogos de serviços de TI. As figuras 16 e 17 apresentam os resultados das respostas das instituições sobre seus processos de gestão de mudanças de ativos de TI. Já as figuras 18 e 19 são resultantes das respostas sobre definição de regras para priorização e escalonamento de incidentes.

Figura 14 – Elaboração do catálogo de serviços de TI



Como pode ser observado na Figura 14, apenas 8 instituições afirmaram ter um catálogo de serviços de TI. A Figura 15 informa que dessas 8, apenas 2 informaram que este catálogo contém as metas definidas para cada serviço. É possível observar que 4 instituições afirmaram que seus catálogos estão atualizados e as informações que neles 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. Quando questionadas sobre a facilidade de acesso e disponibilidade do catálogo para seus usuários e equipes de suporte, todas as 7 instituições afirmaram que sim.

Figura 15 - Nível de maturidade do catálogo de serviços de TI

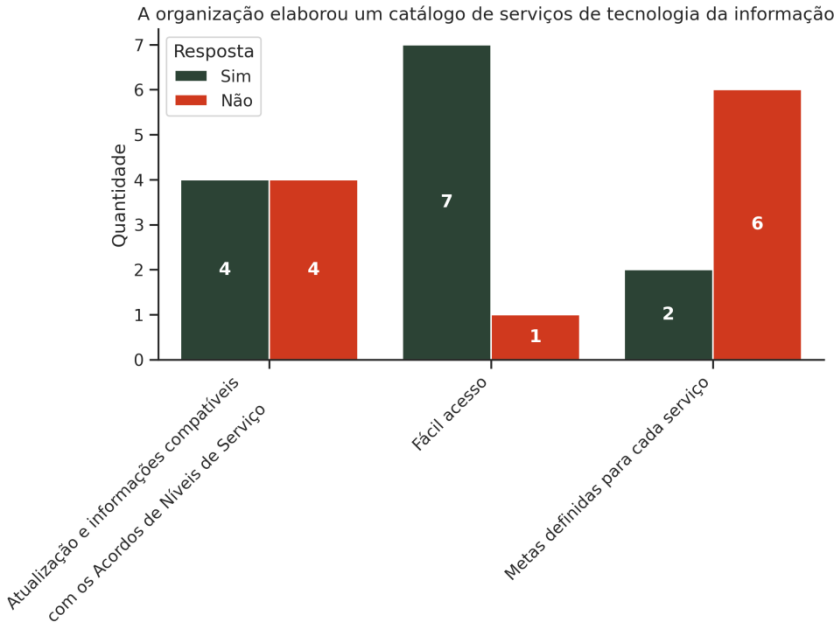
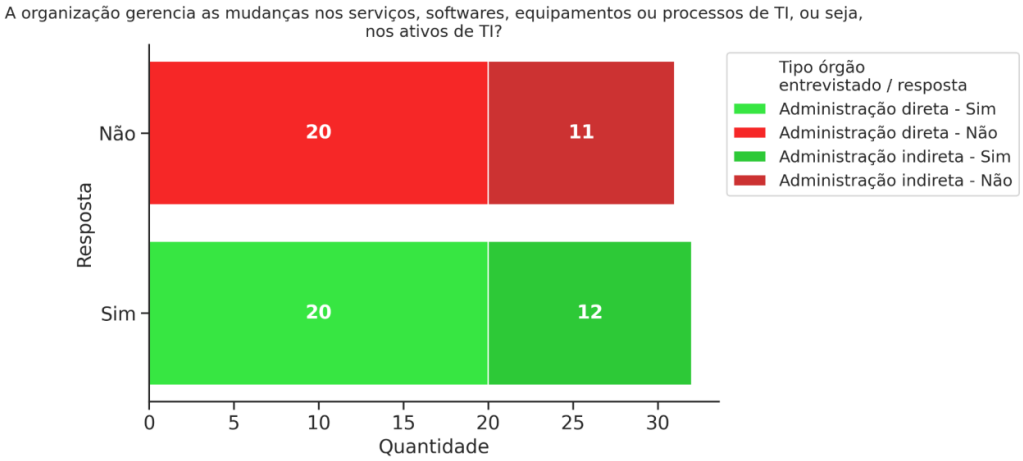
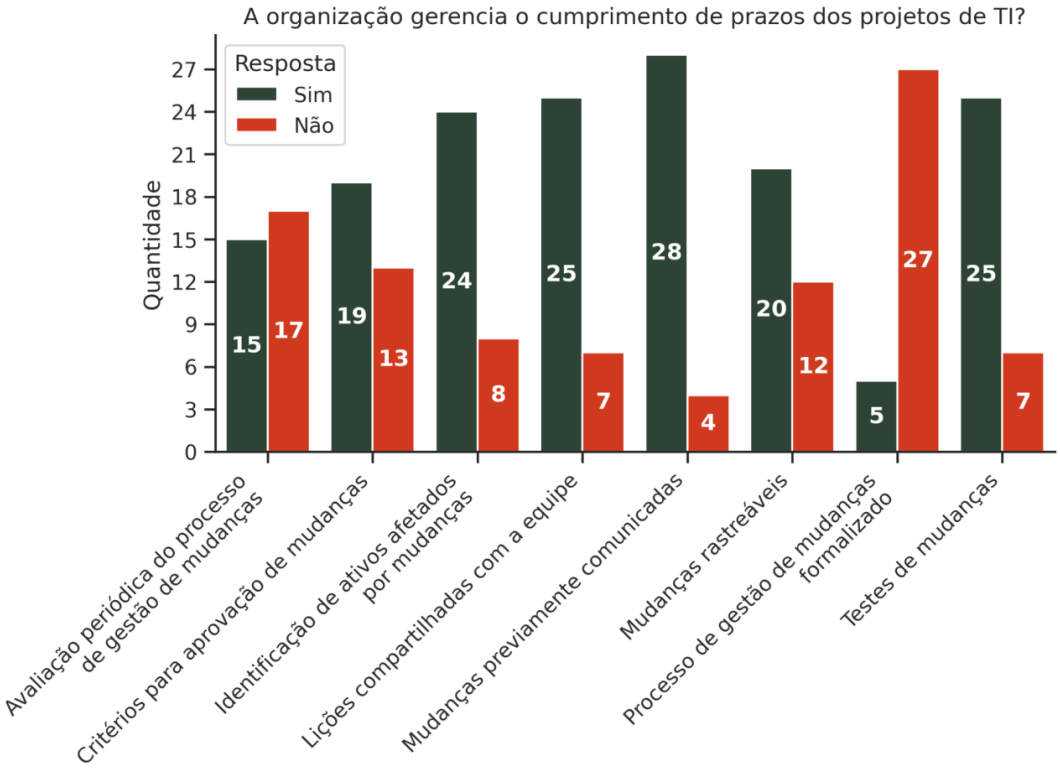


Figura 16 - Gestão das mudanças dos ativos de TI



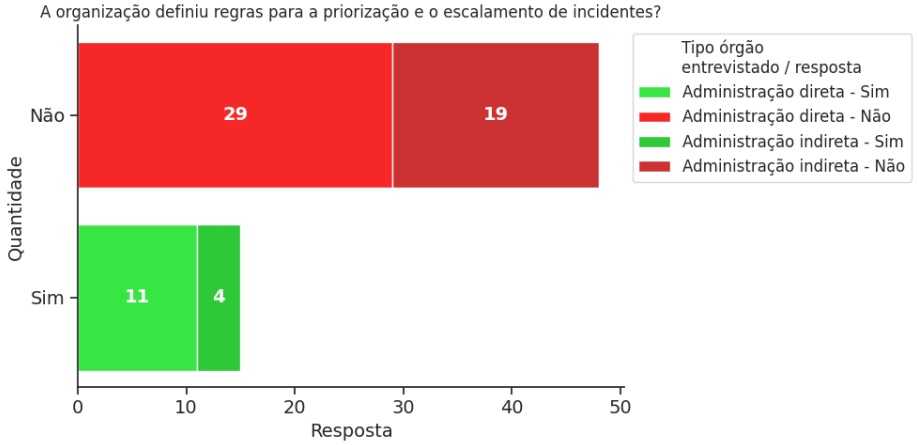
Quando analisadas as respostas sobre o processo de gestão de mudanças, verifica-se que 32 instituições afirmaram gerenciar as mudanças de seus ativos de TI (Figura 16). As demais declararam não gerenciar as mudanças de seus ativos.

Figura 17 - Nível de Maturidade da gestão de mudanças dos Ativos de TI



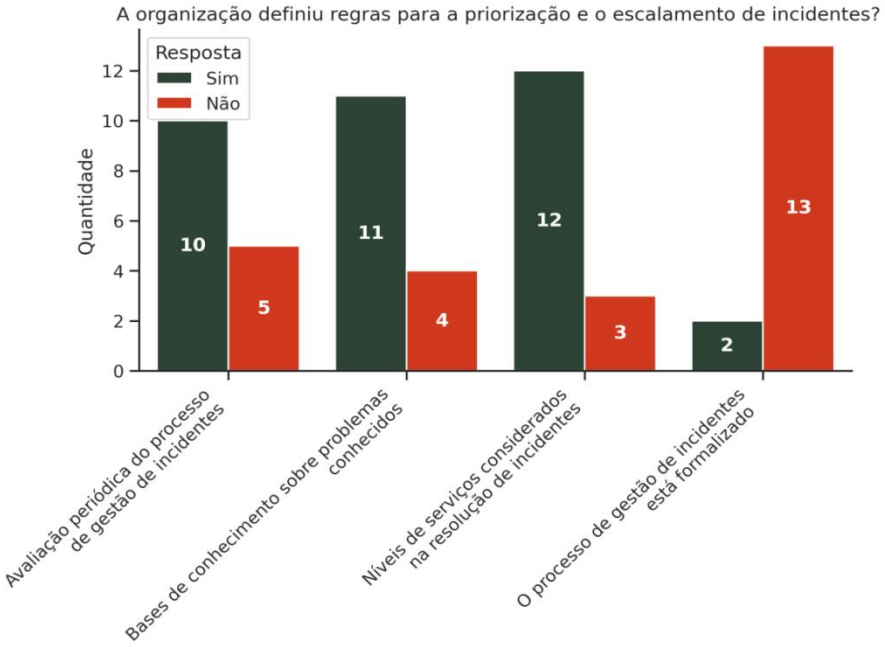
Ao analisar as questões referentes à maturidade da gestão de mudança de ativos de TI, Figura 17, é perceptível que grande parte das instituições afirmou comunicar previamente as mudanças, realizar testes nas mudanças a serem implantadas, identificar ativos afetados pelas mudanças e compartilhar lições aprendidas com a equipe. Porém, a maioria não formaliza este processo.

Figura 18 - Definiu regras para a priorização e o escalamento de incidentes



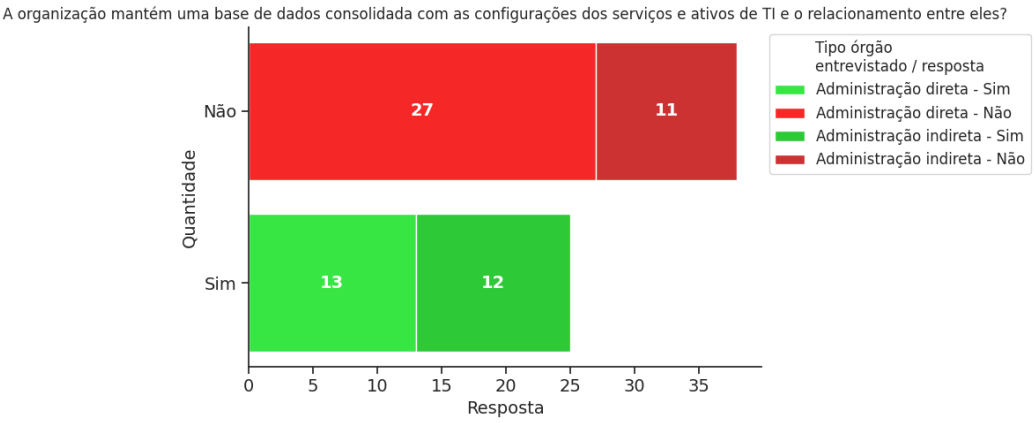
Ao analisar a questão referente à regra para a priorização de gestão de incidentes (Figura 18), verifica-se que 15 instituições afirmaram definir regras para a priorização e o escalonamento de incidentes. Porém, 48 afirmaram não definir essas regras.

Figura 19 - Detalhes sobre as regras para a priorização e o escalamento de incidentes



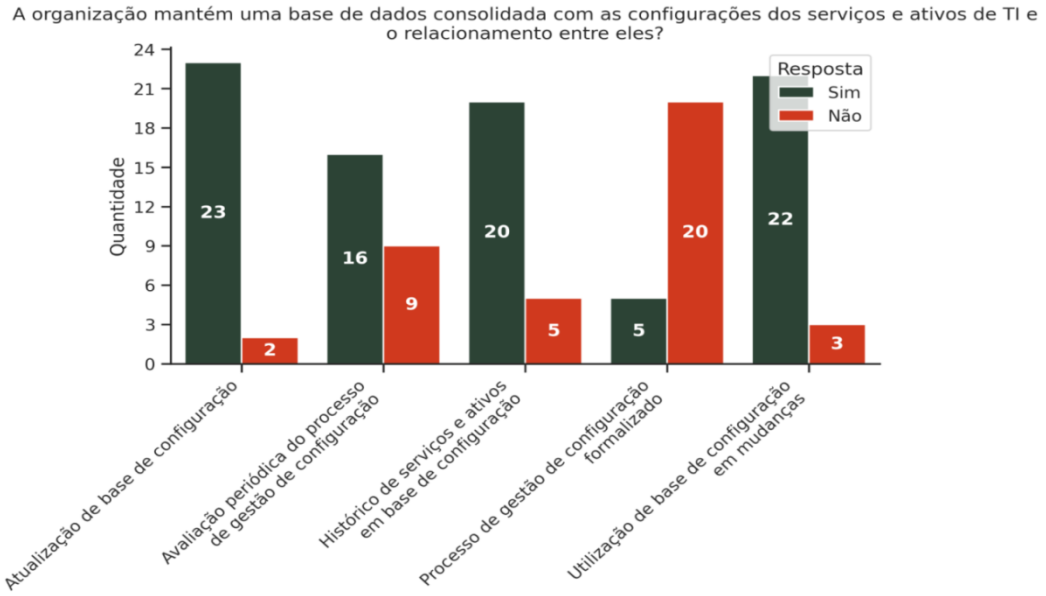
Ao avaliar o detalhamento da forma como essas regras são definidas (Figura 19), verifica-se que das 15 instituições que afirmaram positivamente, 11 afirmaram manter uma base de conhecimento sobre problemas conhecidos e 12 afirmaram considerar os níveis de serviços na priorização da resolução dos incidentes.

Figura 20 - Possui base de dados com as configurações dos serviços e ativos de TI



Ao verificar as respostas relacionadas à manutenção de uma base de dados com as configurações de serviços e ativos de TI (Figura 20), 25 instituições afirmaram realizar a manutenção dessa base.

Figura 21 - Detalhes sobre a base de dados com as configurações dos serviços e ativos de TI



Dessas (Figura 21), 20 informaram que suas bases de configuração permitem à organização conhecer o histórico de situações dos serviços e ativos de TI, 23 informaram que suas bases estão atualizadas e 22 informaram que suas bases são usadas como insumo para o planejamento e acompanhamento das mudanças. Além disso, apenas 5 informaram possuir um processo de gestão de configuração de ativos formalizado e 16 afirmaram realizar avaliação e manutenção periódica nesse processo.

2.2.4. Gestão de níveis de serviços prestados de Tecnologia da Informação

A Gestão de Níveis de Serviços de Tecnologia da Informação é um processo que envolve o estabelecimento, medição e monitoramento dos padrões e níveis de serviços oferecidos pela área de TI de uma organização. Isso implica na definição de acordos de níveis de serviço (do inglês Service Level Agreements, ou SLAs), que são contratos formais entre a área de TI e seus clientes internos ou externos, estabelecendo expectativas claras sobre a qualidade, disponibilidade e desempenho dos serviços de TI oferecidos.

Para os órgãos públicos que fornecem ou usam serviços de TI, a importância da Gestão de Níveis de Serviços de TI é significativa, pois ajuda a garantir que os serviços de tecnologia sejam prestados de maneira eficiente, confiável e alinhada com as necessidades e expectativas dos usuários e da sociedade em geral. Ao definir e monitorar os SLAs, os órgãos públicos podem garantir a transparência na prestação de serviços de TI, melhorar a satisfação dos usuários e otimizar a utilização dos recursos de tecnologia disponíveis.

