Análise das Características de Gestão de Segurança da Informação do Poder Judiciário

Autoria: Lucas de Castro Moura, Carlos André de Melo Alves

Resumo
O objetivo geral deste estudo foi analisar as características de gestão de segurança da informação do poder judiciário em 2014 e em 2016, baseado em levantamentos de governança de tecnologia de informação realizados pelo Tribunal de Contas da União-TCU. Para tal fim realizou-se estudo descritivo, com abordagem qualitativa e quantitativa. A amostra não probabilística abrange os entes do poder judiciário custeados pela União que participaram dos referidos levantamentos. Os dados foram coletados em junho de 2017, por meio de solicitação ao TCU. O tratamento dos dados enfatizou a análise das respostas aos 21 subitens agrupados em 2 itens pertencentes à Questão 5.4 do levantamento, sobre Gestão Corporativa de Segurança da Informação, utilizando-se estatística descritiva, estatística inferencial não paramétrica, análise de resíduos e análise de correspondência. Após exame das 2.709 respostas, a análise dos subitens permitiu constatar mudanças na ótica dos entes do Judiciário, com o movimento dos subitens de se afastar da característica "não adota ou não se aplica" e migrando para "iniciou plano" e "adota parcial" e dessa última para "adota integral". Quanto às características de gestão de segurança da informação, no tocante ao item "Políticas e responsabilidades", os entes do Poder Judiciário sugerem adoção integral nos anos de 2014 e de 2016, mas para o item "Controles e atividades", os resultados dos dois anos sugerem a necessidade de aprimoramentos. Este estudo contribui tanto para auxiliar gestores no diagnóstico e melhoria da gestão de segurança da informação no judiciário, quanto de forma acadêmica e metodológica para estudos futuros.

Palavras-chave: Gestão de Segurança da Informação. Governança de Tecnologia da Informação. Poder Judiciário. Análise Multivariada.

1 Introdução

O Poder Judiciário apresenta-se como um dos principais prestadores de serviço à população, julgando em 2015 cerca de 18.9 milhões de processos. No entanto, o valor ainda ficou abaixo da quantidade de processos distribuídos, cerca de 19.6 milhões. Assim, anualmente o Conselho Nacional de Justiça - CNJ tem traçado metas e buscado melhorar a eficiência do Poder Judiciário (CNJ, 2016).

A Resolução nº 198 de 1º de julho de 2014 do CNJ, que instituiu a estratégia do Poder Judiciário para o período de 2015 a 2020, observou como uma das atuais tendências a intensificação do uso de tecnologia da informação (TI) e definiu como desafio a ser alcançado a melhoria da infraestrutura e da governança de TI.

Desde 2008, por meio do acórdão 1.603 de 13 de agosto de 2008, o TCU recomenda ao CNJ e ao Gabinete de Segurança Institucional da Presidência da República – GSI, que

orientem os Órgãos sob sua tutela, promovendo ações que para estabelecer ou aperfeiçoar práticas relacionadas à segurança da informação.

O GSI, por meio da Norma Complementar 03/IN01/DSIC/GSIPR de 2009 e o CNJ, com o documento Diretrizes para a Gestão de Segurança da Informação no Âmbito do Poder Judiciário de 2012, estabeleceram diretrizes para elaboração de política de segurança da informação e comunicações dos órgãos e entidades da Administração Pública Federal e dos órgãos do Poder Judiciário, respectivamente.

Já o TCU, através da publicação da 4ª edição do documento Boas Práticas em Segurança da Informação, reitera a importância tema. Desde 2007, o Tribunal de Contas da União - TCU - realiza o Levantamento de Governança de TI, com o objetivo de avaliar a situação de governança de TI na Administração Pública Federal, inclusive dos órgãos do Poder Judiciário custeados pela União. A partir de 2012 a avaliação passou a ocorrer em ciclos de dois anos. Em 2014 e 2016, 65 entes do Poder Judiciário (integrados por conselhos e tribunais), participaram dos levantamentos realizados pelo TCU.

O questionário utilizado pelo TCU tem suas questões baseadas em referências tanto internas quanto externas de boas práticas em Gestão e Governança Corporativa de TI, e as respostas desses questionários são utilizadas pelo TCU, inclusive, para calcular um índice, o IGov TI.

Face ao direcionamento dado pelo CNJ, verifica-se a oportunidade de utilizar as respostas da Questão 5.4 do levantamento do TCU, segmentadas em itens e subitens, para analisar as características da gestão da segurança da informação dos entes do Poder Judiciário nos anos de 2014 e de 2016, descritos no 2º parágrafo desta seção.

1.1 Problema e Objetivo Geral

Diante do que foi exposto, o problema de pesquisa é o seguinte: quais são as características de gestão da segurança da informação dos entes do poder judiciário em 2014 e em 2016, baseado em levantamentos de governança de tecnologia da informação do TCU? Dessa forma, o objetivo geral deste estudo é analisar as características de gestão da segurança da informação dos entes do poder judiciário em 2014 e em 2016, baseado em levantamentos de governança de tecnologia da informação do TCU.

Justifica-se o presente estudo do ponto de vista teórico para o melhor entendimento das organizações do poder judiciário, uma vez aborda a gestão corporativa da segurança da informação de um segmento específico, que abrange entes do poder judiciário, como a Justiça do Trabalho, Justiça Federal, Justiça Eleitoral, Tribunais Superiores e Conselhos de Justiça.

Segundo o modelo COBIT versão 5 (ISACA, 2012) para governança e gestão de TI, o objetivo da governança de TI é criar valor a partes interessadas da organização, significando realização de benefícios, minimização de riscos e otimização de recursos. Dessa forma, resultados do estudo podem ser de grande valia para:

- gestores de órgãos do poder judiciário, podendo auxiliá-los no aprimoramento da gestão corporativa da segurança da informação e na identificação os caminhos necessários ao alcance dos objetivos de TI dos referidos órgãos;
- acadêmicos, órgãos de controle externo e demais partes interessadas, advogados, usuários e sociedade em geral.

Por fim, como contribuição metodológica, verifica-se que o emprego da análise inferencial não paramétrica e da técnica multivariada de análise de correspondência, a qual permite a visualização de associações entre variáveis por meio de mapas perceptuais.

2 Referencial Teórico

2.1 Governança de TI

A Governança de TI tem sido objeto de diversos estudos. Segundo Teodoro, Przeybilovicz e Cunha (2012) o conceito reúne aspectos de estrutura, processos, controle e relacionamento da TI com o ambiente da organização.

Segundo Weill e Ross (2006), a governança de TI pode ser definida como a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização de TI. Para Lunardi (2008), governança de TI consiste no sistema responsável pela distribuição de responsabilidades e direitos sobre as decisões de TI, bem como pelo gerenciamento e controle dos recursos tecnológicos da organização, buscando, dessa forma, garantir o alinhamento da TI às estratégias e aos objetivos organizacionais.