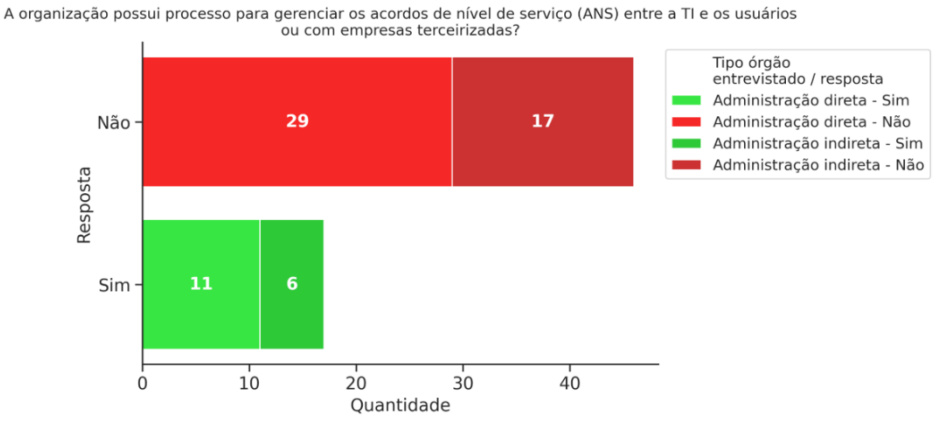
O Tribunal de Contas da União estabelece diretrizes e normativas que podem influenciar a Gestão de Níveis de Serviços de TI nos órgãos públicos brasileiros, através dos acórdãos Acórdão 1.114/2014-TCU-Plenário: 9.1.1 comunicação de resultados de gestão de níveis de serviço de TI. Essas diretrizes visam garantir a qualidade, eficiência e eficácia dos serviços de TI prestados, incentivando a definição adequada de SLAs, o acompanhamento dos indicadores de desempenho e a prestação de contas sobre a qualidade dos serviços oferecidos.

Considerando isso, a aplicação deste questionário avalia o nível de maturidade dos órgãos respondentes quanto à gestão dos acordos de nível de serviços de Tecnologia da Informação. Para possibilitar essa avaliação, se faz necessário verificar:

- Se as organizações possuem controle sobre os níveis de serviços de TI prestados pelos setores internos e por terceiros.
- Se há aderência de seus processos de gestão aos critérios de gestão de nível de serviços TI.
- O nível de formalização dos processos de gestão de acordo de nível de serviços de TI dessas organizações.
- Se há aderência do processo de gestão de mudanças das organizações às normas dos critérios elencados.
- O nível de formalização do processo de gestão de mudanças dessas organizações.
- Se há aderência do processo de gestão de configuração de ativos das organizações às normas dos critérios elencados.
- O nível de formalização do processo de gestão de configuração de ativos das instituições avaliadas.
- Se há aderência do processo de gestão de indicadores da organização às normas dos critérios elencados.
- O nível de formalização do processo de gestão de indicadores.

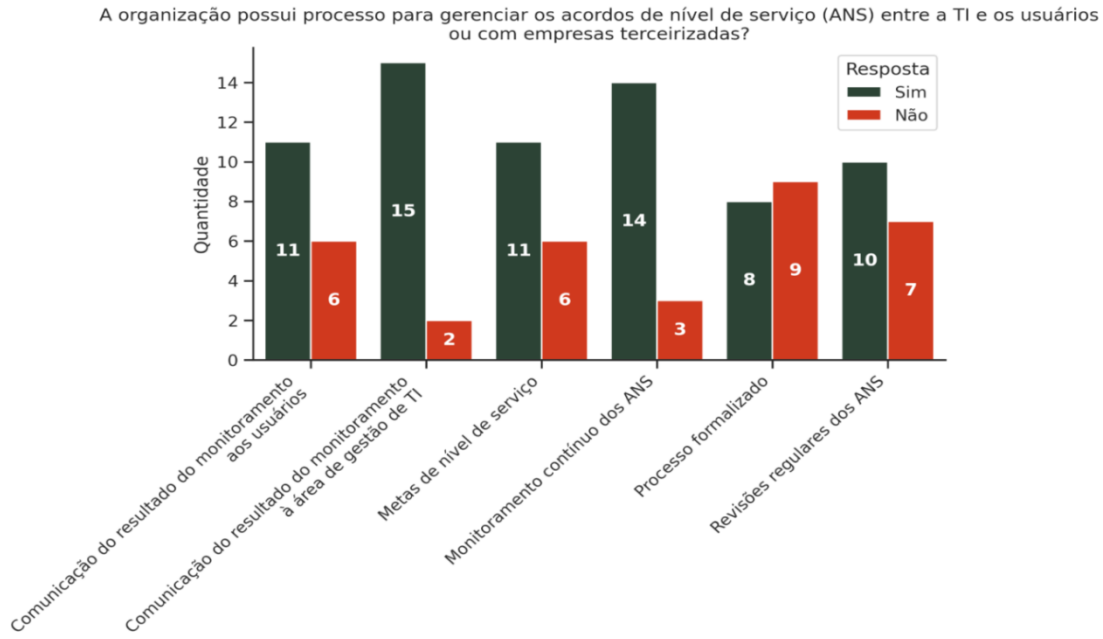
O resultado das informações obtidas está presente nos gráficos que se seguem.

Figura 22 - Possuem processos para gerenciar os ANS entre TI, usuários ou empresas



A Figura 22 apresenta que 17 instituições (27% dos entrevistados) afirmam possuir um processo de gestão de acordo de nível de serviços (ANS) de TI com os usuários e empresas terceirizadas. Já 43 instituições afirmam não possuir um processo de gestão de ANS.

Figura 23 - Nível de maturidade dos processos de gestão de ANS



A Figura 23 mostra que, das 15 instituições que afirmam gerenciar seus ANSs, 11 afirmam comunicar os resultados do monitoramento dos ANSs aos usuários, 13 afirmam comunicar os resultados desse monitoramento à área de gestão de TI, 10 estabelecem metas de nível de serviço acordadas com representantes das áreas de negócio, 12 fazem o monitoramento contínuo dos ANSs, 7 possuem processo de gestão de ANS formalizado e 8 fazem revisão regulares desses processos.

2.2.5. Definição de políticas, processos e responsabilidades para a gestão da Segurança da Informação

O estabelecimento de políticas, processos e responsabilidades para a gestão da Segurança da Informação refere-se à definição e implementação de medidas, procedimentos e práticas destinadas a proteger ativos de informação dentro de uma organização. Isso inclui a identificação de riscos, a implementação de controles de segurança, a gestão de incidentes, a garantia da conformidade com regulamentos e padrões de segurança e a conscientização dos colaboradores da organização. Para os órgãos públicos, essas ações são de extrema importância, uma vez que lidam com ativos de alto custo financeiro, serviços essenciais para o funcionamento da saúde, educação, transporte e segurança, bem como dados sensíveis e informações críticas dos cidadãos e do Estado. A adoção de práticas de Segurança da Informação é crucial para proteger esses ativos contra ameaças internas e

externas, prevenindo paradas de serviços, perda de ativos valiosos, vazamentos de informações sensíveis, violações de dados e garantindo a confidencialidade, integridade e disponibilidade das informações.

A norma ISO 27001 preconiza, em suas cláusulas 4.1 e 4.2, que o contexto de uma organização seja identificado e documentado. Esse é o passo inicial para a determinação do escopo de um Sistema de Gestão de Segurança da Informação e de seu documento principal: a Política de Segurança da Informação. A cláusula 5.2 do padrão ISO 27001 e seu controle A.5.1 contém os requisitos básicos para a construção do documento.

As necessidades da aplicação das boas práticas presentes na ISO 27001 são reforçadas com o Decreto Nº 11.856, de 26 de Dezembro de 2023 institui a Política Nacional de Cibersegurança - PNCiber, com a finalidade de orientar a atividade de segurança cibernética no País.

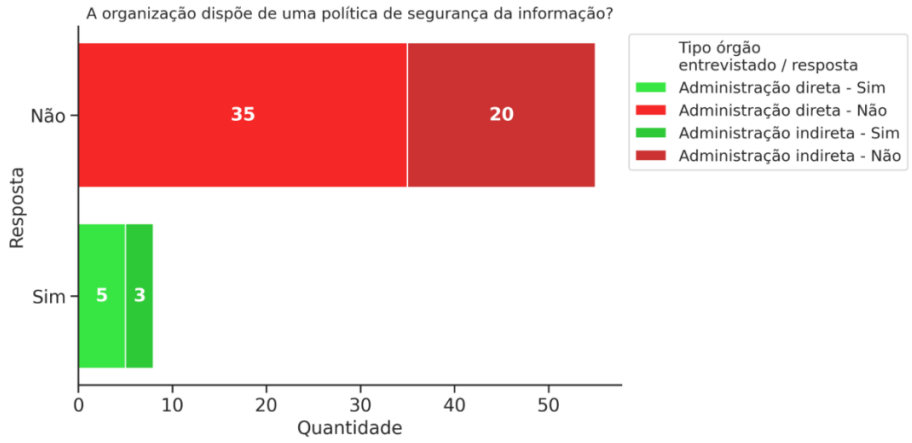
Uma Política de Segurança da Informação define os objetivos estratégicos que guiam o desenvolvimento de um Sistema de Gestão de Segurança da Informação. Ela deve ser aprovada pela alta gestão, publicada e comunicada em todos os níveis da organização. Pode ser desenvolvida de modo iterativo, a depender de sua complexidade, e deve ser revisada regularmente. As partes envolvidas no processo de segurança da informação definido pela política e suas atribuições devem ser claramente identificadas.

Note-se que o padrão ISO 27000 define informação de modo amplo (“informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por meio eletrônico, escrita ou falada”), de modo que a Política de Segurança da Informação deve tratar de proteção a informações de diversas naturezas, atentando primordialmente à confidencialidade, disponibilidade e integridade das informações protegidas.

As perguntas referentes a essa seção do questionário eletrônico buscaram determinar a definição e maturidade das Políticas de Segurança da Informação implantadas nos órgãos respondentes e as ações e diretrizes estabelecidas por aqueles documentos. Inquiriu-se sobre a adesão e suporte da alta gestão aos objetivos da política, os papéis definidos no Sistema de Gestão de Segurança da Informação do órgão e a implementação de aspectos mais técnicos relacionados à proteção da informação. As respostas coletadas são apresentadas a seguir.

A primeira pergunta da presente seção do questionário tratou da existência de uma Política de Segurança da Informação em vigência nos órgãos participantes (Figura 24). Depreende-se da leitura do gráfico a seguir que apenas uma minoria, dentre os respondentes, dispõe desse instrumento.

Figura 24 - Dispõe de uma política de segurança da informação

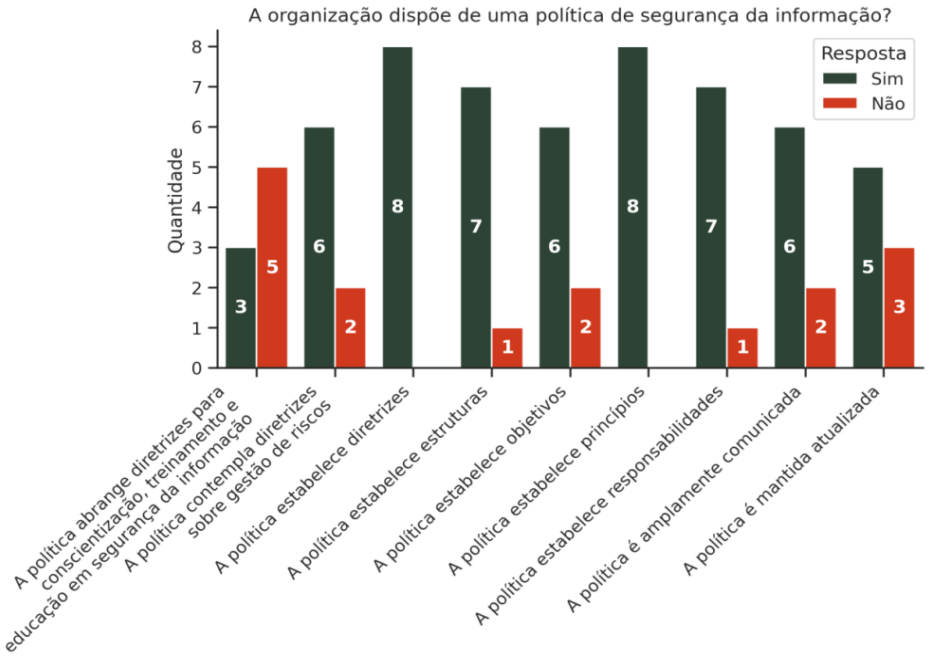


O resultado obtido aponta a imaturidade dos órgãos analisados no tocante à Segurança da Informação. Foram apenas 8 respostas positivas em um total de 63, representando 12,69% do universo analisado. Os órgãos que afirmaram possuir Política de Segurança da Informação são: Procuradoria Geral de Justiça, Tribunal de Contas do Estado, Hospital Maria Alice Fernandes, Tribunal de Justiça e Escola da Magistratura do RN (administração direta) e Companhia Potiguar de Gás, Agência de Fomento do RN S/A, Companhia Estadual de Habitação e Desenvolvimento Urbano (administração indireta).

Os aspectos subjacentes a uma Política de Segurança da Informação foram aferidos por meio de perguntas associadas. Vê-se no gráfico da Figura 25 que, apesar da ausência de Política de Segurança da Informação na maioria dos órgãos entrevistados, aqueles que implementam o instrumento quase sempre estabelecem princípios, diretrizes, objetivos, estruturas e responsabilidades associadas à segurança da informação em suas políticas.

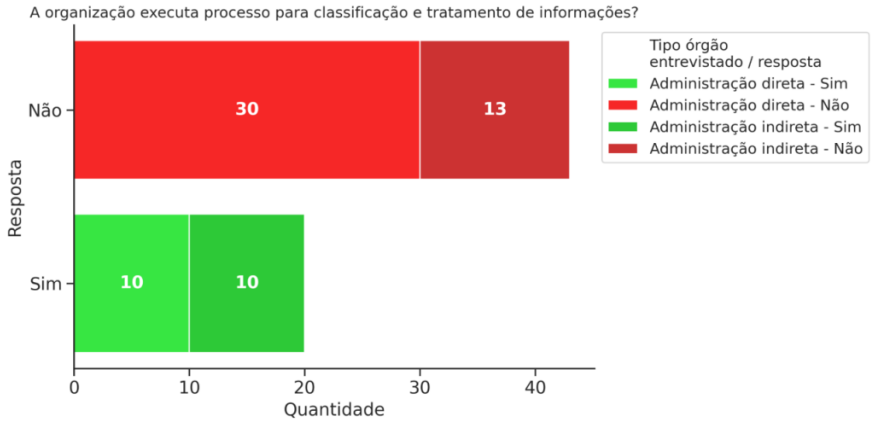
Os maiores índices de respostas negativas associadas aos atributos das Políticas de Segurança da Informação referem-se à atualização e ao treinamento acerca do conteúdo destas.