Apesar da diversidade de conceitos, Pereira e Ferreira (2015) citam como pontos em comum das definições: o alinhamento entre negócio e TI, estruturas de tomada de decisão e responsabilidades relacionadas com as estratégias, alcançar objetivos e valor definidos para a organização dos investimentos realizados e Mecanismos de medição e controle.

Nesse sentido, a governança de TI, propriamente dita, envolve a aplicação de princípios de governança corporativa para dirigir e controlar a TI de forma estratégica, preocupando-se exclusivamente com o valor que ela proporciona à organização e o controle e a diminuição dos riscos relacionados a si mesma (LUNARDI, BECKER, MAÇADA, 2010).

Segundo De Haes e Van Grembergen (2015), a literatura identifica um conjunto diversificado de práticas ou mecanismos de Governança de TI, no entanto, a decisão de quais devem ser implementados tem que atender ao contexto e especificidades da organização, nomeadamente o seu setor de atividade, dimensão e cultura organizacional. Weill e Ross (2006) citam que cada mecanismo de governança de TI deve apresentar três características: ser simples, transparente e adequado.

Na implantação de práticas de Governança de TI no Tribunal Regional Eleitoral de Santa Catarina – TRE/SC, Klumb e Azevedo (2014) citam o aumento da eficiência, da agilidade e da qualidade dos serviços disponibilizados aos usuários refletindo positivamente na qualidade dos serviços disponibilizados e ainda, a formação de uma visão mais gerencial da TI, que por meio de indicadores de desempenho proporciona uma tomada de decisão mais efetiva.

Nas organizações, podem-se adotar conjuntos de práticas ou de mecanismos de TI tidos por modelos ou *frameworks*, no entanto, tomando por exemplo, tanto *Control Objectives for Information and Related Technology* - COBIT quanto o *Information Technology Infrastruture Library* - ITIL atuam como guias de referência na gestão da TI, não exigindo que todos os seus processos e objetivos de controle sejam adotados (LUNARDI, BECKER, MAÇADA 2010). Alguns dos *frameworks* mais utilizados nas organizações são COBIT e ITIL (LUNARDI E DOLCI 2009).

O COBIT foi desenvolvido pelo *Information Systems Audit and Control Association* - ISACA, uma associação para profissionais de TI e Auditores de TI com mais de 140.000 membros e presente em 187 países. Segundo o ISACA (2016), COBIT 5 provê um *framework* compreensivo que auxilia o empreendimento a alcançar seus objetivos para a governança e gestão dos empreendimentos de TI.

Por sua vez, o ITIL é uma biblioteca contendo um conjunto de melhores práticas de gestão de infraestrutura de TI. Foi desenvolvido pelo *Office Government of Commerce* – OGC

– Secretaria de Comércio do governo britânico, a partir da necessidade de tornar os processos relacionados à TI mais claros e organizados (LUNARDI; DOLCI, 2009).

A última versão do ITIL é dividida em 5 estágios do ciclo de vida de serviço e cada estágio do ciclo de vida do ITIL relaciona-se com um conjunto de processos, que por sua vez estão associados a papéis que necessitam ser cumpridos no ciclo de vida. Um processo é um conjunto estruturado de atividades, desenhado para atingir um objetivo específico. Um processo utiliza um ou mais inputs e os transforma em outputs, definindo ações, dependências e sequências. O ITIL provê um guia para qualidade dos processos de TI e nesses processos, funções e outras capacidades necessárias para suporte (CABINET OFFICE 2011).

O melhor mix de estruturas, processos e mecanismos de relacionamento será diferente para cada organização e dependerá de múltiplas contingências, incluindo setor e ambiente da organização (SETHIBE, CAMPBELL E MCDONALD 2007).

Atualmente, o Levantamento do TCU é o principal instrumento de avaliação e de análise em Governança de TI na Administração Pública Federal (RAMOS, 2014). Um índice, o IGovTI, é obtido por meio do cálculo da média aritmética das variáveis avaliadas, a partir de um questionário padronizado pelo TCU, com a escala Likert variando de 0 a 10 pontos. O TCU utiliza como referência o modelo COBIT, para caracterizar os níveis de maturidade dos processos de governança de TI das organizações (MEDEIROS, 2016).

2.2 Segurança da Informação

Com a finalidade de garantir um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de passar para a seleção de soluções específicas de segurança (BEAL, 2005).

Segundo Omar e Rolt (2015), os gestores de cartórios no Brasil elegeram a segurança da informação como de alta prioridade. Em serviços de natureza pública, as informações são críticas à própria prestação do serviço. No âmbito do poder executivo, o GSI define por Segurança da Informação e Comunicações (SIC): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (GSI, 2015).

Segurança da informação, conforme definido pela ISO/IEC 27002:2008, é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades (MONTEIRO, 2009).

Devido ao interesse em um padrão internacional de segurança da informação, em dezembro de 2000, foi publicada a norma internacional ISO 17799:2000 (NETTO e SILVEIRA, 2007). Atualmente são utilizadas as normas 27001, 27002 e 27005 ABNT NBR ISO/IEC.

A ISO/IEC 27002 é um código de prática de SI, ou seja, "um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança" (OLIVEIRA et al., 2015). A ISO/IEC 27002 possui 15 capítulos, incluindo 133 controles que estão divididos em 11 capítulos, chamados seções de controles de segurança da informação. Há também um capítulo que é uma seção introdutória, que aborda análise, avaliação e tratamento de riscos (OLIVEIRA et al., 2015).

O TCU utiliza por base em seu levantamento os diversos conceitos da ISO/IEC 27002:2013, como Política de segurança da informação, Responsabilidades e papéis, Política de controle de acesso, Cópias de segurança das informações, Gestão de ativos, Classificação da informação e Gestão de vulnerabilidades técnicas.

O GSI, no Guia Básico de Orientação ao Gestor em Segurança da Informação e Comunicações, sugere que temas ainda não normatizados no governo federal, mas já amparados por normas da família ISO 27.0001/27.0002, também sejam analisados à luz das

necessidades específicas de cada órgão para inclusão na Política de Segurança da Informação e Comunicações.

Segundo o ITIL, a gestão da segurança da informação garante que o serviço é desenhado para proteger a confidencialidade e integridade da organização, e que o serviço está em conformidade com as políticas e requisitos de segurança organizacionais. Além disso, para o ITIL a segurança deve cobrir os aspectos como: uso autorizado e responsabilizável dos serviços, proteção dos ativos do cliente de acesso não autorizado ou malicioso, zonas de segurança entre ativos do cliente e ativos do serviço e garantir a integridade e confidencialidade da informação utilizada pela organização e seus clientes (CABINET OFFICE, 2011).

Para o Poder Judiciário, o CNJ (2012) entende-se por Segurança da Informação: preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação; adicionalmente, outras propriedades, tais como responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.Para os conceitos citados, o CNJ baseia-se na norma ISO/IEC 13335-1:2004, e os define conforme Quadro 1.

Conceito	**Definição**
Confidencialidade	propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos que não possuam autorização.
Autenticidade	propriedade que permite a validação de identidade de usuários e sistemas.
Disponibilidade	propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.
Integridade	propriedade de proteção à precisão e perfeição da informação e de recursos.