Figura 25 - Detalhes sobre a política de segurança da informação



Outros aspectos da segurança da informação são tratados no bojo de uma Política de Segurança da Informação. Dentre estes, a classificação de informações destaca-se por sua importância, especialmente à luz da lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD). Acerca do tema, obteve-se o seguinte resultado dos órgãos entrevistados, apresentado na Figura 26:

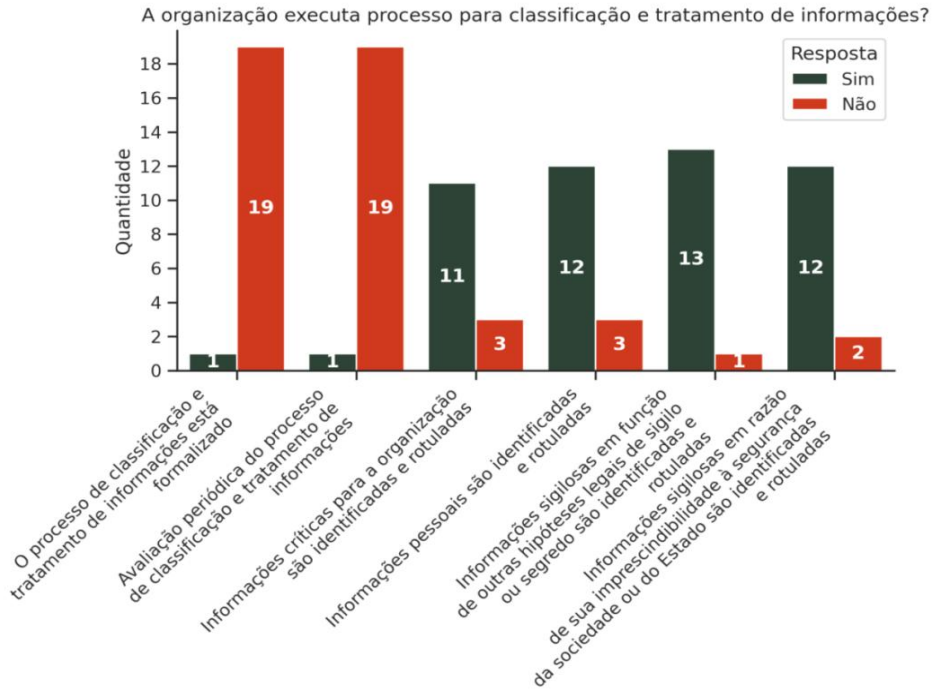
Figura 26 - Executa processo para classificação e tratamento de informações



Na administração direta, os órgãos que afirmaram realizar a classificação de suas informações foram: Procuradoria Geral de Justiça, Secretaria de Estado de Turismo, Defensoria Pública Geral do Estado, Polícia Civil, Secretaria de Estado da Administração, Departamento Estadual de Imprensa, Hospital Maria Alice Fernandes, Secretaria de Estado da Administração Penitenciária, Secretaria de Estado da Infraestrutura e Secretaria de

Estado da Educação, da Cultura, do Esporte e do Lazer. Na administração indireta, os órgãos Departamento Estadual de Trânsito, Instituto de Previdência dos Servidores do RN, Companhia Estadual de Habitação e Desenvolvimento Urbano, Fundação de Atendimento Socioeducativo do Estado do RN, Empresa de Pesquisa Agropecuária do RN, Junta Comercial do Estado do RN, Universidade do Estado do Rio Grande do Norte, Instituto de Desenvolvimento Sustentável e Meio Ambiente do RN, Departamento de Estradas e Rodagens do RN e Instituto de Pesos e Medidas do RN responderam positivamente à mesma pergunta. Em relação à forma de execução do processo de classificação das informações, obteve-se o conjunto de informações exposto no gráfico da Figura 27.

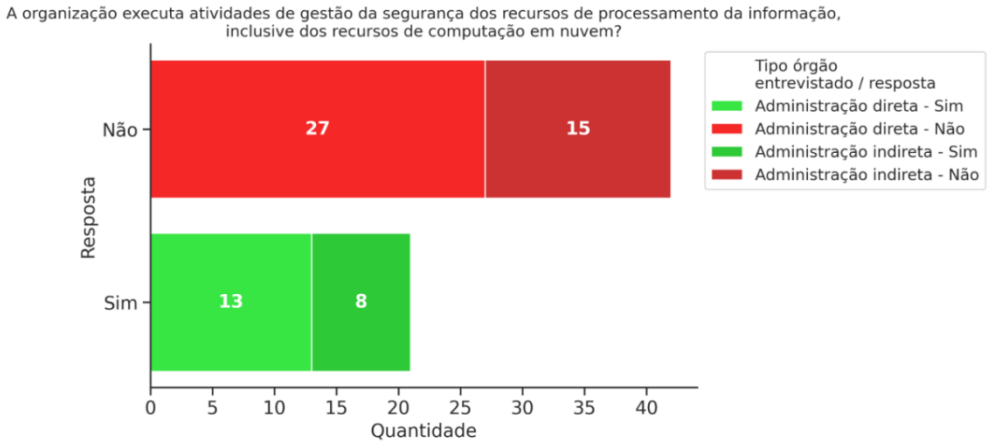
Figura 27 - Detalhes do processo para classificação e tratamento de informações



A formalização do processo de classificação de informações ocorreu apenas no Hospital Maria Alice Fernandes e somente o Departamento Estadual de Trânsito informa que periodicamente avalia o seu processo. Por outro lado, a maioria daqueles que informam executar os processos de classificação de informação também afirmam realizar a atribuição de níveis de acesso restrito às informações críticas tratadas.

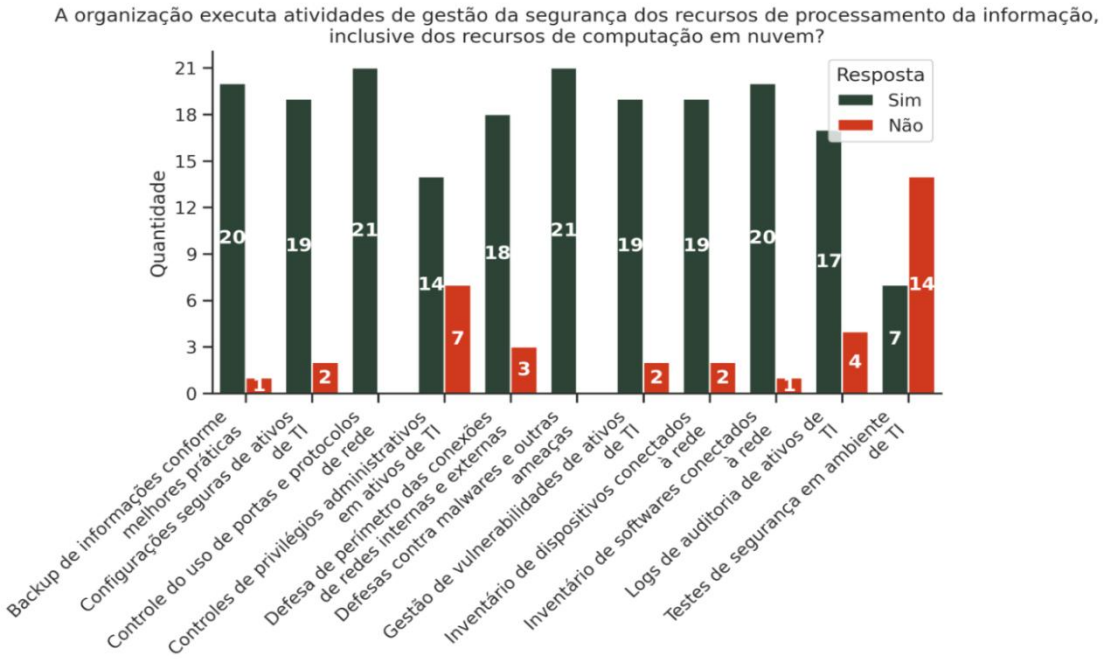
A segurança da informação perpassa forçosamente a segurança dos recursos computacionais que a armazena. Nesse sentido, o questionário inquiriu acerca da gestão da segurança dos recursos de processamento da informação (Figura 28):

Figura 28 - Executa atividades de gestão da segurança dos recursos de processamento da informação



As perguntas associadas ao tema (Figura 29) trataram de aspectos mais técnicos da operacionalização da segurança da informação.

Figura 29 - Detalhes das atividades de gestão da segurança dos recursos de processamento da informação



Os órgãos que declararam realizar a gestão de segurança em recursos de Tecnologia da Informação responderam predominantemente de forma positiva à realização da maioria das atividades técnicas subjacentes ao tema. Somente em relação à realização de testes de segurança houve uma maioria de respostas negativas registradas.

Figura 30 - Executa processo de gestão de incidentes de segurança da informação

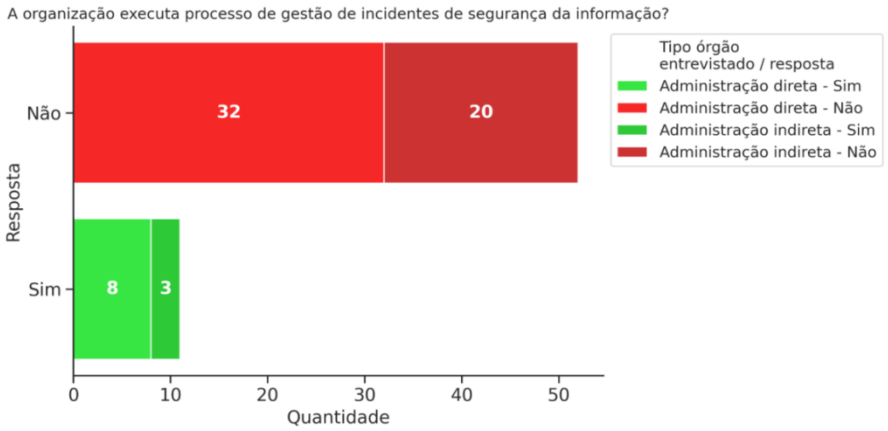
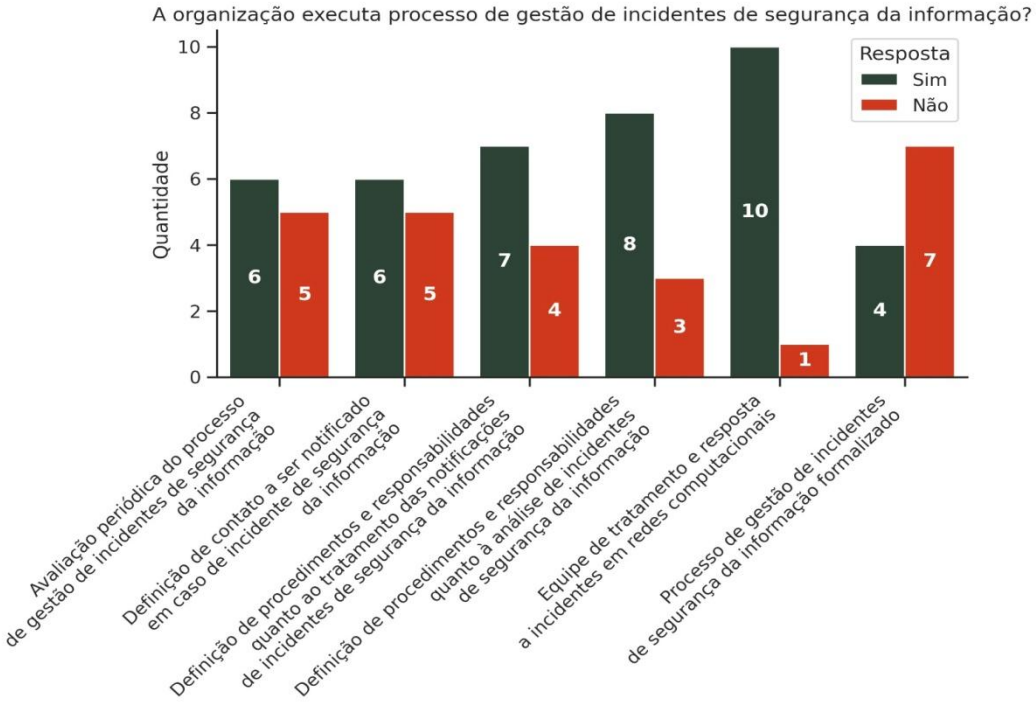


Figura 31 - Detalhes do processo de gestão de incidentes de segurança da informação

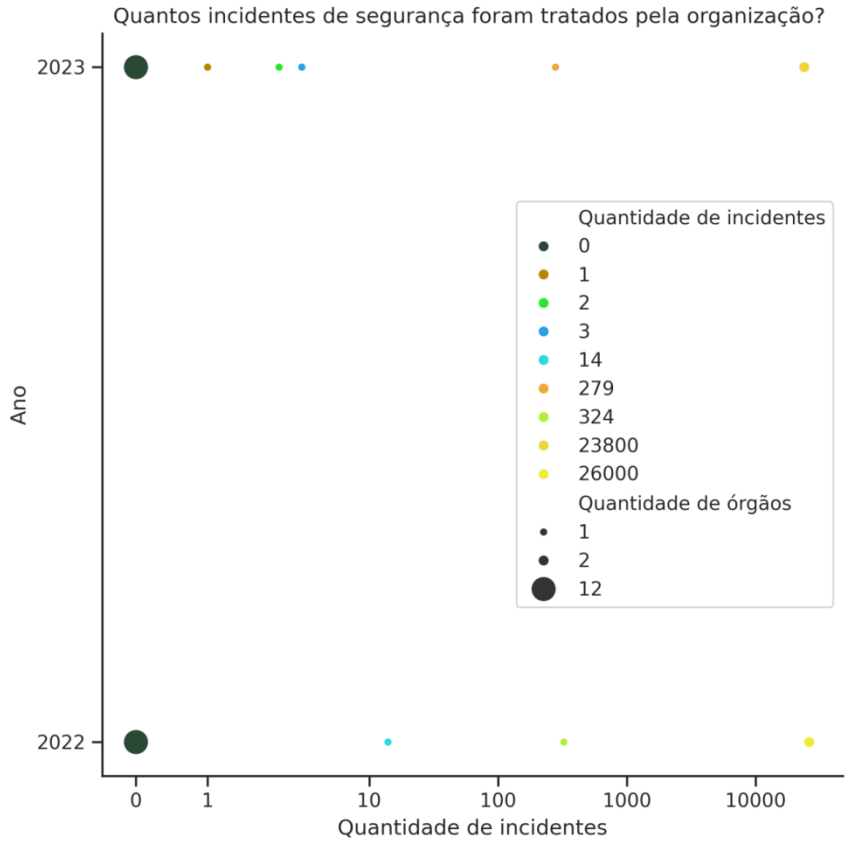


Não obstante a implementação de medidas de segurança da informação, as organizações estão sujeitas a incidentes de segurança provocados por atores mal intencionados. O Anexo A da norma ISO 27001 traz controles referentes à gestão de incidentes de segurança (controles 5.24 a 5.28). Em relação ao tema, as informações apresentadas nas Figuras 30 e 31 foram aferidas no questionário eletrônico.

Somente 11 órgãos afirmaram possuir um processo de gestão de incidentes de segurança da informação (e apenas quatro afirmaram tê-lo formalizado). Nesse ponto do questionário

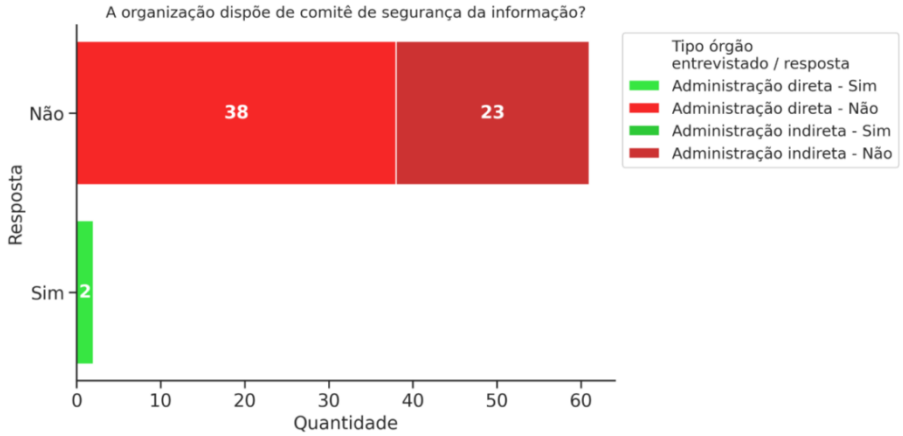
foram coletadas as quantidades de incidentes registrados nos anos de 2022 e 2023. O gráfico da Figura 32 agrupa em seu eixo horizontal a quantidade de incidentes (pontos mais à direita indicam maior concentração de registros) e órgãos (o tamanho do ponto refere-se à quantidade de órgãos agrupados naquela região de quantidade de incidentes) por ano. Infere-se da leitura da figura que a maioria dos órgãos registrou nenhum incidente. De fato, apenas uma minoria relata ter mais de 100 registros: AGN com 324 incidentes em 2022 e 279 em 2023; TJRN e ESMARN com 26.000 incidentes em 2022 e 23.800 incidentes. O eixo horizontal do gráfico foi ajustado à escala logarítmica para melhor visualização dos dados.