Quadro 1 – Definição CNJ conceitos Segurança da Informação
Fonte: Adaptado CNJ (2012)

Considerando tanto a ênfase nas estruturas e práticas de segurança da informação, bem como o direcionamento do TCU e do Poder Judiciário em relação aos itens avaliados na Questão 5.4 da Dimensão 'Processos', relacionados à gestão de segurança da informação, apresenta-se o Quadro 2, a seguir, descreve itens e subitens propostos para caracterizar a gestão da segurança da informação. O referido quadro reproduz itens da questão 5.4, e nele pode-se observar a similaridade com o ITIL v.3 na definição de papeis, como gestor de segurança da informação e na definição de responsabilidades na gestão dos ativos da organização.

Subitens associados ao item 'Políticas e responsabilidades'
a. a organização dispõe de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório.
b. a organização dispõe de comitê de segurança da informação, formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.
c. a organização possui gestor de segurança da informação, formalmente designado, responsável pelas ações corporativas de segurança da informação.
d. a organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída como norma de cumprimento obrigatório.

e. a organização dispõe de política de cópias de segurança (backup) formalmente instituída como norma de cumprimento obrigatório.
Subitens associados ao item 'Controles e atividades'
f. a organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.
g. o processo de gestão de ativos está formalmente instituído como norma de cumprimento obrigatório.
h. a organização executa processo para classificação e tratamento de informações.
i. o processo para classificação e tratamento de informações está formalmente instituído como norma de cumprimento obrigatório.
j. a organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.
k. a organização executa processo de gestão de riscos de segurança da informação.
l. o processo de gestão de riscos de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.
m. a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas.
n. o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído como norma de cumprimento obrigatório.
o. a organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas.
p. o processo de monitoramento do uso dos recursos de TI está formalmente instituído como norma de cumprimento obrigatório.
q. a organização executa processo de gestão de incidentes de segurança da informação.
r. o processo de gestão de incidentes de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.
s. a organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída.
t. a organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.
u. a organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações.

Quadro 2 – Itens propostos para caracterizar a Gestão da Segurança da Informação
Fonte: Adaptado TCU (2016)

3 Metodologia

Esta seção apresenta como a pesquisa foi realizada, sendo dividida entre: tipo e descrição geral da pesquisa, caracterização do setor estudado, população e amostra e os procedimentos de coleta e análise dos dados.

3.1 Tipo e descrição geral da pesquisa

A pesquisa, quanto ao alcance será descritiva, que conforme Sampieri, Collado e Lucio (2013) busca especificar as propriedades, as características e os perfis de pessoas, grupos, comunidades, processos, objetos, ou qualquer outro fenômeno que se submeta a uma análise. Adicionalmente, a presente pesquisa possui abordagem qualitativa e quantitativa.

3.2 Caracterização da organização, setor estudado

O Poder Judiciário é regulado pela Constituição Federal nos seus artigos 92 a 126. No sistema Judiciário brasileiro, há órgãos que funcionam no âmbito da União e dos estados, incluindo o Distrito Federal e Territórios. No campo da União, o Poder Judiciário conta com as seguintes unidades: a Justiça Federal – incluindo os juizados especiais federais – e a Justiça Especializada – composta pela Justiça do Trabalho, a Justiça Eleitoral e a Justiça Militar (STF, 2011).

Além dos Tribunais, verificamos outros entes, que são: O CNJ, vinculado ao STF, o Conselho da Justiça Federal - CJF, vinculado ao STJ e o Conselho Superior da Justiça do Trabalho - CSJT, vinculado ao TST.

A Missão do Poder Judiciário, foi definida como: Realizar Justiça – Fortalecer o Estado Democrático e fomentar a construção de uma sociedade livre, justa e solidária, por meio de uma efetiva prestação jurisdicional (CNJ, 2014).

Em complemento, a Visão do Poder Judiciário: Ser reconhecido pela sociedade como instrumento efetivo de justiça, equidade e paz social – Ter credibilidade e ser reconhecido como um poder célere, acessível, responsável, imparcial, efetivo e justo, que busca o ideal democrático e promove a paz social, garantindo o exercício pleno dos direitos de cidadania (CNJ, 2014).

3.3 População e amostra

A população abrange todos os respondentes do levantamento do TCU, que são 372 em 2014 e 379 em 2016. A amostra não probabilística abrange todos os entes do poder judiciário custeados pela União que responderam, em cada ano, as questões apresentadas no referido levantamento. O Quadro 3 apresenta a amostra, a qual contempla 65 entes do Poder Judiciário, incluindo-se o TJDFT, que também é custeado pela União. De acordo com o TCU, as respostas do Tribunal Regional Eleitoral do Pará, embora recebidas, não foram consideradas válidas para o levantamento referente ao ano de 2016, considerando os critérios de qualidade estabelecidos pelo próprio TCU.

1	Conselho Nacional de Justiça – CNJ	34	Tribunal Regional Eleitoral - TRE-BA
2	Conselho da Justiça Federal – CJF	35	Tribunal Regional Eleitoral - TRE-PB
3	Conselho Superior da Justiça do Trabalho - CSJT	36	Tribunal Regional Eleitoral - TRE-AL
4	Supremo Tribunal Federal – STF	37	Tribunal Regional Eleitoral - TRE-GO
5	Superior Tribunal Militar – STM	38	Tribunal Regional Eleitoral - TRE-MG
6	Superior Tribunal de Justiça – STJ	39	Tribunal Regional Eleitoral - TRE-PE
7	Tribunal Superior do Trabalho – TST	40	Tribunal Regional Eleitoral - TRE-RO
8	Tribunal Superior Eleitoral - TSE	41	Tribunal Regional Eleitoral - TRE-RR
9	Tribunal de Justiça do DF e Territórios - TJDFT	42	Tribunal Regional Eleitoral - TRE-SC
10	Tribunal Regional do Trabalho - TRT 1ª Região	43	Tribunal Regional Eleitoral - TRE-SP
11	TRT 2ª Região	44	Tribunal Regional Eleitoral - TRE-SE
12	TRT 3ª Região	45	Tribunal Regional Eleitoral - TRE-TO
13	TRT 4ª Região	46	Tribunal Regional Eleitoral - TRE-AC
14	TRT 5ª Região	47	Tribunal Regional Eleitoral - TRE-AP

15	TRT 6ª Região	48	Tribunal Regional Eleitoral - TRE-AM
16	TRT 7ª Região	49	Tribunal Regional Eleitoral - TRE-CE
17	TRT 8ª Região	50	Tribunal Regional Eleitoral - TRE-DF
18	TRT 9ª Região	51	Tribunal Regional Eleitoral - TRE-ES
19	TRT10ª Região	52	Tribunal Regional Eleitoral - TRE-MA
20	TRT11ª Região	53	Tribunal Regional Eleitoral - TRE-MT
21	TRT12ª Região	54	Tribunal Regional Eleitoral - TRE-MS
22	TRT13ª Região	55	Tribunal Regional Eleitoral - TRE-PA
23	TRT14ª Região	56	Tribunal Regional Eleitoral - TRE-PR
24	TRT15ª Região	57	Tribunal Regional Eleitoral - TRE-PI
25	TRT16ª Região	58	Tribunal Regional Eleitoral - TRE-RJ
26	TRT17ª Região	59	Tribunal Regional Eleitoral - TRE-RN
27	TRT18ª Região	60	Tribunal Regional Eleitoral - TRE-RS
28	TRT19ª Região	61	Tribunal Regional Federal - TRF-1ª Região
29	TRT20ª Região	62	TRF-2ª Região
30	TRT21ª Região	63	TRF-3ª Região
31	TRT22ª Região	64	TRF-4ª Região
32	TRT23ª Região	65	TRF-5ª Região
33	TRT24ª Região		

Quadro 3 – Amostra
Fonte: Adaptado TCU, 2016

3.4 Procedimentos de coleta e de análise de dados

Os dados foram coletados junho de 2017, por meio de solicitação realizada à Ouvidoria do TCU em 16/05/2017 que foi deferida em 19/06/2017. De notar que as respostas foram enviadas sem a identificação do ente respondente. Para cada ente e em cada ano, enfatizou-se a análise das respostas aos 21 subitens agrupados em 2 itens relativos à Questão 5.4 do levantamento, sobre Gestão Corporativa de Segurança da Informação. No total, foram obtidas 1365 respostas válidas em 2014 e 1344 respostas válidas em 2016, totalizando 2709 respostas válidas.

Para tratamento dos dados, utilizou-se a estatística descritiva, a estatística inferencial, com abordagem não paramétrica, empregando-se os testes qui-quadrado, análise de resíduos e técnica multivariada de análise de correspondência - ANACOR (FÁVERO et al, 2009).

Cada resposta válida foi dada no questionário do TCU numa escala de 5 categorias, sendo previamente aglutinadas as categorias “não se aplica” e “não adota”, totalizando, ao final, 4 categorias que indicam as características de gestão de segurança da informação nesta pesquisa (Quadro 4). Tal aglutinação foi necessária para permitir o tratamento adequado dos dados, em especial o emprego de testes qui-quadrado (SIEGEL, CASTELLAN, 2006).

Característica	Resposta
Não adota ou não se aplica	1 e 2
Iniciou plano para adotar	3
Adota parcialmente	4
Adota integralmente	5

Quadro 4 – operacionalização das respostas relativas às características em categorias.
Obs.: As categorias "não adota" e "não se aplica" foram aglutinadas, formando a categoria "não adota ou não se aplica", para permitir o tratamento adequado dos dados, conforme SIEGEL e CASTELLAN (2006).
Fonte: Adaptado TCU (2016)

A ANACOR considerou o método simétrico de normalização, buscando hierarquizar a informação através dos valores do coeficiente de correlação R de Pearson entre os scores das duas variáveis e, assim a primeira dimensão é a que mais explica a variação existente nos dados (PESTANA e GAGEIRO, 2005). Segundo Fávero, et al. (2009) as categorias (subitens) mais explicativos para cada dimensão, são os que apresentam maior inércia por dimensão e por consequência, maior distância da origem (0,0).

Por fim, para a elaboração dos quadros e tabelas empregou-se o software Excel e para a execução da análise de resíduos, dos testes qui-quadrado e da ANACOR empregou-se o Software SPSS.

4 Resultados e Discussão

4.1 Análise das Respostas aos Subitens em 2014

A Tabela 1 apresenta a tabulação dos dados de 2014 com o total de respostas por cada cartacterística. Os subitens "a" e "b" atingiram o percentual de respostas do tipo "adota integral", de 61,54% e 70,77% com 40 e 46 respostas respectivamente. Os subitens "k" e "n" obtiveram apenas 1 resposta "adota integral" enquanto "l", "m", "p" e "h" obtiveram 2 respostas.

Verificado o total da amostra a característica "não adota ou não se aplica" somou 43,81% das respostas dos subitens, "iniciou plano" obteve 23,30% das respostas. Já "adota parcial" foi encontrada em 16,70% das respostas e "adota integral" em 16,19%.

Tabela 1 – Respostas aos subitens em 2014

Subitem	não adota ou não se aplica (%)	iniciou plano (%)	adota parcial (%)	adota integral (%)	Total (%)
Total	598 (43,81%)	318 (23,30%)	228 (16,70%)	221 (16,19%)	1365 (100,00%)
Resultados do Teste² : 593,89		GL: 60	Sig.: 0,00***		

Fonte: resultado da pesquisa
Legenda: 'GL' são os graus de liberdade; 'Sig.' é significância. ² é qui-quadrado. *** Significante a 1%.

No Teste qui-quadrado, descrito na Tabela 1, a hipótese nula é de que não há diferenças entre as respostas dadas aos subitens. O resultado do teste obteve significância de

0,00, com sessenta graus de liberdade. Considerando um nível de significância de 1,00%, a hipótese nula deve ser rejeitada, demonstrando que há diferenças significativas a 1,00%

Na Tabela 2, segue a análise de resíduos referente aos subitens em 2014. A análise de resíduos revela os padrões característicos segundo o excesso ou falta de ocorrências (BATISTA; ESCUDER; PEREIRA, 2004).

Tabela 2 – Resíduos padronizados - subitens em 2014

Subitem	não adota ou não se aplica	iniciou plano	adota parcial	adota integral
a)	**-4,59**	-0,55	-0,87	**9,09**
b)	**-4,21**	**-3,12**	-0,26	**10,94**
c)	-0,65	-1,32	-0,87	**3,54**
d)	**-2,15**	-0,04	-0,87	**4,46**
e)	-1,21	0,99	0,04	0,76
f)	-0,84	-0,29	**3,08**	-1,39
g)	1,60	0,73	-1,17	**-2,32**
h)	0,47	**2,02**	-0,56	**-2,63**
i)	1,78	0,48	-1,47	**-2,01**
j).	0,29	-0,04	1,86	**-2,32**
k)	0,66	1,76	-0,26	**-2,94**
l)	1,41	**2,02**	**-2,08**	**-2,63**
m)	1,22	-1,32	**2,17**	**-2,63**
n)	**4,41**	-0,81	**-3,30**	**-2,94**
o)	-1,59	0,22	**3,38**	-1,09
p)	**3,10**	-0,29	**-2,08**	**-2,63**
q)	0,47	1,25	-0,26	**-2,01**
r)	**3,28**	0,22	**-2,99**	**-2,63**
s)	1,04	-0,29	-1,78	0,46
t)	0,10	0,48	1,56	**-2,32**
u)	**-4,59**	**-2,09**	**6,72**	**3,23**

Fonte: resultado da pesquisa
Observação: a descrição dos subitens de a) a u) encontra-se no Quadro 3.