Figura 32 - Quantidade de incidentes de segurança da informação tratados pela organização



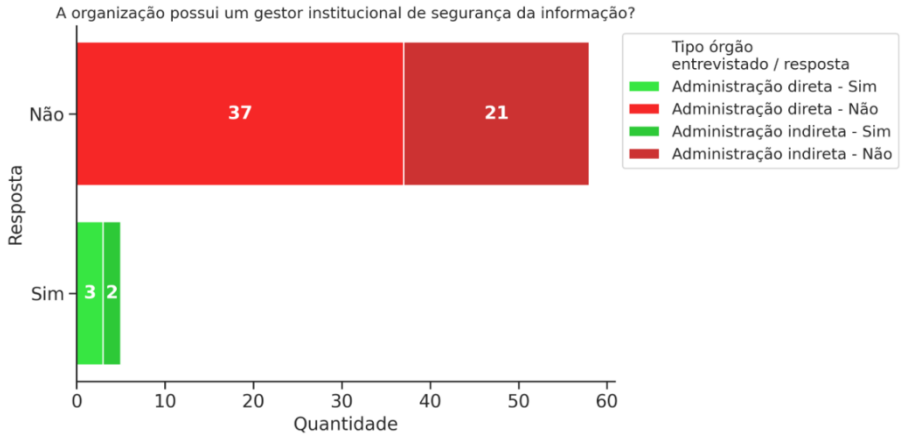
Por fim, as responsabilidades próprias da segurança da informação foram aferidas em perguntas sobre a existência de comitê e gestor institucional de segurança da informação (Figuras 33 e 34). Acerca do comitê, verificou-se que apenas 2 órgãos declararam tê-lo instituído: o TJRN e sua Escola da Magistratura (ESMARN). Ambos responderam positivamente às perguntas: ***"O comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo?"***, ***"O comitê formula diretrizes para a segurança da informação?"***, ***"O comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação?"*** e ***"O comitê é composto por representantes de áreas relevantes da organização?"***.

Figura 33 - Dispõe de comitê de segurança da informação



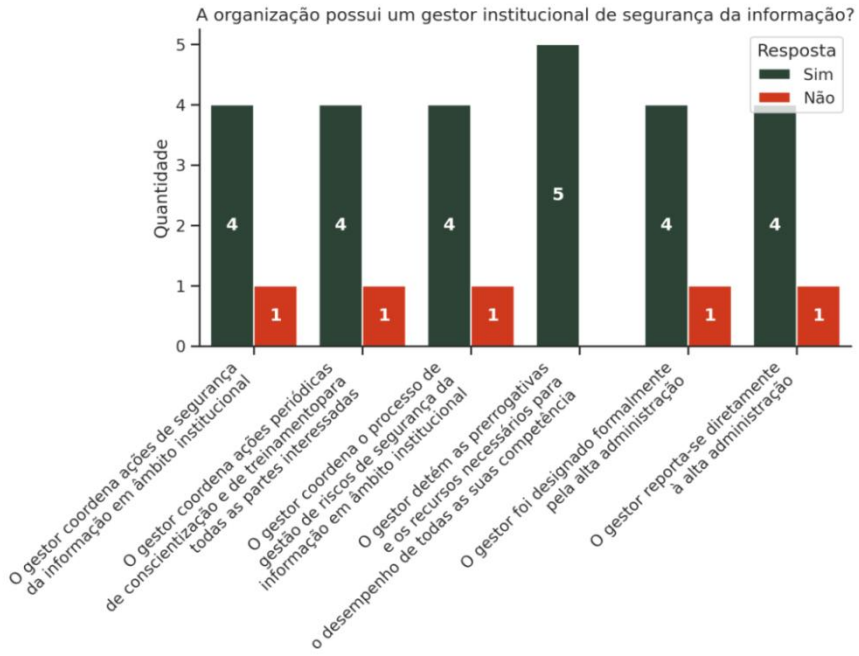
De modo semelhante, apenas uma pequena quantidade de órgãos (5 entrevistados) informaram ter instituído a figura do gestor de segurança da informação: Instituto de Previdência dos Servidores do RN, Centrais de Abastecimento do RN S/A, Secretaria de Estado de Turismo, Tribunal de Justiça, Escola da Magistratura do RN.

Figura 34 - Possui gestor institucional de segurança da informação



No tocante às questões associadas ao tema, a pergunta ***"O gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências?"*** obteve um resultado positivo unânime. Somente a Secretaria de Estado de Turismo respondeu negativamente para as outras perguntas referentes às atribuições de seu gestor, assinalando que o cargo de fato não realiza as atividades esperadas da função (Figura 35).

Figura 35 - Detalhes sobre a gestão institucional de segurança da informação



2.2.6.Gestão de Riscos de Segurança da Informação

As boas práticas (cláusula 6.1.2 da norma ISO 27001:2022) orientam que uma organização deve possuir um processo de avaliação de riscos de segurança da informação. O processo aplicado deve identificar riscos, responsáveis e critérios de aceitação de riscos, além de analisar suas probabilidades de ocorrência e consequências. A avaliação de riscos de segurança da informação deve ser um processo formal e produzir “resultados consistentes, válidos e comparáveis” (cláusula 6.1.2.b). Além disso, o processo deve ser periodicamente revisado e monitorado.

O framework COBIT 2019 também trata do tema. O objetivo “APO12 - Risco Gerenciado” de seu domínio “Alinhar, Planejar e Organizar” (APO) contém práticas relacionadas à coleta e análise de dados de riscos, manutenção de um perfil de risco e ações para a comunicação e resposta a riscos relacionados a tecnologia da informação. O COBIT 2019 descreve as atividades relacionadas a cada prática, assim como os responsáveis por suas execuções.

Há diversas abordagens à gestão de riscos de segurança da informação aderentes às normas aludidas. De modo geral, uma organização deve construir um inventário de seus ativos de informação e identificar ameaças e vulnerabilidades inerentes a eles. Avalia-se, a partir dessas informações, o impacto causado pela exploração de uma ameaça ou vulnerabilidade na disponibilidade, confidencialidade e integridade dos ativos atingidos (cláusulas 6.1.2.d e 6.1.2.e da norma 27001:2022).

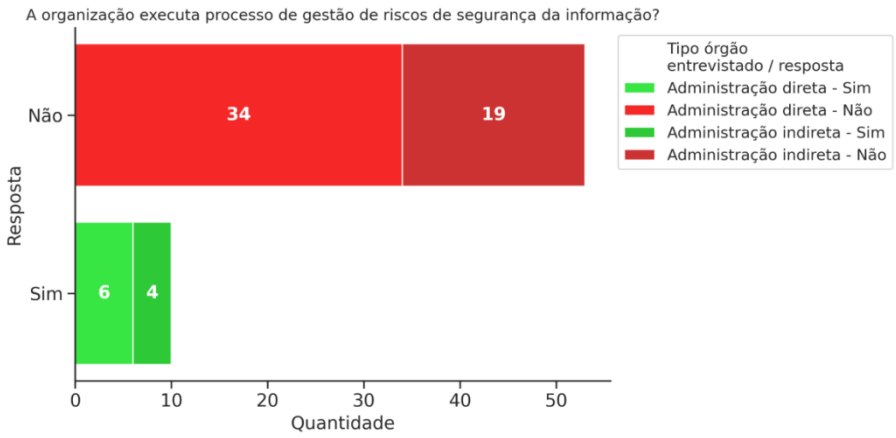
O possível dano à organização deve ser tratado em um processo de tratamento de risco (cláusula 6.1.3), onde se definem as opções para o tratamento de riscos de segurança da informação e os controles necessários para implementá-las.

Para avaliar a maturidade dos órgãos selecionados frente às boas práticas da norma 27001:2022, foram solicitadas informações acerca da formalização e abrangência de seus processos de gestão de riscos, o controle exercido sobre seus ativos de tecnologia da informação e o acesso concedido a eles. As respostas obtidas encontram-se delineadas nas seções abaixo.

Na seção específica sobre o tema no questionário aplicado, inquiriu-se acerca da existência e características do processo de Gestão de Riscos existente nos órgãos respondentes.

Na primeira questão, ***"A organização executa processo de gestão de riscos de segurança da informação?"***, apenas 10 órgãos afirmaram possuí-lo (Agência de Fomento do RN S/A, Departamento Estadual de Trânsito, Instituto de Previdência dos Servidores do RN, Controladoria Geral do Estado, Universidade do Estado do Rio Grande do Norte, Secretaria de Estado da Administração, Departamento Estadual de Imprensa, Hospital Maria Alice Fernandes, Tribunal de Justiça e Escola da Magistratura do RN), conforme se vê na Figura 36. Esses órgãos representam 15,87% do conjunto de respostas.

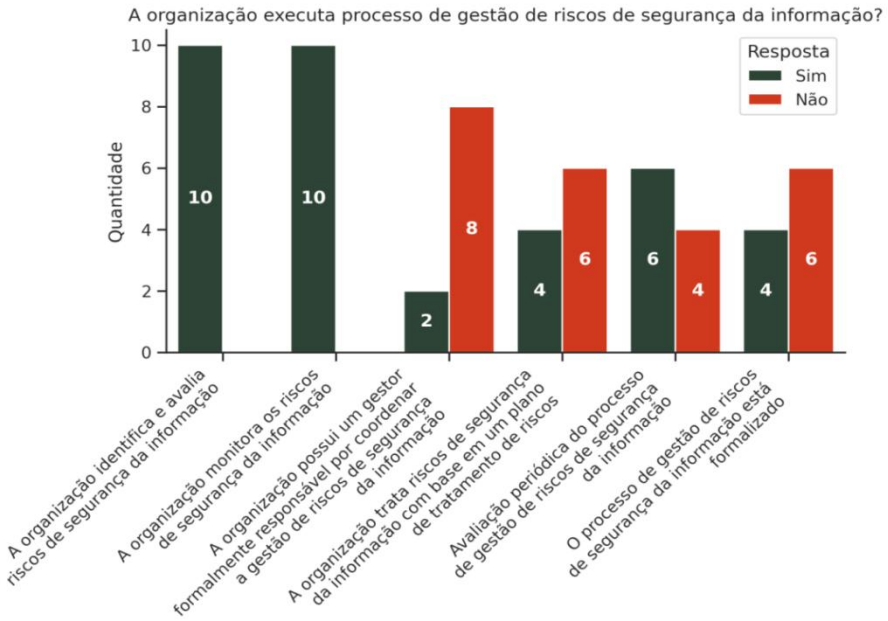
Figura 36 - Processo de Gestão de Riscos de Segurança da Informação



Conforme esperado, todos os órgãos que executam processos de gestão de riscos responderam positivamente às questões ***"A organização identifica e avalia riscos de segurança da informação?"*** e ***"A organização monitora os riscos de segurança da informação?"***. Todavia, o tratamento adequado só é realizado por 4 desses órgãos (respostas positivas para as perguntas ***"A organização trata riscos de segurança da informação com base em um plano de tratamento de riscos?"*** e ***"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)?"***. No tocante à avaliação periódica do processo de Gestão de Riscos, seis órgãos afirmaram realizá-la. Em apenas dois órgãos (Instituto de Previdência dos Servidores do RN e Hospital Maria Alice

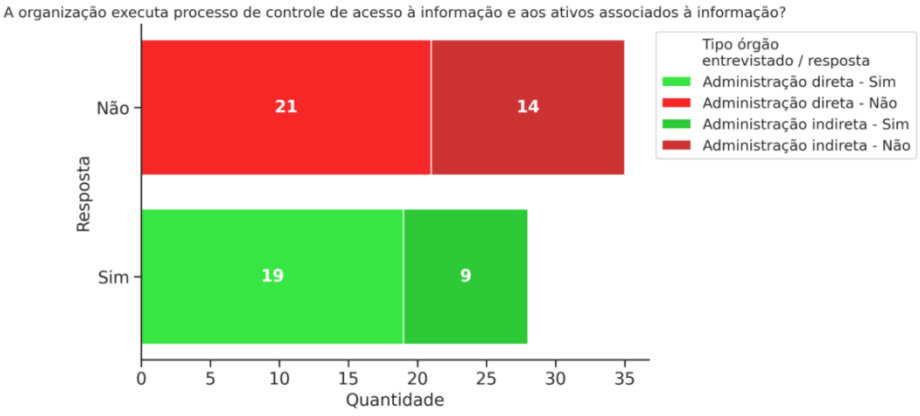
Fernandes) há um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação. A Figura 37 ilustra a situação dos processos de gestão de riscos encontrados nos participantes do levantamento que declararam executar processo de gestão de riscos de segurança da informação.

Figura 37 - Processo de Gestão de Riscos de Segurança da Informação



Segundo a norma ISO 27002:2022, os riscos de segurança de tecnologia da informação são modificados pela criação de mecanismos de controle de acesso. O questionário aplicado solicitou informações acerca da implementação de controles dessa natureza. A Figura 38 apresenta o resumo das respostas enviadas.

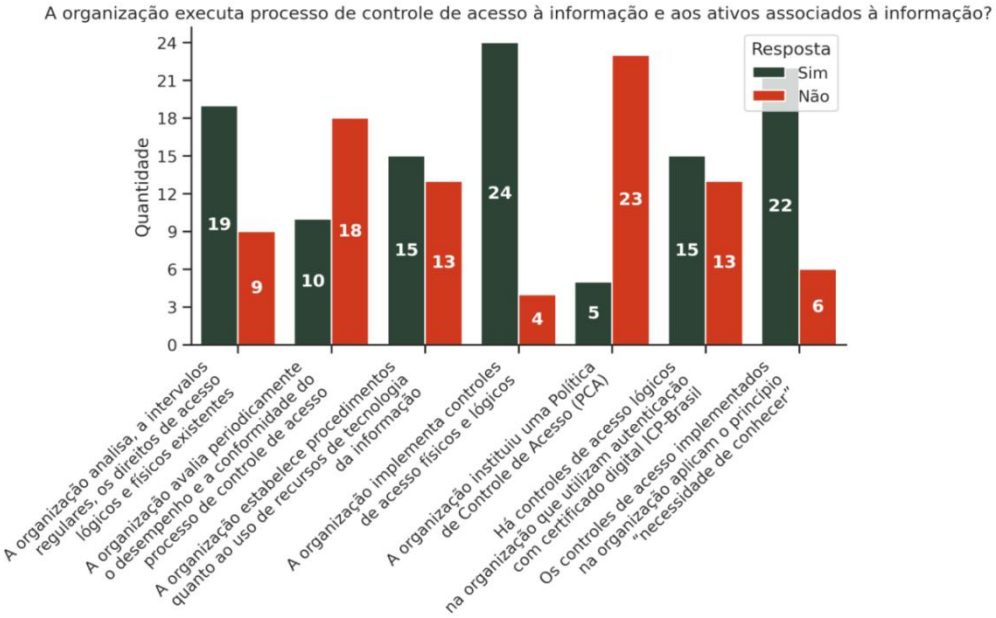
Figura 38 - Processo de Controle de Acesso à Informação e aos Ativos Associados



Um total de 44% dos órgãos participantes informou realizar medidas de controle de acesso a seus ativos de informação (28 respostas positivas). A natureza e abrangência desse

controle foram aferidas por meio de subquestões associadas ao tema. O resultado agrupado destas pode ser visualizado na Figura 39.

Figura 39 - Detalhamento do Processo de Controle de Acesso à Informação e aos Ativos Associados



Percebe-se uma predominância na implantação de controles de acesso físico e lógico (apenas 4 responderam negativamente à pergunta ***"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?"***).

Outros aspectos comumente presentes nos processos de controle de acesso identificados foram a aplicação do princípio da necessidade de conhecer e o estabelecimento de termos de uso de tecnologia da informação (19 respostas positivas para a pergunta ***"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?"*** e 18 respostas positivas para ***"A organização estabelece procedimentos quanto ao uso de recursos de tecnologia da informação (Termo de Responsabilidade/Compromisso)?"***).

Somente 5 órgãos responderam que instituíram formalmente uma Política de Controle de Acesso (Agência de Fomento do RN S/A, Instituto de Previdência dos Servidores do RN, Departamento Estadual de Imprensa, Secretaria de Estado do Planejamento e das Finanças e Empresa Potiguar de Promoção Turística S/A).