Os resíduos padronizados entre -1,96 e 1,96, dentro de um intervalo de confiança de 95,00% indicam, para a significância verificada, que o subitem se comporta de forma semelhante ao valor esperado (PESTANA e GAGEIRO, 2005). Os valores que foram acima ou abaixo desse intervalo foram destacados na tabela 2, pois os subitens se comportaram de forma diferente da esperada na distribuição qui-quadrado.

Pode-se verificar especialmente falta de ocorrências dos subitens “a”, “b” e “u” na característica “não adota” ou “não se aplica”. Também há falta de ocorrências para os subitens “g” até “n”, “p” e “t” na categoria “adota integral”. Há excesso de ocorrências para os subitens “n”, “p”, e “r” para a característica “não adota” ou “não se aplica” e para os subitens “a”, “b”, “c” e “d” na característica “adota integral”.

As constatações da análise de resíduos sugerem predomínio de ocorrências “adota integral” em subitens mais associados ao item “Políticas e responsabilidades” e falta de ocorrências dessa característica em subitens ligados ao item “Controles e atividades”, descritos no Quadro 3.

4.2 Análise das Respostas aos Subitens em 2016

A Tabela 3 apresenta o total por características em 2016. No total, a característica "não adota ou não se aplica" apresentou o percentual de 28,65% das respostas, seguida de "iniciou plano" com 27,83%, "adota integral" (24,26%) e "adota parcial" (19,27%).

Tabela 3 – Respostas aos subitens em 2016

Subitem	não adota ou não se aplica (%)	iniciou plano (%)	adota parcial (%)	adota integral (%)	Total (%)
Total	385 (28,65%)	374 (27,83%)	259 (19,27%)	326 (24,26%)	1344 (100,00%)
Resultados do Teste	² : 530,97	GL: 60	Sig.: 0,00***		

Legenda: 'GL' são os graus de liberdade; 'Sig.' é significância. *** Significante a 1%.
Fonte: resultado da pesquisa

Para 2016, os resultados do teste qui-quadrado descritos na tabela 3 indicaram, em um nível de significância de 1,00%, que houve diferenças significativas entre as respostas.

A Tabela 4 apresenta os Resíduos padronizados para 2016. Em 2016 verifica-se falta de ocorrências dos subitens "a", "b", "d" e "u", descritos no Quadro 3, para a característica não adota ou não se aplica. Há falta de ocorrências para os subitens "h", "k", "m", "n", "p", "r" e "t" na categoria adota integral. Há excesso de ocorrências para os subitens "m", "n", "p", e "r" para a característica "não adota ou não se aplica" e para os subitens "a", "b", "c" e "d" na característica "adota integral".

Tabela 4 – Resíduos padronizados - subitens em 2016

Subitem	não adota ou não se aplica	iniciou plano	adota parcial	adota integral
a)	**-3,81**	-1,61	**-2,66**	**8,24**
b)	**-4,05**	**-2,32**	**-2,37**	**9,00**
c)	-0,78	-0,43	**-2,09**	**3,17**
d)	**-2,88**	0,52	-0,38	**2,91**
e)	-1,95	0,76	-0,38	1,64
f)	-1,71	0,05	**3,89**	-1,66
g)	0,62	1,23	-1,23	-0,89
h)	-0,08	1,94	1,04	**-2,92**
i)	1,79	0,28	-0,66	-1,66
j).	0,62	0,52	0,47	-1,66
k)	0,16	1,47	0,76	**-2,42**
l)	1,09	1,70	**-2,37**	-0,89
m)	**2,49**	-0,90	0,76	**-2,42**
n)	**5,29**	0,28	**-2,94**	**-3,43**
o)	-1,01	**-2,09**	**5,60**	-1,66
p)	**3,66**	-0,67	-0,95	**-2,42**
q)	0,16	0,99	0,76	-1,91
r)	**2,96**	1,70	**-2,66**	**-2,67**
s)	0,16	-0,43	-1,80	1,90
t)	0,39	0,28	1,61	**-2,16**
u)	**-3,11**	**-3,27**	**5,60**	1,90

Fonte: resultado da pesquisa
Observação: a descrição dos subitens encontra-se no Quadro 3.

Diferente de 2014 o subitem "m" - a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas - possui excesso de ocorrências em 2016 para a característica "não adota ou não se aplica".

A análise de resíduos de 2016 sugere predomínio de ocorrências "adota integral" em subitens mais associados ao item "Políticas e responsabilidades" e falta de ocorrências dessa característica em subitens ligados ao item "Controles e Atividades", descritos no Quadro 3.

4.3 Comparação Entre Subitens de 2014 para 2016

Para iniciar a comparação dos subitens de 2014 para 2016, empregou-se a técnica multivariada ANACOR, previamente citada na metodologia. A ANACOR utiliza o teste qui-quadrado para padronizar valores das frequências e formar a base de associações (FÁVERO; JUNIOR, 2009). Inicialmente apresenta-se a Tabela 5 a qual mostra o resultado dos testes qui-quadrado considerando os subitens em cada ano:

Tabela 5 – Testes qui-quadrado – comparação entre subitens de 2014 para 2016

Ano	N	Qui-quadrado	GL	Significância
2014	1365	266,97	3	0,00***
2016	1344	230,08	3	0,00***
Total	2709	481,73	3	0,00***

Fonte: dados da pesquisa.
Legenda: 1. 'GL' são os graus de liberdade. 2. 'N' é a quantidade de respostas obtidas em cada ano para cada subitem. ***Significativo a 1%.

Os resultados do teste qui-quadrado descritos na tabela 5 indicaram, em um nível de significância de 1,00%, diferenças significativas entre as respostas obtidas para os subitens.

Os dados da Tabela 6 mostram que para a ANACOR realizada os valores apresentados nas duas dimensões são 93,09% da inércia total (67,40% da inércia para a primeira dimensão e 25,69% da inércia para a segunda dimensão).

Tabela 6 – ANACOR - resumo dos resultados – comparação entre subitens de 2014 para 2016

Dimensão	Valor singular	Inércia	Qui-quadrado	Significância
1	0,54	0,29		
2	0,33	0,11		
3	0,17	0,03		
Total		0,43	1183,79	0,00***

Fonte: dados da pesquisa.
Observação:*** Significativo a 1%.

O Mapa perceptual mostra a posição de cada subitem em 2014 e 2016 (Figura 3). Foram traçadas 21 setas para exemplificar o movimento de cada subitem de 2014 para 2016.

Pode-se verificar dois movimentos principais no mapa (BLASIUS; GREENACRE,1998). O primeiro é a aproximação da característica “adota integral”, realizado pelos subitens “a”, “b”, “c”, “d”, “e”, e “s”, descritos no Quadro 3.

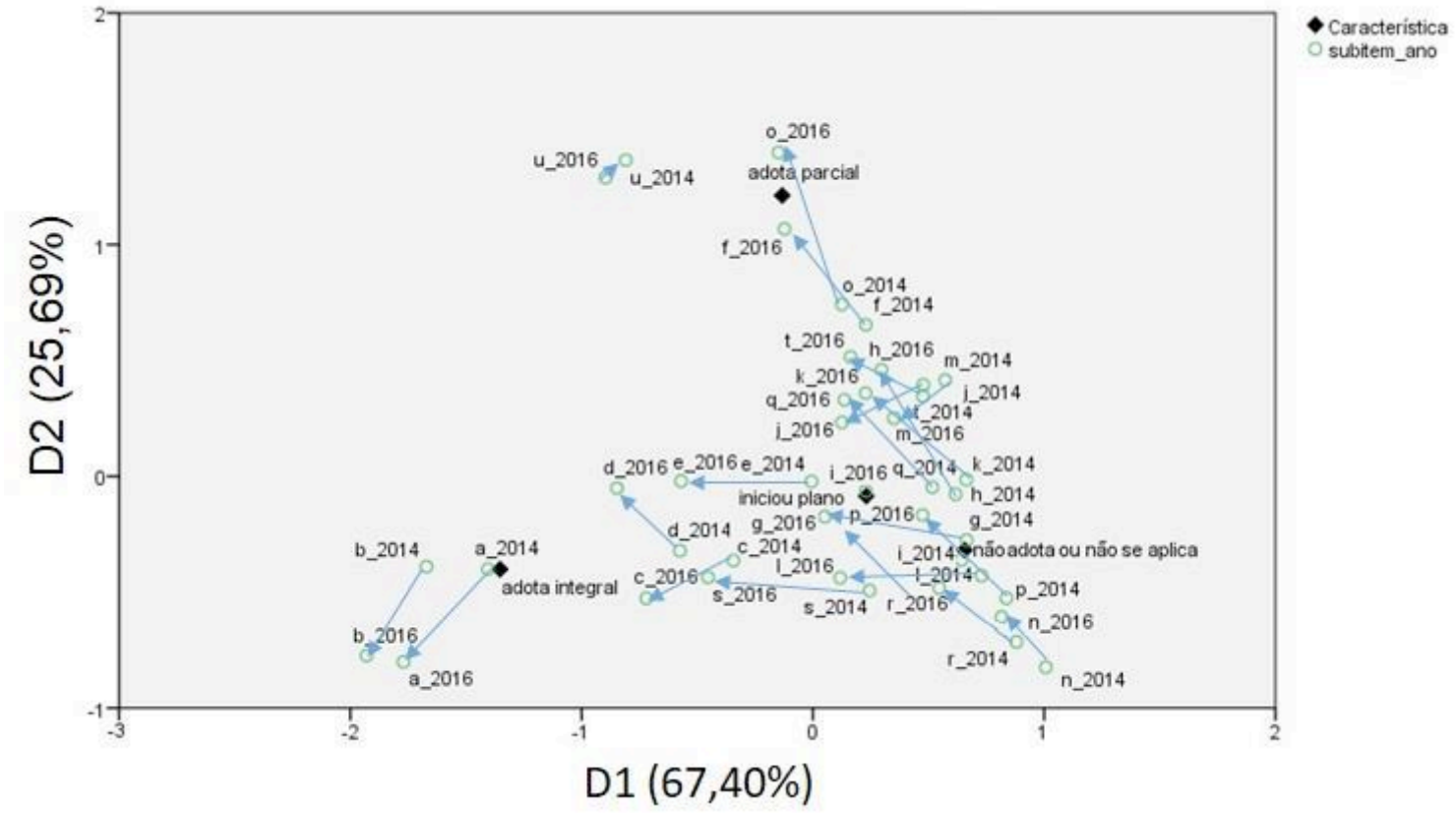

Figura 3 – Mapa Perceptual (comparação entre subitens de 2014 para 2016)
Observações: D1 é a 1ª dimensão, que explica 67,40% dos dados. D2 é a 2ª dimensão, que explica 25,69% dos dados.
Cada letra corresponde ao subitem analisado. O número corresponde ao período, 2014 ou 2016.
A descrição dos subitens de "a" até "u" encontra-se no Quadro 2.

De acordo com a Figura 3, os subitens “a” e “b” que já se encontravam próximos de “adota integral”, se distanciaram ainda mais dos demais subitens. Os subitens “c”, “d”, “e” e “s” mostraram evolução e conseguiram se aproximar de “adota integral”, com destaque para “s” – a organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída – que realizou grande deslocamento no mapa perceptual e avançou mais que os demais subitens pertencentes a “Controles e atividades”.

O segundo movimento é de se afastar da característica “não adota ou não se aplica”, para próximo das características “adota parcial” e “iniciou plano”. Verifica-se os subitens “h” - a organização executa processo para classificação e tratamento de informações - e “k” - a organização executa processo de gestão de riscos de segurança da informação - se afastam da característica “não adota” ou “não se aplica” e se aproximam de “adota parcial”.

Já os subitens “p” - o processo de monitoramento do uso dos recursos de TI está formalmente instituído como norma de cumprimento obrigatório e “i” - o processo para classificação e tratamento de informações está formalmente instituído como norma de cumprimento obrigatório – afastam-se de “não adota” ou “não se aplica” em direção a “iniciou plano”.

Os subitens “f” - a organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos - e “o” - a organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas – aproximaram-se ainda mais da característica “adota parcial”.

O subitem “u” - a organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações – relativo a criptografia e certificação digital manteve-se próximo a “adota parcial”.

4.4 Comparação entre itens de 2014 para 2016

Para efetuar a comparação entre itens de 2014 para 2016, inicialmente a Tabela 7, mostra os dados utilizados para realização da ANACOR. Verifica-se a concentração do item 2 em 2014 em não adota ou não se aplica e reforçando o encontrado nas Tabelas 1 e 3.

Tabela 7– Tabela de Correspondência – Comparação entre itens de 2014 para 2016

Característica	item 1 2014	item 2 2014	item 1 2016	item 2 2016	Total
não adota ou não se aplica	74	524	34	351	983
iniciou plano	60	258	76	298	692
adota parcial	45	183	34	225	487
adota integral	146	75	176	150	547
Total	325	1040	320	1024	2709

Fonte: resultado da pesquisa

A Tabela 8 mostra que a dimensão 1 representa 93,87% da inércia total e que as dimensões 1 e 2 somadas totalizam 99,57% da inércia total

Tabela 8 – ANACOR - resumo dos resultados – comparação entre itens de 2014 para 2016

Dimensão	Valor singular	Inércia	Qui-quadrado	Significância
1	0,44	0,19		
2	0,11	0,01		
3	0,03	0,00		
Total		0,20	559,33	0,00***

Legenda: ***Significante a 1,00%.
Fonte: resultado da pesquisa.

O Mapa Perceptual da Figura 4 permite identificar 3 agrupamentos, delimitados por elipses. O Mapa mostra claramente a diferença posicional dos agrupamentos, resultado que valida a divisão proposta pelo TCU.