2.2.7.Gestão de continuidade de serviços de tecnologia da informação

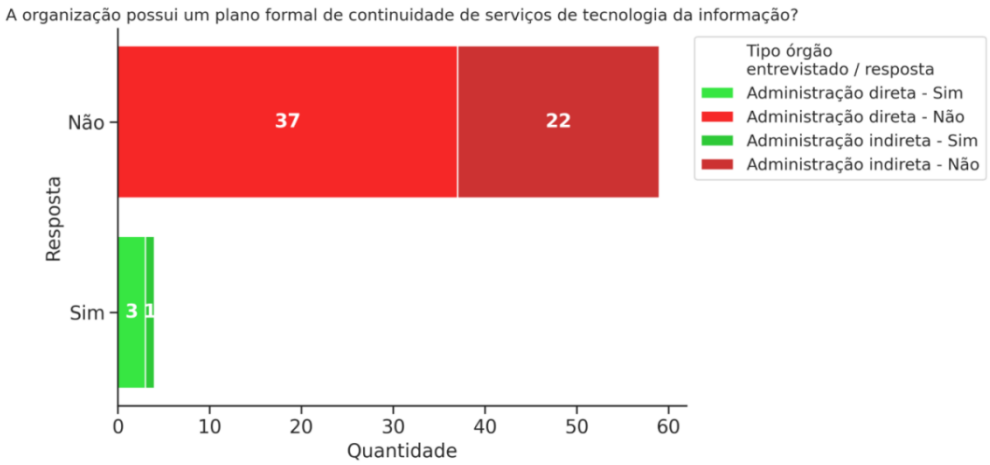
A norma ISO 22301 trata de Sistemas de Gestão de Continuidade. De modo análogo aos Sistemas de Gestão de Segurança da Informação e Sistemas de Gestão de Riscos, deve-se conhecer o contexto da organização e avaliar seus riscos para então formular as estratégias e soluções de continuidade. A norma traz também diretrizes para a construção de Planos e Procedimentos de Continuidade.

De modo sucinto, o Processo de Gestão de Continuidade de Serviços de TI tem por objetivo planejar e implantar medidas de redução de riscos e de recuperação de serviços em caso de incidentes. Seu escopo se limita a eventos em caráter de desastre. Periodicamente se reavalia os riscos do ambiente, através da análise do contexto atual identificando alterações na organização, seja na parte de TI ou na área finalística, para identificar novas ameaças. Simulações dos planos de recuperação são elaboradas e executadas a fim de garantir que o processo está íntegro e com baixo risco de falhas. Sempre que algum desastre de fato ocorre, o plano de recuperação deve entrar em ação para cumprir as etapas de recuperação. Neste processo não se trabalha com eventos menores, para isso outros processos são mais apropriados (por exemplo, gestão de incidentes).

As questões do questionário concernentes a esse tema são apresentadas nas seções que seguem.

Neste tópico do questionário inquiriu-se acerca da existência de um plano de continuidade de serviços no âmbito dos órgãos entrevistados (Figura 40). Somente 4 órgãos afirmaram possuí-lo: Agência de Fomento do RN S/A, Defensoria Pública Geral do Estado, Tribunal de Justiça e a Escola da Magistratura do RN.

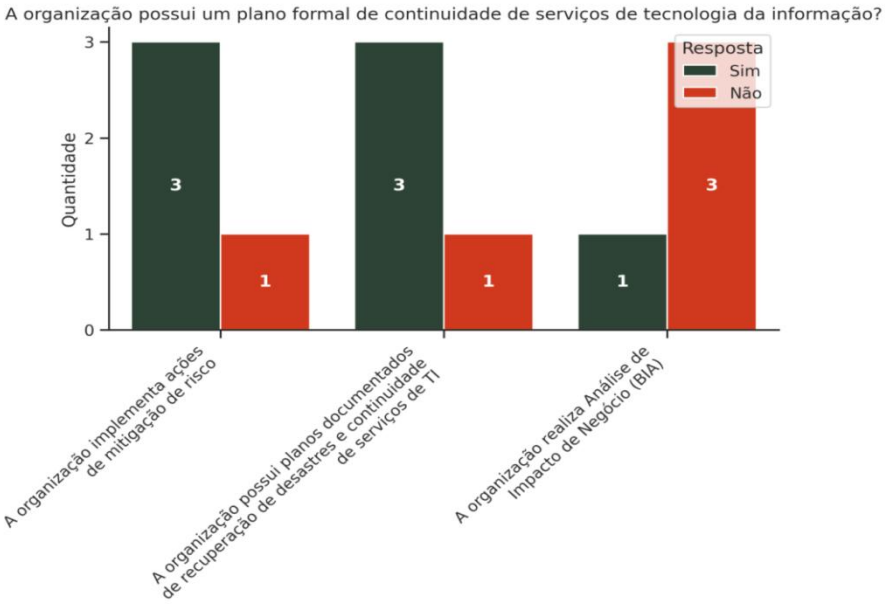
Figura 40 - Plano Formal de Continuidade de Serviços de Tecnologia da Informação



Em relação à mitigação de risco e planos de recuperação de desastres e continuidade de serviços, aspectos comuns aos Planos de Continuidade de Serviços de Tecnologia da Informação, somente a Defensoria Pública Geral do Estado respondeu que não executa ações com esses objetivos. Por outro lado, no tocante à Análise de Impacto de Negócio

(Business Impact Analysis ou BIA), apenas a Agência de Fomento do RN S/A a realiza. O gráfico a seguir (Figura 41) apresenta as respostas obtidas.

Figura 41 - Detalhamento do Plano Formal de Continuidade de Serviços de Tecnologia da Informação



2.2.8.Processo de software

Um processo de desenvolvimento de software é um conjunto de atividades, parcialmente ordenadas, com a finalidade de obter um produto de software. É estudado dentro da área de Engenharia de Software, sendo considerado um dos principais mecanismos para se obter software de qualidade e cumprir corretamente os contratos de desenvolvimento e uma das respostas técnicas adequadas para reduzir riscos inerentes ao desenvolvimento de um sistema. Desse modo, o levantamento realizado nessa ação do TCE-RN considerou relevante avaliar o nível de maturidade dos órgãos considerando o aspecto de processo de desenvolvimento de software.

Acerca do tema, o Acórdão 1.558/2003-TCU-Plenário versa: *"ACORDAM os Ministros do Tribunal de Contas da União, reunidos em Sessão Plenária, em determinar à CGSG/MDIC com fulcro no art. 71, IX, da Constituição Federal que: ... faça com que os trabalhos de elaboração e implantação de sistemas de software solicitados pelo Ministério a empresas contratadas sejam precedidos de planejamento detalhado, estabelecendo, com base em estudos prévios e fundamentados nas necessidades dos usuários, as especificações técnicas desses sistemas, de forma que seu desenvolvimento não sofra atraso ou solução de continuidade;"*.

Esse Acórdão mostra a importância da adoção de um processo de software aceito no mercado que reduza os riscos quando a organização pretende contratar uma empresa ou desenvolver seus próprios sistemas. Dessa forma, a ISO/IEC 12207 é uma norma que define processo de Engenharia de Software, atividades e tarefas que são associados com

os processos do ciclo de vida do software desde sua concepção até a retirada/descontinuação do software.

A norma internacional ISO/IEC 12207, usada como base de elaboração dessa seção do levantamento, tem como objetivo principal estabelecer uma estrutura comum para os processos de ciclo de vida e de desenvolvimento de softwares visando ajudar as organizações a compreenderem todos os componentes presentes na aquisição, desenvolvimento e fornecimento de software e, assim, conseguirem firmar contratos e executarem projetos de forma mais eficaz. Para isso é necessário que compradores, fornecedores, desenvolvedores, mantenedores, operadores, gerentes e técnicos envolvidos no desenvolvimento de software usem uma linguagem/framework comum.

Outra fonte de informações importante foi o MPSBR (Melhoria do Processo de Software Brasileiro), um programa da Softex com apoio do Ministério da Ciência, Tecnologia e Inovação (MCTI) que teve início em dezembro de 2003. Este programa tem como objetivo melhorar a capacidade de desenvolvimento de software, serviços e as práticas de gestão de RH na indústria de TI. A área de Qualidade da Softex é responsável por apoiar a inserção da cultura da qualidade de software e serviços, principalmente nas micro, pequenas e médias organizações, evidenciando a contribuição tanto para a melhoria de processos e do desempenho nos negócios quanto para a alavancagem da inovação, tornando-as mais competitivas.

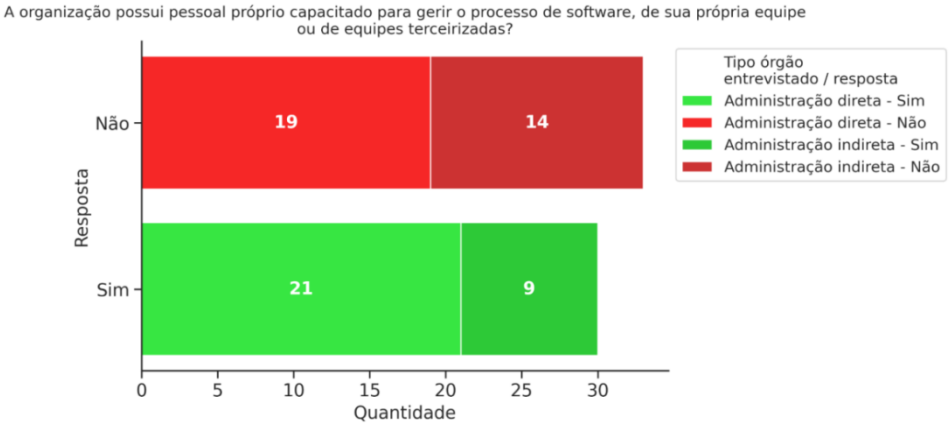
Para verificar a adesão a essas normas pelas instituições avaliadas, se faz necessário entender os seus respectivos processos de software.

Considerando tudo isso, ficou decidido solicitar informações aos jurisdicionados envolvidos neste levantamento em busca das respostas para a seguinte questão: ***A organização executa processo de software?***

Para identificar a existência de processo de software, bem como o seu nível de detalhamento, foram elaboradas perguntas exploratórias aos órgãos participantes. A primeira pergunta foi: ***"A organização possui pessoal próprio capacitado para gerir o processo de software, de sua própria equipe ou de equipes terceirizadas?"***.

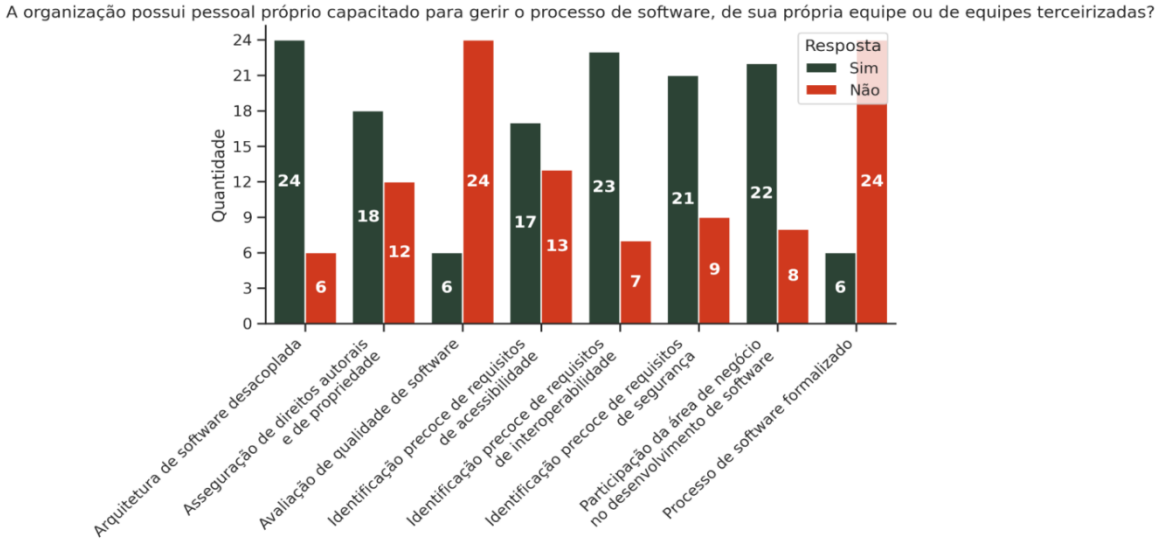
A Figura 42 demonstra que 30 instituições afirmaram possuir pessoal próprio capacitado para gerir o processo de software e 33 declararam não possuir.

Figura 42 - Possui pessoal próprio capacitado para gerir o processo de software



Para identificar o nível de aderência do processo de software utilizado pelos jurisdicionados às boas práticas de engenharia de software, algumas questões foram levantadas e suas respostas estão presentes no gráfico representado pela Figura 43 a seguir:

Figura 43 - Detalhes sobre pessoal próprio capacitado para gerir o processo de software



Como pode ser observado, quase todos os jurisdicionados que afirmam possuir pessoal próprio capacitado para gerir o processo de software informam que usam uma arquitetura de software desacoplada, fazem identificação precoce de requisitos de segurança e fomentam a participação da área de negócio no desenvolvimento do sistema. Também é possível observar que apenas 6 instituições afirmaram que fazem a avaliação da qualidade de software e que possuem o processo formalizado.

2.2.9.Gestão de projetos de Tecnologia da Informação

A gestão de projetos de TI impacta diretamente no sucesso de ações e projetos de tecnologia, como sistemas de informação e soluções de infraestrutura de tecnologia. Projetos dessa natureza possuem riscos conhecidos, como o aumento dos custos inicialmente previstos e a dilação do prazo de entrega do produto almejado. Não raro, um projeto fracassa no alcance de seus objetivos e na implantação de serviços necessários à organização, comprometendo ações institucionais. Nesse sentido, a gestão de projetos de TI foi tratada por este questionário, com o objetivo de identificar o nível de maturidade dos órgãos nesse aspecto. A questão "***A organização gerencia projetos de Tecnologia da Informação?"*** agrupa as informações solicitadas sobre o tema.

Por oportuno, cabe destacar que o assunto foi objeto de atenção do TCU no Acórdão 1.233/2012-TCU-Plenário, que recomendou a elaboração de um modelo de estrutura de gerenciamento de projetos e a formalização de um processo de gerenciamento de projetos, observando as boas práticas sobre o tema, como o guia Project Management Body of Knowledge (PMBOK).

Como referência para elaboração das questões deste levantamento, foi utilizado também o Cobit 5, que apresenta o processo 'BAI01 – Gerenciar Programas e Projetos' com o objetivo de realizar benefício de negócio e reduzir o risco de atrasos inesperados, custos e valores extrapolados, por meio de melhoria da comunicação e do envolvimento do negócio com os usuários finais, assegurando o valor e a qualidade dos projetos entregues e maximizando sua contribuição para o portfólio de serviços e investimentos. Também foi utilizada a ISO 21500:2012, um padrão internacional desenvolvido pela Organização Internacional de Normalização a partir de 2007 e lançado em 2012. A norma destina-se a fornecer orientação genérica, explicar princípios fundamentais e que constitui uma boa prática na gestão de projetos.

A elaboração da norma ISO 21500 foi liderada pelo comitê técnico ISO/PC 236 da *American National Standards Institute* (ANSI). O grupo é responsável pela criação de quatro normas referentes à gestão de projetos de TI, todas alinhadas aos padrões da *Project Management Institute (*PMI). A norma ISO 21500 foi planejada para ser a primeira de uma família de padrões sobre o tema. Ademais, a aludida norma foi desenhada para alinhar-se a outras normas congêneres, a saber: ISO 10006:2003 (Sistemas de Gestão da Qualidade - Diretrizes para a gestão da qualidade em projetos), ISO 10007:2003 (Sistemas de Gestão da Qualidade - Diretrizes para o gerenciamento de configuração) e ISO 31000:2009 (Gestão de Riscos).

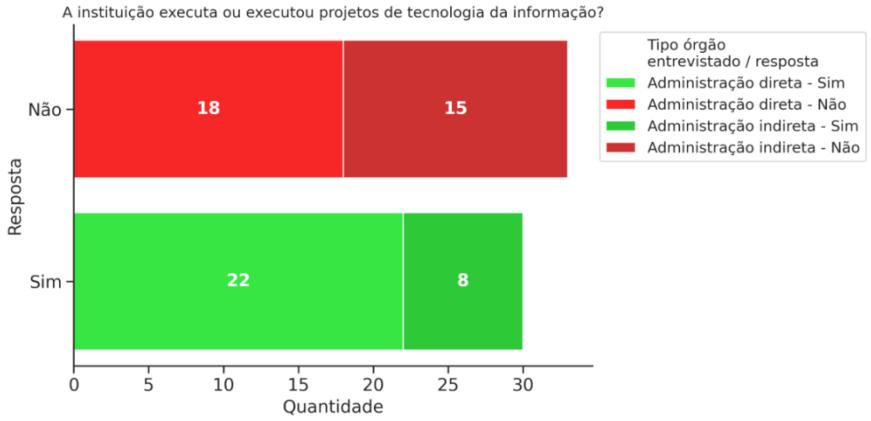
Com o intuito de verificar o alinhamento das instituições analisadas aos padrões internacionais de gestão de projeto de TI, a seguinte questão foi proposta: ***"Qual o nível de maturidade dessas organizações quanto à execução de processo de gestão de projetos de Tecnologia da Informação"***.