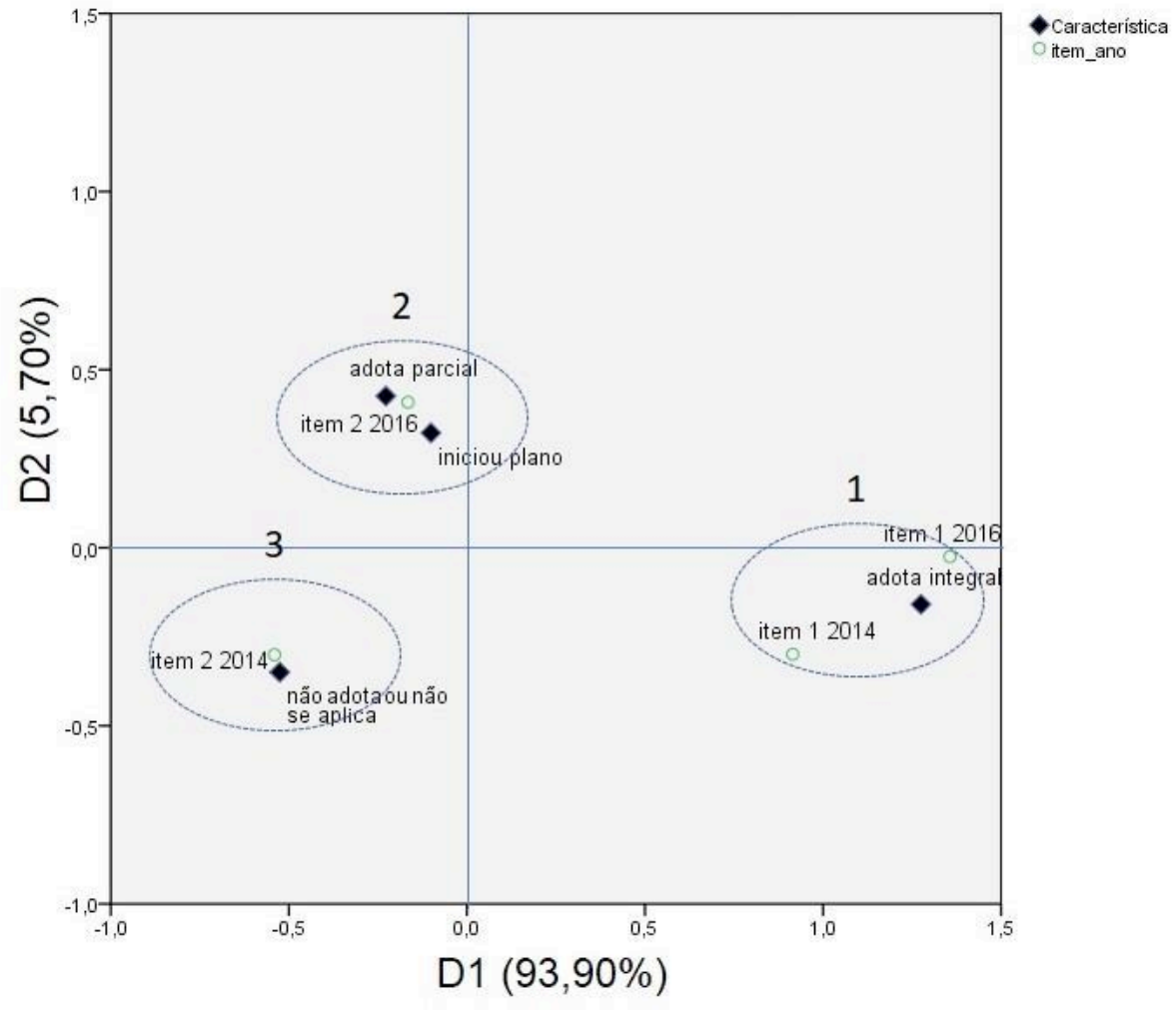

Figura 4 – Mapa perceptual – comparação entre itens de 2014 para 2016
Fonte: resultado da pesquisa
Observações: D1 é a primeira dimensão e explica 93,90% dos dados e D2 é a segunda dimensão e explica 5,70% dos dados. 'Item 1 2014' e 'Item 1 2016' referem-se às respostas

para o Item ‘Políticas e responsabilidades’ em 2014 e em 2016. ‘Item 2 2014’ e ‘Item 2 2016’ referem-se às respostas para o Item ‘Controles e atividades’ em 2014 e em 2016, A descrição dos itens e dos subitens associados a cada item consta do Quadro 2.

A elipse 1, contém o item 1 em 2014 e 2016 está próxima da característica “adota integral”. O item 1 se mostra mais uniforme e homogêneo por estar próximo a “adota integral” em ambos os períodos.

A elipse 2 contém o item 2 em 2014 estava próximo à característica não adota ou não se aplica. A elipse 3 contém o item 2 em 2016 que está na proximidade das características adota parcial e iniciou plano, mostrando o movimento realizado pelo item “Controles e atividades”, descrito no Quadro 3.

Considerando a migração do item 2 para próximo de adota parcial e iniciou plano, pode se verificar que na ótica dos entes do Judiciário houve interesse na melhoria e acreditam ter atendido, ao menos parcialmente alguns subitens do item “Controles e atividades”.

As diferenças entre os itens 1 e 2 no mapa perceptual mostram que a proposta do TCU de agrupar os subitens em ‘Políticas e responsabilidades’ e ‘Controles e atividades’ é adequada, tendo em vista que ambos apresentam perfis diferentes de comportamento de um ano para outro, considerando os resultados das análises mostrados na Figura 4.

Pode-se ainda verificar que para o item “Políticas e responsabilidades”, que abrange a parte de políticas, normas, estruturas internas e responsabilização, pela ótica dos entes do Poder Judiciário da amostra, grande parte os subitens avaliados são atendidos. Porém, no item “Controles e atividades”, que envolve os processos e atividades práticas a serem executadas, ainda existem subitens a serem aperfeiçoados.

5 Considerações Finais

O Objetivo Geral desse estudo foi analisar as características de gestão da segurança da informação dos entes do poder judiciário em 2014 e em 2016, com base em levantamentos de governança de TI do Tribunal de Contas da União.

Como principais resultados obtidos, a análise mostrou que, em 2014, a característica “não adota ou não se aplica” foi encontrada em 43,81% das respostas e “iniciou plano” foi encontrada em 23,30% das respostas. Em 2016, a característica com maior número de respostas foi “não adota ou não se aplica”, com o percentual de 28,65%, seguida de “iniciou plano” com 27,83%.

A verificação dos resíduos padronizados mostrou que houve excesso de ocorrências em 2014 e 2016 na característica “não adota ou não se aplica” para os subitens “m” - a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas -, “n” - o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído como norma de cumprimento obrigatório. -, “p” - o processo de monitoramento do uso dos recursos de TI está formalmente instituído como norma de cumprimento obrigatório. -, e “r” - o processo de gestão de incidentes de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.