Para responder a essa questão, se fez necessário analisar as questões a seguir:

a. A organização executa projetos de TI?
b. Se a organização gerencia o escopo dos projetos de TI?
c. Se a organização gerencia o custo dos projetos de TI?
d. Se a organização gerencia os recursos dos projetos de TI?
e. Se a organização gerencia o prazo dos projetos de TI?
f. Se a organização gerencia o risco dos projetos de TI?

Primeiramente, deve-se identificar quais das organizações executam projetos de TI, em uma unidade interna própria. Só faz sentido avaliar a gestão dos projetos de TI nas organizações que realizam esses projetos.

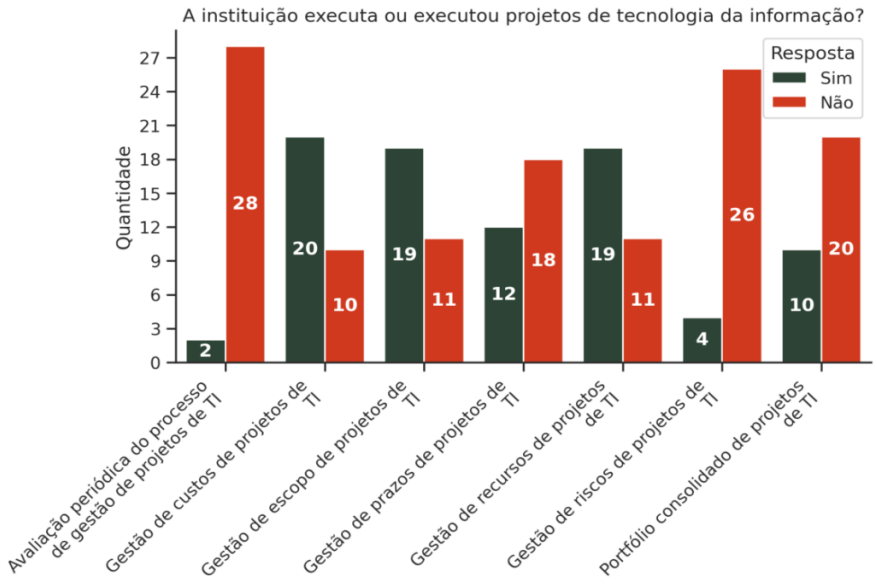
Figura 44 - Executa projeto de Tecnologia da Informação



A Figura 44 apresenta o resultado das informações obtidas acerca da execução de projetos de TI pelos jurisdicionados. De todos os avaliados, 30 declararam ter executado projetos de TI e 33 afirmam que não.

Para as instituições que executam projetos de TI, foram elaboradas questões para avaliar como está a qualidade da gestão desses projetos, com base na ISO 21500 e no PMBOK. O resultado pode ser visto no gráfico abaixo.

Figura 45 - Gestão dos projetos de TI



Percebe-se que a maior parte das organizações (quase todas) não faz avaliação periódica de seus processos, não trabalham a gestão de riscos em seus projetos e não possuem portfólio consolidado dos projetos de TI (apenas 2, 4 e 10 respostas positivas, respectivamente). Por outro lado, percebe-se um avanço na gestão de custo, escopo e recursos dos projetos. Todavia, a maioria não realiza a gestão de prazo, e sabe-se que não é possível realizar gestão de custo sem gerir prazos.

Seguindo a análise sobre o processo de gestão das organizações que executam projetos, a Figura 45 mostra que a maior parte faz a gestão de escopo dos projetos de TI (19 jurisdicionados), sendo que 12 afirmaram utilizar um processo conhecido como ferramenta e apenas duas formalizam esse processo.

Figura 46 - Gestão de escopo dos projetos de TI

Das 19 instituições que afirmaram fazer a gestão de escopo, 12 informaram utilizar um processo conhecido (Figura 46), mas apenas 2 formalizaram esse processo.

Figura 47 - Gestão de custos dos projetos de TI

Avaliando o resultado sobre o uso do processo de gestão de custos, a Figura 47 mostra que das 20 instituições fazem a gestão de custos, 12 utilizam um processo conhecido, 6 utilizam alguma técnica de centro de custo e nenhuma formalizaram esse processo.

Figura 48 - Gestão de cumprimento de prazos dos projetos de TI

Para fazer uma análise mais aprofundada das organizações que gerenciam o cumprimento de prazos de seus projetos de TI, estas organizações tiveram que responder a perguntas sobre como essa gestão é feita (Figura 48). Analisando as respostas, percebe-se que apenas 3 instituições afirmam formalizar seus processos e 7 utilizam técnicas para gestão de prazos.

2.2.10. Sistemas Eletrônicos Informacionais Relevantes

A oferta dos serviços públicos, bem como o alcance dos objetivos institucionais da administração pública, está muitas vezes relacionada ou é fortemente dependente do pleno funcionamento de sistemas eletrônicos informacionais. A interrupção do funcionamento desses sistemas pode gerar relevantes impactos negativos à sociedade, tais como: perda de vidas humanas, danos à saúde, danos financeiros ou à imagem do ente governamental e até mesmo a parada de serviços essenciais.

Considerando a importância desses ativos de TI, necessário se faz planejar auditorias, tanto por parte dos jurisdicionados como do Tribunal de Contas. Essas fiscalizações podem ter como objetivo avaliar a segurança desses ativos, os custos envolvidos e os riscos inerentes ao seu funcionamento. Além disso, uma fiscalização deve revisar e avaliar os controles de um sistema para determinar se este atinge os objetivos esperados, mantém a integridade dos dados, cumpre as regulamentações pertinentes e utiliza eficientemente os recursos disponíveis, mantendo bons níveis de usabilidade e satisfação dos usuários.

Nesse cenário, é mister obter informações com vistas a mapear os sistemas de maior relevância sob a gestão de seus jurisdicionados. Esse mapeamento possibilitará a elaboração da melhor estratégia de atuação das equipes de fiscalização do Tribunal no que se refere às auditorias de sistemas a serem realizadas em Planos de Fiscalização futuros.

Para tanto, foi solicitado aos participantes da pesquisa o preenchimento de planilha onde foram informados até cinco sistemas relevantes ou essenciais, na opinião do órgão respondente. Para cada sistema informado, o gestor indicou os respectivos impactos e vulnerabilidades existentes a partir de um rol de situações elencadas na planilha, conforme tabelas 1, 2 e 3 a seguir:

Tabela 1 - Relação de impactos

Relação de IMPACTOS: para responder as questões do grupo Impacto, considere se o item representa uma possível consequência de um incidente de segurança da informação (indisponibilidade ou comprometimento da integridade ou da confidencialidade) ou de uma falha decorrente de defeitos do sistema.	
1. Perda de vidas humanas ou danos graves para a saúde humana.	( ) Sim ( ) Não
2. Danos ambientais graves.	( ) Sim ( ) Não
3. Degradação significativa na prestação de serviço essencial ao cidadão.	( ) Sim ( ) Não
3.1 Caso SIM, informe o serviço impactado.	( ) Sim ( ) Não
3.2 Caso SIM, informe a abrangência do serviço.	( ) Sim ( ) Não
4. Danos financeiros significativos à Administração Pública (própria organização ou outro órgão/entidade) ou aos cidadãos.	( ) Sim ( ) Não
5. Danos significativos à reputação ou à credibilidade da organização.	( ) Sim ( ) Não
6. Impedimento do funcionamento de atividade finalística da organização.	( ) Sim ( ) Não
7. Degradação significativa da produtividade dos servidores/funcionários da organização que utilizam ou dependem do sistema.	( ) Sim ( ) Não
8. Degradação significativa do funcionamento de atividades ou processos com características multi-institucionais e que envolvam diferentes esferas da administração ou dos poderes.	( ) Sim ( ) Não
10. Exposição indevida de dados pessoais sensíveis e que possa causar dano ao titular.	( ) Sim ( ) Não
11. Efeito negativo na execução da política econômica do Estado.	( ) Sim ( ) Não
12. Degradação significativa do funcionamento de atividades ou serviços relacionados às infraestruturas críticas do Estado.	( ) Sim ( ) Não

Tabela 2 - Relação de vulnerabilidades

Relação de VULNERABILIDADES: para responder as questões deste grupo, considere se o item representa uma vulnerabilidade do sistema ou do ambiente em que ele opera de ter sua disponibilidade, integridade ou confidencialidade comprometida.

13. O sistema está coberto por solução de continuidade de serviços de TI (alta disponibilidade, recuperação de desastres e planos de contingência)?	( ) Sim ( ) Não
14. O sistema é suportado por equipe de respostas a incidentes?	( ) Sim ( ) Não
15. As vulnerabilidades e os riscos de TI relacionados ao sistema e à infraestrutura que o sustenta estão identificados, classificados, analisados e tratados?	( ) Sim ( ) Não
16. O sistema possui tecnologia obsoleta ou desatualizada (hardware e software)?	( ) Sim ( ) Não
17. O sistema está hospedado em sala segura ou sala cofre?	( ) Sim ( ) Não
18. O sistema ou a infraestrutura que o suporta estão cobertos por processo de gestão de patches de segurança?	( ) Sim ( ) Não
19. São realizados testes de invasão ou auditorias de segurança no sistema ou na infraestrutura que o sustenta?	( ) Sim ( ) Não
20. O sistema é alvo de frequentes ataques?	( ) Sim ( ) Não
21. O sistema possui controles para a proteção dos dados e do código (criptografia, backup, controle de acesso, trilhas de auditoria, etc.)?	( ) Sim ( ) Não
22. O sistema e a infraestrutura que o suporta estão incluídos em processo de gestão de ativos de TI?	( ) Sim ( ) Não

Tabela 3 - Outras informações

Outras informações:	
23. Custo anual de sustentação do sistema (correção, adaptação e evolução dos sistemas) - Valor empenhado em 2023:	
24. Local de hospedagem do sistema:	( ) Datacenter próprio ( ) Datacenter de terceiros ( ) Modelo nuvem
24.1 Se local diferente de "Próprio", indique o responsável pela hospedagem (Cotic, Google, Amazon, etc.):	

O resultado do levantamento apresentou a existência de 101 sistemas informacionais considerados relevantes ou essenciais pelos gestores públicos envolvidos. Dentre esses sistemas, merecem uma atenção diferenciada aqueles que foram classificados pelos gestores por possuir relação de impacto com perdas de vidas humanas ou dano grave para saúde humana, em casos de incidentes de segurança da informação ou falha decorrente de defeitos do sistema. Esses sistemas estão relacionados na Tabela 4.

Tabela 4 - Sistemas críticos - relação de impacto: perda de vidas humanas ou dano grave para a saúde humana

Jurisdicionado	Nome do Sistema	Descrição/Finalidade do Sistema
Instituto de Gestão das Águas do Estado do Rio Grande do Norte	Sistema Integrado de Gestão de Águas do Rio Grande do Norte	Gestão do uso da água do RN
Hospital Monselhor Walfredo Gurgel	Salux	Sistema de Gerenciamento Hospitalar
Hospital Monselhor Walfredo Gurgel	Telepacs	Sistema de Armazenamento de Imagens Médicas e Laudos
Secretaria da Segurança Pública e da Defesa Social	Nutanix Prism Central	Orquestração da infraestrutura de Virtualização de Hardware
Secretaria da Segurança Pública e da Defesa Social	Central Telefônica Call Center	Gerenciamento de chamadas telefônicas para centrais de emergência 190
Secretaria da Segurança Pública e da Defesa Social	CAD RN	Gerenciamento de ocorrências e despachos policiais e de emergências
Instituto de Defesa e Inspeção Agropecuária	SIDIARN	CONTROLE E GESTÃO DE ATIVIDADES DE DEFESA AGROPECUÁRIA DO ESTADO DO RN
Polícia Civil	SISPOL	informações funcionais do servidor policial
Polícia Civil	INFOSEG	Banco nacional de Informações relacionadas com a Segurança Pública

Outra informação coletada que merece destaque é a identificação do sistema relevante de maior custo anual de sustentação (correção, adaptação e evolução do sistema). Essa situação foi caracterizada no Sistema Integrado de Gestão da Educação - SIGEDUC, gerenciado pela Secretaria de Estado da Educação, da Cultura, do Esporte e do Lazer, com custo anual de aproximadamente R$ 2,5 milhões de reais.

Por fim, importante se faz destacar que a Secretaria de Estado da Saúde Pública (SESAP), a Companhia de Águas e Esgotos do RN (CAERN), a Fundação Djalma Marinho (FDM) e o Hospital Regional Tarcísio Maia (HRTM) não enviaram as informações solicitadas. Além disso, alguns jurisdicionados enviaram a informação incompleta ou em desacordo com a planilha modelo, impossibilitando a identificação e/ou a classificação dos sistemas relevantes desses órgãos[2].

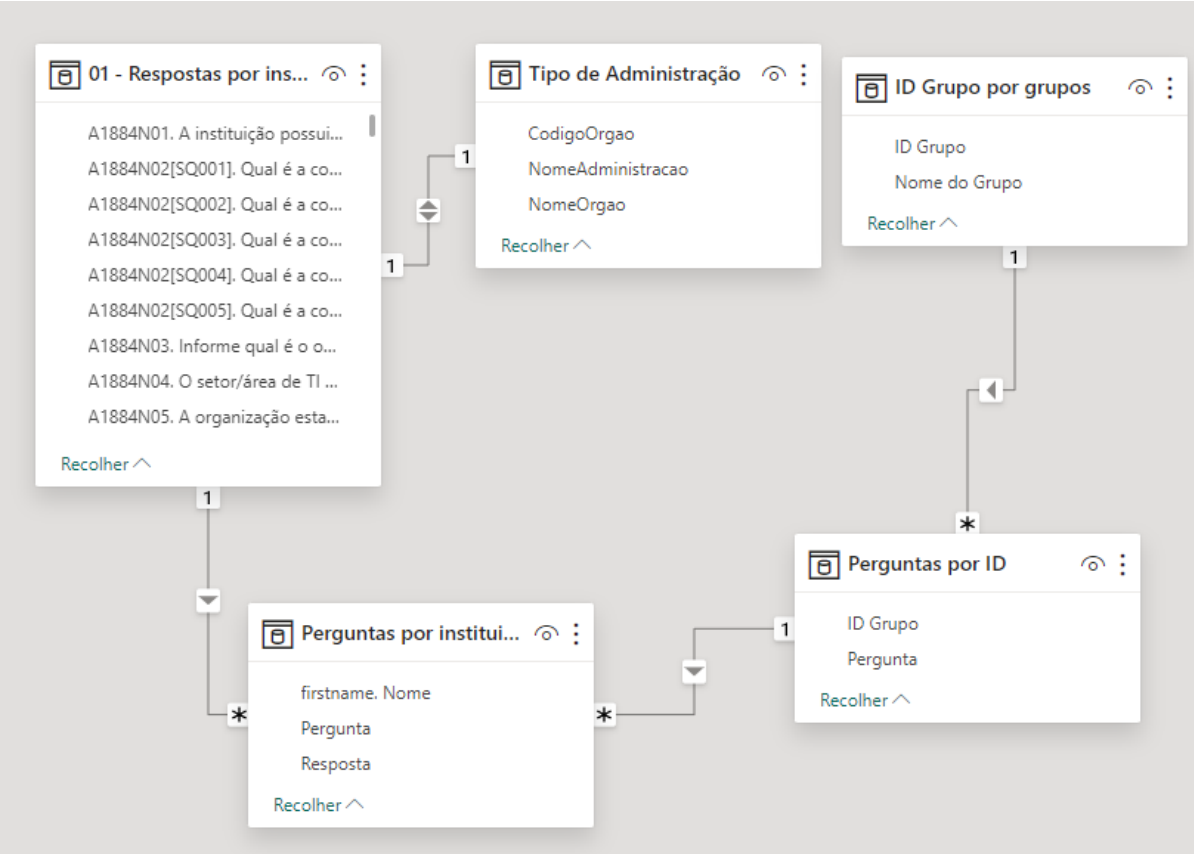
[2] Agência Reguladora de Serviços Públicos do RN (ARSEP); Controladoria Geral do Estado (CONTROL); Diretoria de Saúde da Policia Militar (DSPM); Empresa Gestora de Ativos do RN (EMGERN); Hospital Regional Doutor Cleodon Carlos de Andrade (HCCA); Hospital Regional Nelson Inácio dos Santos (HRNIS); Instituto de Desenvolvimento Sustentável e Meio Ambiente do RN (IDEMA); Instituto de Pesos E Medidas do RN (IPEM); Procuradoria Geral de Justiça (PGJ); Secretaria de Estado da Agricultura, da Pecuária e da Pesca (SAPE); Secretaria de Estado do desenvolvimento Econômico (SEDEC); Secretaria de

3.METODOLOGIA DE AVALIAÇÃO DE RISCOS

A partir dos dados coletados neste trabalho, foi desenvolvida uma metodologia de avaliação de riscos para representar, de forma quantificada, a maturidade da Governança de TI nos órgãos avaliados. A partir dessa metodologia foram construídos painéis para a visualização da métrica de risco.

Os dados utilizados foram extraídos da ferramenta LimeSurvey (software empregado para a criação do questionário eletrônico). Utilizou-se a linguagem de programação Python para o tratamento inicial dos dados. Realizada a transformação das informações, estas foram carregadas na ferramenta Microsoft PowerBI para a sua visualização (Figura 49).

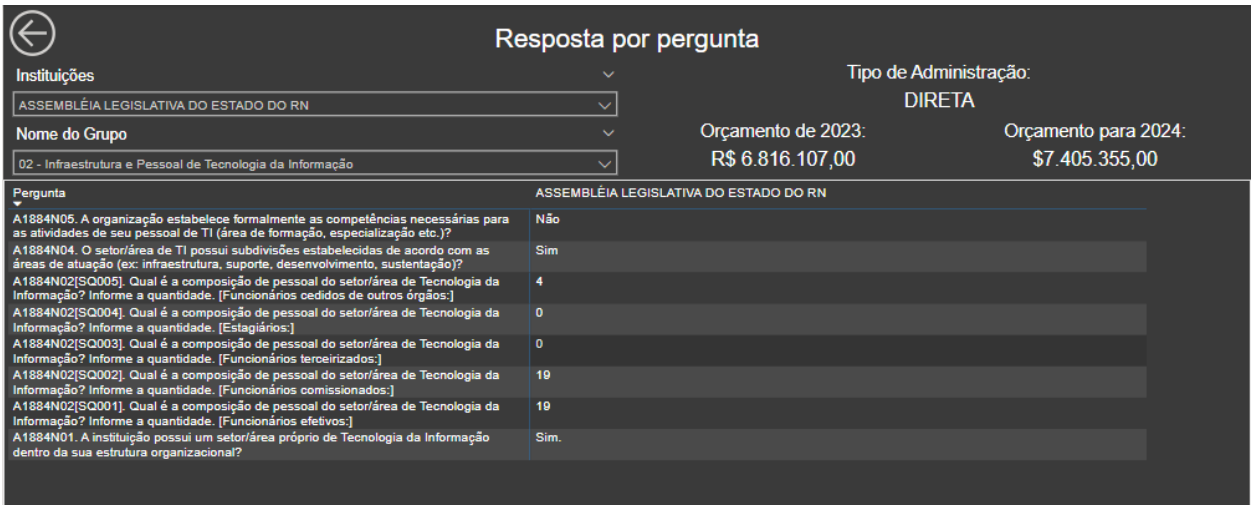
Figura 49 - Modelo Dimensional de Dados (Floco de Neve)



As informações foram separadas em dimensões abrangendo as questões aplicadas, seus grupos temáticos e os órgãos respondentes. Foram criados painéis para cada grupo de questões, conforme se vê na figura 50.

Estado das Mulheres, da Juventude, da Igualdade Racial e dos Direitos Humanos (SEMJIDH); Vice Governadoria (VICEGOV).

Figura 50 - Modelo Dimensional de Dados (Floco de Neve)



Atribuiu-se pontuação para cada questão concernente à adoção de normas e boas práticas (0 para respostas negativas, 1 para positivas). Itens que se dividem em questões derivadas tiveram seu cálculo subdividido de modo uniforme, sendo sua pontuação computada pela soma de suas pontuações subjacentes. Por exemplo, grupos de cinco subquestões tiveram pontuações de 0,2 por cada elemento, formando ao final a nota máxima de 1 para a questão. Foram definidos também pesos intermediários entre 0 e 1 para os casos onde haviam respostas variáveis entre sim e não (e.g. adoção de boas práticas sem evidências ou realização ocasional de procedimento). As figuras 51 e 52 demonstram os cálculos aqui descritos.

Figura 51 - Cálculos para respostas sim/não e com marcações múltiplas

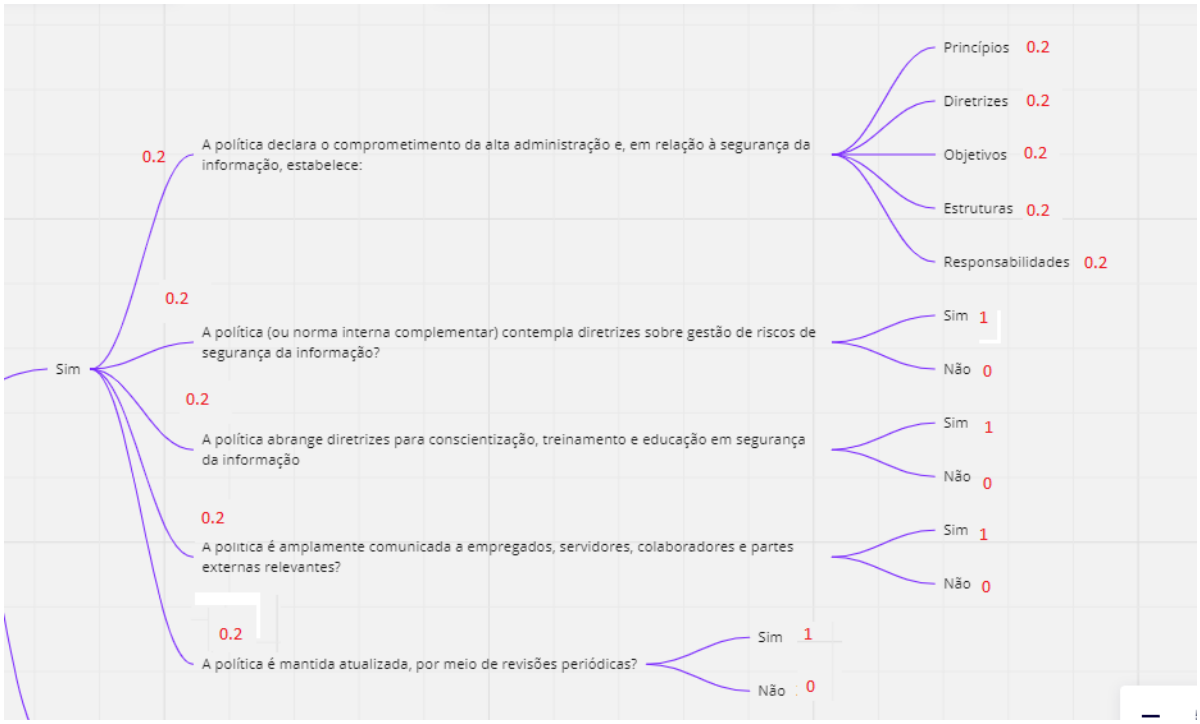
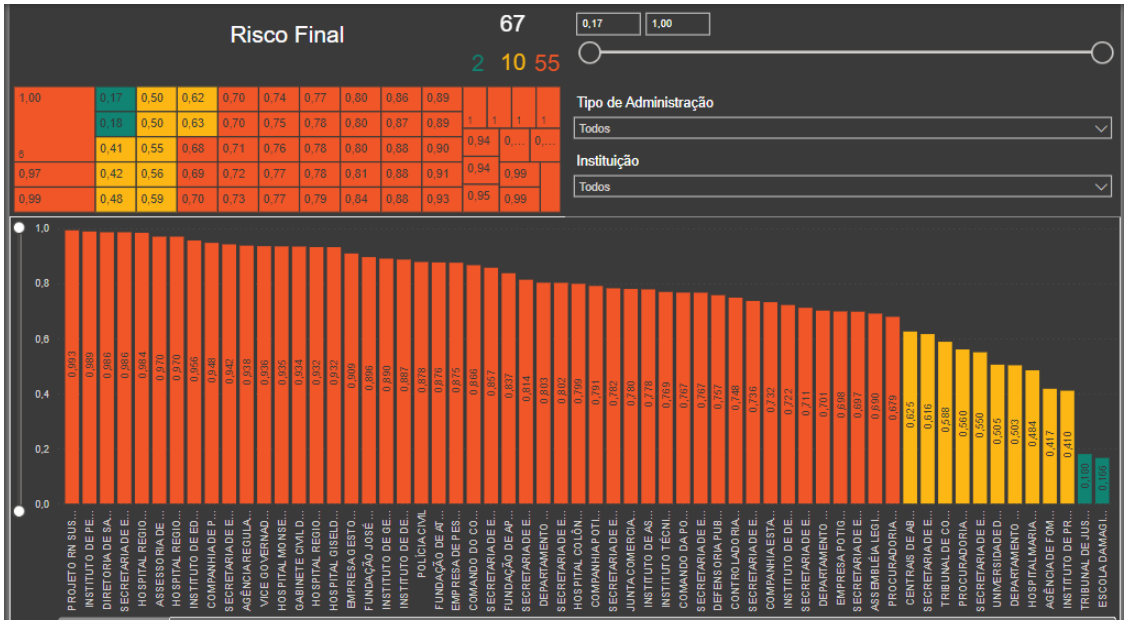


Figura 52 - Cálculos para respostas escalonadas e marcação múltiplas

Um índice de risco foi construído a partir da metodologia descrita. Seus resultados são apresentados no painel ilustrado na Figura 53. A aludida métrica varia entre 0 e 1, sendo os valores maiores referentes a riscos mais agudos. Níveis baixos de risco (valores abaixo de 0,33) são mostrados na cor verde, riscos médios aparecem em amarelo (valores entre 0,33

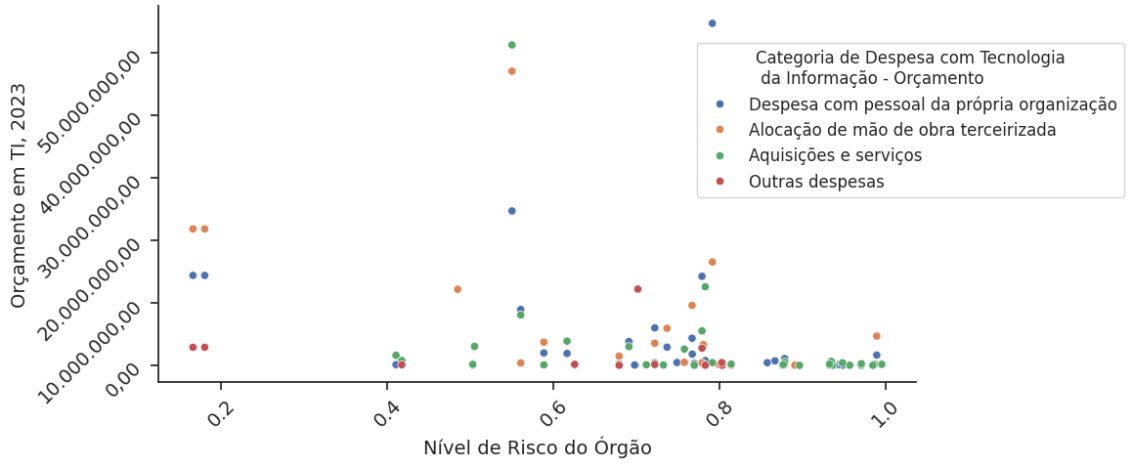
e 0,66) e a cor vermelha aponta as instituições que apresentam riscos elevados (valores acima de 0,66).

Figura 53 - Painel de Riscos com base nas respostas



Foram realizados testes de correlação estatística entre a medida elaborada e características dos órgãos participantes. O gráfico da Figura 54 mostra a distribuição dos níveis de risco aferidos nos órgãos e seus respectivos orçamentos para TI em 2023. Vê-se que não há ligação entre as duas informações. Uma regressão linear dos dois valores atesta que são completamente independentes (R^2 de 0,08).

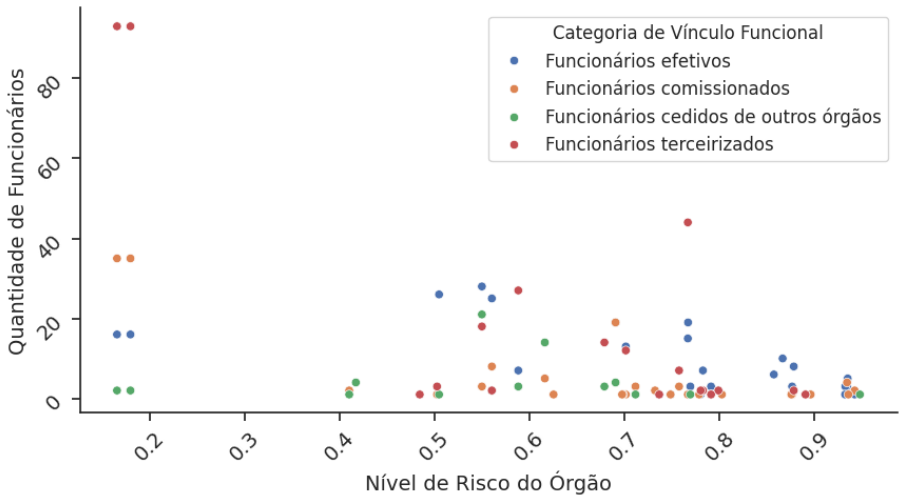
Figura 54 - Dispersão entre risco e orçamento



A mesma técnica de regressão linear foi aplicada para o nível de risco e a quantidade de funcionários em setores de TI. Esta apresentou um resultado ligeiramente mais significativo (R^2 de 0,45). Todavia, o coeficiente aferido não é suficiente para provar uma correlação

forte entre as duas variáveis. Deduz-se, portanto, que o porte de um setor de tecnologia da informação não determina a maturidade de sua governança. A Figura 55 apresenta a dispersão dos valores em comento.

Figura 55 - Dispersão entre Quantidade de funcionários e risco



4.CONCLUSÃO

As informações coletadas no presente levantamento possibilitaram a obtenção do conhecimento acerca da situação da Governança de TI nos órgãos da Administração Pública Estadual, identificando as suas potenciais fragilidades e os riscos associados à entrega de valor da área de TI das instituições envolvidas neste trabalho. Constatou-se um cenário de baixa adesão às principais normas e boas práticas concernentes ao tema, evidenciando a necessidade de melhoria da Governança de Tecnologia da Informação na grande maioria dos órgãos da APE.

O questionário aplicado buscou abranger 67 órgãos da administração direta e indireta da esfera estadual. Cumpre repisar que a Secretaria de Estado da Saúde Pública, a Companhia de Águas e Esgotos do RN, a Fundação Djalma Marinho e o Hospital Regional Tarcísio Maia não forneceram as informações solicitadas, sendo assim o mapeamento da situação da Governança de TI alcançou 63 jurisdicionados.

O orçamento somado dos participantes, em 2023, perfaz R$ 366.183.905,69. O montante expressivo destaca a importância da correta gestão desses recursos e sua fiscalização por parte dos órgãos de controle.

No âmbito da estrutura e pessoal de Tecnologia da Informação, verificou-se uma predominância de vínculos de terceirização nos quadros funcionais dos órgãos participantes. Essa terceirização não pode ser tratada, por si só, como algo negativo. No entanto, a falta de vínculo prolongado com a administração pode comprometer o alinhamento da TI com as estratégias da instituição. Sendo assim, é aconselhado que a

gestão da Tecnologia da Informação seja exercida por profissionais com forte vínculo institucional, ou seja, por servidores, preferencialmente efetivos, e capacitados para tal atribuição.

Um total de 24% dos respondentes estabeleceu formalmente as competências necessárias para as atividades de seu pessoal de TI (tais como área de formação, por exemplo). Some-se a isso a constatação de que somente 6% dos órgãos possuem um Plano de Tecnologia da Informação vigente e tem-se circunstâncias pouco condutoras a uma gestão racional das ações institucionais na área de TI, fato agravado pela estatística levantada de que apenas 13% dos participantes estabeleceram critérios para orientar a seleção e a priorização das iniciativas em Tecnologia da Informação. Esses dados podem indicar uma fragilidade em todo o processo de gestão da TI, indicando um risco a ser monitorado.

No tocante à gestão de serviços de TI, em que pese 51% dos órgãos terem respondido que realizam a gestão de mudanças em seus ativos de TI, apenas 13% elaboraram um catálogo de serviços de TI. Na mesma esteira, somente 17 órgãos (27% do universo de pesquisa) afirmaram gerenciar os Acordos de Níveis de Serviços de Tecnologia da Informação ofertados a seus usuários. A ausência de ANSs, que tem o condão de delinear metas claras para serviços contratados, dificulta a fiscalização das obrigações das partes contratadas e da entrega dos resultados almejados, resultando em risco de prejuízo ao Erário.

Uma parte considerável dos setores responsáveis pela Tecnologia da Informação na Administração Pública Estadual executa projetos para a construção de soluções na área (47,61% dos entrevistados). A maioria dos entrevistados que executam projetos afirmaram realizar gestão de custos (67% dos entrevistados), escopo e recursos (63% de respostas positivas para ambas as áreas). Todavia, somente 6% avaliam periodicamente seu processo de gestão de projetos e 13% gerenciam seus riscos. A deficiência observada nessas áreas pode ensejar o fracasso de projetos devido a fatores que, em uma gestão mais madura, poderiam ser previstos, mitigados e monitorados. E, como enfatizado pelas boas práticas, projetos fracassados traduzem-se em elevados danos financeiros.

Em relação aos projetos de TI que envolvem a codificação de uma solução, 47% dos órgãos inquiridos confirmaram possuir pessoal próprio para gerir processos de software. Esses produtos podem ser desenvolvidos por suas próprias equipes ou por equipes terceirizadas. Observou-se um cenário de razoável implementação das boas práticas na gestão de processo de software, com predominância de respostas positivas nas questões atinentes ao tema, excetuando-se a formalização do processo (verificada em apenas 20% dos casos) e a avaliação de qualidade do software produzido (também realizada por somente 20% do universo entrevistado).

Para avaliar a maturidade da Segurança da Informação dos entrevistados inquiriu-se, inicialmente, sobre a implantação de uma Política de Segurança da Informação. Somente 8 órgãos dispõem do documento. Além disso, apenas 3 desses 8 órgãos afirmaram que suas políticas abrangem diretrizes para a conscientização, treinamento e educação em segurança da informação. A norma ISO 27001 é clara quanto à necessidade de comunicação do conteúdo da política a todos os setores de uma instituição. Do mesmo

modo, a norma é explícita em relação à importância de se definir formalmente as responsabilidades referentes ao tema. Porém, verificou-se a existência de um gestor institucional de segurança da informação em meramente 5 órgãos e somente 2 participantes possuem um comitê de segurança da informação. A reduzida taxa de implementação desses requisitos formais pode prejudicar a capacidade de planejamento e execução de ações na área de Segurança da Informação, aumentando assim a probabilidade de ocorrência de incidentes de segurança.

Uma parte maior dos órgãos, 47,61% do universo de pesquisa, afirmou classificar e tratar as informações sob sua custódia. Todavia, a formalização do processo de classificação de informações e sua avaliação periódica foi observada em apenas 1 dos órgãos. Quanto ao processo de controle de acesso à informação, este foi implementado em 44% dos órgãos pesquisados. Assinale-se que a Lei Geral de Proteção de Dados traz, em seus Art. 23 e 24, regras para classificação da informação quanto ao grau e prazos de sigilo, atribuindo caráter de obrigação legal aos procedimentos destacados.

A gestão da segurança de recursos de processamento de informação é realizada por 21 dos 63 órgãos que participaram da pesquisa. Nos casos positivos, a maioria dos respondentes afirmaram realizar a maior parte das técnicas de segurança concernentes a este tópico.

A gestão de riscos de segurança da informação, por outro lado, ocorre tão somente em 10 órgãos. Há um gestor formalmente responsável pela área em apenas 2 órgãos. No que tange ao processo de gestão de incidentes de segurança da informação, também observou-se um baixo índice de execução (17% dos entrevistados). Infere-se desses números a possibilidade de ocorrência de falhas de segurança da informação não detectadas nos órgãos que não executam essas boas práticas. Por fim, há planos formais de continuidade de serviços em apenas 4 órgãos. Ou seja, em caso de ocorrência gravíssima de incidente, a maioria dos órgãos possuem um alto risco de ter dificuldades em restabelecer os serviços de TI que oferecem aos seus usuários.

O presente trabalho também permitiu a identificação dos sistemas eletrônicos informacionais considerados de maior relevância pelos próprios gestores envolvidos. Destacam-se 9 sistemas que, em casos de incidentes de segurança da informação ou falha decorrente de defeitos do sistema, os gestores declararam possuir relação de impacto com perdas de vidas humanas ou dano grave para saúde humana (Tabela 4). Ademais, o Sistema Integrado de Gestão da Educação - SIGEDUC, gerenciado pela Secretaria de Estado da Educação, da Cultura, do Esporte e do Lazer, foi identificado como o de maior custo anual de sustentação (correção, adaptação e evolução do sistema), com valor aproximado de R$ 2,5 milhões de reais.

Por fim, a metodologia de avaliação de risco desenvolvida sintetiza, quantitativamente, as informações relatadas. Um bom nível de conformidade às normas e às boas práticas de Governança de TI foi aferido em 2 participantes do levantamento de informações (o Tribunal de Justiça e a Escola de Magistratura do RN), refletindo assim em um baixo nível de risco. Em nível intermediário de risco encontram-se 10 órgãos. O restante do espaço amostral (55

instituições) foi classificado na categoria de alto risco, por apresentar baixa conformidade ou por não ter enviado as informações solicitadas. A relação completa dos jurisdicionados classificados pelo nível de risco se encontra discriminada na Tabela 5.

Não foram encontradas correlações estatísticas significativas entre o nível de risco de um órgão e o tamanho ou orçamento de seu setor de tecnologia da informação. Conclui-se que o cenário constatado de baixa maturidade da Governança de TI abrange órgãos de características diversas.

Tabela 5 - Relação de jurisdicionados classificados pelo nível de risco

Nível de Risco	Jurisdicionado
Baixo (bom nível de conformidade com as boas práticas de Governança de TI)	• TRIBUNAL DE JUSTIÇA • ESCOLA DA MAGISTRATURA DO RN
Médio (intermediário nível de conformidade com as boas práticas de Governança de TI)	• AGÊNCIA DE FOMENTO DO RN S/A • CENTRAIS DE ABASTECIMENTO DO RN S/A • DEPARTAMENTO ESTADUAL DE IMPRENSA • HOSPITAL MARIA ALICE FERNANDES • INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO RN • PROCURADORIA GERAL DE JUSTIÇA • SECRETARIA DE ESTADO DA ADMINISTRAÇÃO • SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA E DA DEFESA SOCIAL • TRIBUNAL DE CONTAS DO ESTADO • UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE
Alto (baixo nível de conformidade com as boas práticas de Governança de TI ou omissão no envio das informações solicitadas)	• ASSEMBLÉIA LEGISLATIVA DO ESTADO DO RN • ASSESSORIA DE COMUNICAÇÃO SOCIAL DO RN • COMANDO DA POLÍCIA MILITAR DO RN • COMANDO DO CORPO DE BOMBEIROS MILITAR DO RN • COMPANHIA DE ÁGUAS E ESGOTOS DO RN (não submeteu as respostas) • COMPANHIA DE PROCESSAMENTO DE DADOS DO RN • COMPANHIA ESTADUAL DE HABITAÇÃO E DESENVOLVIMENTO URBANO • COMPANHIA POTIGUAR DE GÁS • CONTROLADORIA GERAL DO ESTADO • DEFENSORIA PÚBLICA GERAL DO ESTADO • DEPARTAMENTO DE ESTRADAS E RODAGENS DO RN • DEPARTAMENTO ESTADUAL DE TRÂNSITO • DIRETORIA DE SAÚDE DA POLÍCIA MILITAR • EMPRESA DE PESQUISA AGROPECUÁRIA DO RN • EMPRESA GESTORA DE ATIVOS DO RN • EMPRESA POTIGUAR DE PROMOÇÃO TURÍSTICA S/A • FUNDAÇÃO DE APOIO À PESQUISA DO ESTADO DO RN • FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO DO ESTADO DO RN • FUNDAÇÃO DJALMA MARINHO (não submeteu as respostas) • FUNDAÇÃO JOSÉ AUGUSTO • GABINETE CIVIL DO GOVERNADOR • GÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DO RN • HOSPITAL COLÔNIA DOUTOR JOÃO MACHADO • HOSPITAL DOUTOR JOSÉ PEDRO BEZERRA • HOSPITAL GISELDA TRIGUEIRO • HOSPITAL MONSENHOR WALFREDO GURGEL • HOSPITAL REGIONAL DEOCLÉCIO MARQUES DE LUCENA • HOSPITAL REGIONAL DOUTOR CLEODON CARLOS DE ANDRADE • HOSPITAL REGIONAL NELSON INÁCIO DOS SANTOS • HOSPITAL REGIONAL TARCÍSIO MAIA (não submeteu as respostas) • INSTITUTO DE ASSISTÊNCIA TÉCNICA E EXTENSÃO RURAL • INSTITUTO DE DEFESA E INSPEÇÃO AGROPECUÁRIA DO RN • INSTITUTO DE DESENVOLVIMENTO SUSTENTÁVEL E MEIO AMBIENTE DO RN • INSTITUTO DE EDUCAÇÃO SUPERIOR PRESIDENTE KENNEDY

Alto (baixo nível de conformidade com as boas práticas de Governança de TI ou omissão no envio das informações solicitadas)	• INSTITUTO DE GESTÃO DAS ÁGUAS DO ESTADO • INSTITUTO DE PESOS E MEDIDAS DO RN • INSTITUTO TÉCNICO-CIENTÍFICO DE PERÍCIA • JUNTA COMERCIAL DO ESTADO DO RN • POLÍCIA CIVIL • PROCURADORIA GERAL DO ESTADO • PROJETO RN SUSTENTÁVEL • SECRETARIA DE ESTADO DA ADMINISTRAÇÃO PENITENCIÁRIA • SECRETARIA DE ESTADO DA AGRICULTURA, DA PECUÁRIA E DA PESCA, • SECRETARIA DE ESTADO DA EDUCAÇÃO, DA CULTURA, DO ESPORTE E DO LAZER • SECRETARIA DE ESTADO DA INFRA-ESTRUTURA • SECRETARIA DE ESTADO DA SAÚDE PÚBLICA (não submeteu as respostas) • SECRETARIA DE ESTADO DA TRIBUTAÇÃO • SECRETARIA DE ESTADO DAS MULHERES, DA JUVENTUDE, DA IGUALDADE RACIAL E DOS DIREITOS HUMANOS • SECRETARIA DE ESTADO DE TURISMO • SECRETARIA DE ESTADO DO DESENVOLVIMENTO ECONÔMICO • SECRETARIA DE ESTADO DO DESENVOLVIMENTO RURAL E DA AGRICULTURA FAMILIAR • SECRETARIA DE ESTADO DO MEIO AMBIENTE E DOS RECURSOS HÍDRICOS • SECRETARIA DE ESTADO DO PLANEJAMENTO E DAS FINANÇAS • SECRETARIA DE ESTADO DO TRABALHO, DA HABITAÇÃO E DA ASSISTÊNCIA SOCIAL • VICE GOVERNADORIA

5.PROPOSTA DE ENCAMINHAMENTO

Diante de todo o exposto neste relatório, esta Comissão de Fiscalização submete os autos à consideração superior propondo:

a) A divulgação deste relatório, via Portal do Gestor, aos gestores dos órgãos envolvidos neste Levantamento da Governança de TI, para fins de conhecimento e para que possam fazer a melhor utilização possível dos dados levantados;

b) Nos termos do art. 6º, parágrafo único, da Resolução nº. 017/2016-TCE/RN, a ciência à Secretaria de Controle Externo – SECEX, para efetivar o cadastramento dos pontos de controle abordados neste relatório como demanda fiscalizatória no Sistema de Gerenciamento do PFA – SisPFA, a fim de subsidiar a avaliação e a viabilidade de ações fiscalizatórias futuras;

c) E por fim sugere-se o arquivamento do processo.

Natal/RN, 06 de março de 2024.

gov.br Documento assinado digitalmente
ALEXANDRE LUIZ GALVAO DAMASCENO
Data: 26/04/2024 11:27:21-0300
Verifique em https://validar.iti.gov.br

(assinado digitalmente)
Alexandre L. G. Damasceno
Auditor de Controle Externo
Mat. 9.988-0

EDUARDO PEREIRA LIMA:05911205424
Assinado digitalmente por EDUARDO PEREIRA LIMA:05911205424
ND: C=BR, O=ICP-Brasil, OU=AC SOLUTI Multipla v5, OU=09461647000195, OU=Presencial, OU=Certificado PF A3, CN=EDUARDO PEREIRA LIMA:05911205424
Razão: Eu sou o autor deste documento
Localização:
Data: 2024.04.29 11:19:28-03'00'
Foxit PDF Reader Versão: 2024.1.0

(assinado digitalmente)
Eduardo Pereira Lima
Auditor de Controle Externo
Mat. 9.874-4

MARCELO SANTOS DE ARAUJO:02486960414
Assinado digitalmente por MARCELO SANTOS DE ARAUJO:02486960414
ND: C=BR, O=ICP-Brasil, OU=AC SOLUTI Multipla v5, OU=09461647000195, OU=Presencial, OU=Certificado PF A3, CN=MARCELO SANTOS DE ARAUJO:02486960414
Razão: Eu sou o autor deste documento
Localização:
Data: 2024.05.01 16:15:16-03'00'
Foxit PDF Reader Versão: 2023.3.0

(assinado digitalmente)
Marcelo Santos de Araújo
Auditor de Controle Externo
Mat. 9.908-2

6.BIBLIOGRAFIA

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 12207 – Engenharia de sistemas e software – Processos de ciclo de vida de software. Rio de Janeiro, ABNT, 2009

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 21500 – Gerenciamento de projeto, programa e portfólio – Contexto e conceitos. Rio de Janeiro, ABNT, 2009

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação. Rio de Janeiro, ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 38500 – Tecnologia da informação – Governança da Tecnologia da Informação. Rio de Janeiro, ABNT, 2013

BRASIL. Tribunal de Contas da União. Acórdão 1.021/2014. Ata n° 12/2014 - Plenário. Brasília, DF. 16/04/2014. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201021%252F2014/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.163/2008. Ata n° 23/2008 - Plenário. Brasília, DF. 18/06/2008. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/acordao%25201163%252F2008/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.233/2012. Ata n° 19/2012 - Plenário. Brasília, DF. 23/05/2012. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201233%252F2012/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.328/2012. Ata n° 20/2012 - Plenário. Brasília, DF. 30/05/2012. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201328%252F2012/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.328/2012. Ata n° 20/2012 - Plenário. Brasília, DF. 30/05/2012. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201328%252F2012/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.558/2003. Ata n° 40/2003 - Plenário. Brasília, DF. 15/10/2003. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201558%252F2003/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.620/2014. Ata n° 22/2014 - Plenário. Brasília, DF. 18/06/2014. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201620%252F2014/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.684/2014. Ata n° 23/2014 - Plenário. Brasília, DF. 25/06/2014. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/Ac%25C3%25B3rd%25C3%25A3o%25201684%252F2014/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 1.684/2014. Ata n° 23/2014 - Plenário. Brasília, DF. 25/06/2014. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/acordao%25201684%252F2014/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

BRASIL. Tribunal de Contas da União. Acórdão 2.308/2010. Ata n° 33/2010 - Plenário. Brasília, DF. 08/09/2010. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2308%2520ANOACORDAO%253A2010%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

ISACA (ed.). COBIT 2019 Framework: introduction and methodology. Illinois: ISACA, 2018. Disponível em:

https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

ITGI. Board Briefing on IT Governance, 6ª edição, Rolling Meadows, IL (USA): IT Governance Institute, 2003. ISBN 1-893209-64-4. Disponível em: https://www.itgovernance.co.uk/files/download/Board_Briefing_on_IT_Governancev6.pdf

PMI. Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK® 5ª ed. – EUA: Project Management Institute, 2013.