Ainda na análise de resíduos, em 2014 e 2016 para os subitens “a” - a organização dispõe de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório.-, “b”- a organização dispõe de comitê de segurança da informação, formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.-, “c” - a organização possui gestor de segurança da informação, formalmente designado, responsável pelas ações corporativas de segurança da informação. - e “d” - a organização

dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída como norma de cumprimento obrigatório -, há excesso de ocorrências para a característica "adota integral".

Ao analisar a existência de diferenças entre as características da gestão de segurança da informação apuradas para 2014 e para 2016, por meio da ANACOR, observou-se mudança na adoção das práticas pelos entes do Judiciário, com o movimento dos subitens de se afastar da característica "não adota ou não se aplica" e indo em direção a "iniciou plano" e "adota parcial" e dessas últimas para "adota integral".

Os resultados da pesquisa mostram, quanto às características de gestão de segurança da informação, que no tocante a "Políticas e responsabilidades", os entes do Poder Judiciário sugerem uma adoção integral nos anos de 2014 e de 2016. Por sua vez, quanto a "Controles e atividades", os resultados dos dois anos de análise das respostas desses entes sugerem a necessidade de aprimoramentos.

Este estudo tratou um tema atual e relacionado à gestão de segurança da informação nos entes do poder judiciário. As opiniões expressas nesta pesquisa delimitam-se aos dados coletados dos levantamentos do TCU nos anos de 2014 e 2016. Como sugestões para estudos futuros, pode-se sugerir a replicação desta pesquisa em outros períodos de análise, inclusive para verificar se, na ótica dos entes do poder judiciário, a adoção de controles e atividades relacionados à gestão corporativa de segurança da informação apresentará diferenças dos resultados obtidos nesta pesquisa.

Referências

ABNT NBR ISO/IEC 27.001/2013. Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos. São Paulo: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27.002/2013. Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação. São Paulo: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27.005/2011 . Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação – Requisitos. São Paulo: Associação Brasileira de Normas Técnicas.

Batista, L. E., Escuder, M. M. L., Pereira, J. C. R. (2004). A cor da morte: Causas de óbito segundo características de raça no estado de São Paulo, 1999 a 2001. Revista Saúde Pública *38*. pag. 630. Recuperado de: http://www.scielo.br/pdf/rsp/v38n5/21749.pdf.

Beal, A. (2005). Segurança da Informação: Princípios e Melhores Práticas para a Proteção Dos ativos de Informação nas Organizações. São Paulo: Atlas.

Blasius, J., Greenacre, M. Editado por. (1998) Visualization of Categorical Data. San Diego, CA: Academic Press.

Cabinet Office. (2011). Itil® Service Strategy, (2nd ed.). Norwich, UK: The Stationery Office (TSO),

CNJ (2012). Segurança da informação diretrizes para a gestão de segurança da informação no âmbito do poder judiciário. Recuperado de: http://www.cnj.jus.br/images/dti/comite_gestao_tic/diretrizes_gestao_si_pj.pdf

CNJ (2014). Resolução 198 de 2014. Recuperado de: http://www.cnj.jus.br/atos-normativos?documento=2029.

CNJ (2015). Resolução 211 de 2015. Recuperado de: http://www.cnj.jus.br/atos-normativos?documento=2227.

CNJ (2016). Relatório de metas 2015. Recuperado de: http://www.cnj.jus.br/gestao-e-planejamento/metas

Constituição da República Federativa do Brasil de 1988. Recuperado de: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

De Haes, S., Van Grembergen, W. (2015). Enterprise Governance of Information Technology Achieving Alignment and Value, featuring Cobit (2nd ed). London: Springer.

Fávero, L. P. L., Belfiore, P. P., Júnior, M. F. F. (2006). Utilização da Anacor para a Identificação de meios de pagamento em populações de média e baixa renda. IX SEMEAD - Seminários em Administração FEA-USP, São Paulo. Recuperado de: http://sistema.semead.com.br/9semead/resultado_semead/trabalhospdf/24.pdf.

Fávero, L.P., Belfiore, P. P., Silva, F.L., Chan, B.L. (2009). Análise Multivariada de Dados: Modelagem Multivariada para Tomada de Decisões. Rio de Janeiro: Elsevier.

GSI (2009). Norma Complementar 03/IN01/DSIC/GSIPR. Recuperado de: http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

Isaca (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA. Recuperado de: http://www.isaca.org/COBIT/Pages/Product-Family.aspx.

Isaca (2016). About Cobit. Recuperado de: https://cobitonline.isaca.org/about.

Klumb, R., Azevedo, B.M. A Percepção dos Gestores Operacionais sobre os impactos gerados nos Processos de Trabalho após a Implementação das Melhores Práticas de Governança de Ti no TRE/SC. Rev. Adm. Pública — Rio de Janeiro 48(4):961-982, jul./ago. 2014. Recuperado de: http://dx.doi.org/10.1590/0034-76121651.

Lunardi, G.L. (2008). Um Estudo Empírico e Analítico do Impacto da Governança de Ti no Desempenho Organizacional. Tese de doutorado. Porto Alegre, 2008. Universidade Federal do Rio Grande do Sul.

Lunardi, G.L., Becker, J. L., Maçada, A.C.G. (2010). Impacto da Adoção de Mecanismos de Governança de tecnologia de informação (TI) no desempenho da gestão da TI: uma análise baseada na percepção dos executivos. Revista de Ciências da Administração, *12*

Florianópolis, n. 28, p. 11-39, set/dez 2010. Recuperado de: https://periodicos.ufsc.br/index.php/adm/issue/view/1576.

Lunardi, G.L., Dolci, P. (2009). Governança de ti e seus mecanismos: uma análiseda sua disseminação entre as empresas brasileiras. In: encontro de administração da informação – enadi, 2, Recuperado de: http://www.anpad.org.br/diversos/trabalhos/enadi/enadi_2009/2009_enadi196.pdf.

Medeiros, B,C, Danjour, F.M., Neto, M. V. S., Mól, A. L. R. (2016). Governança de Tecnologia da Informação: Diferenças entre Organizações Públicas Brasileiras, Gestão pública e Governança. R. Adm. Faces Journal *15* - Belo Horizonte n. 2 p. 81-99 abr./jun. 2016.

Mendonça, C.M. C., Guerra, L.C.B.G, Neto, M. V. S, Araújo, A. G. (2012). Rev. Adm. Pública — Rio de Janeiro *47* (2):443-468, mar./abr. 2013 artigo recebido em 16 jul. 2012 e aceito em 23 nov. 2012.

Monteiro, I.L.C. (2009). Proposta de um guia para elaboração de políticas de segurança da informação e comunicações em órgãos da administração pública federal. Monografia de especialização. Departamento de Ciência da Computação, Universidade de Brasília.

Netto, A.S., Silveira, M.A.P. (2007) Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias. Revista de gestão da tecnologia e sistemas de informação *4*, no. 3, 2007, p. 375-397. Recuperado de: http://www.scielo.br/pdf/jistm/v4n3/07.pdf

Oliveira, M. S. O., Peixoto, S. C., Santos, A. F., Maniçoba R. H. C., Guimarães, M. A. (2015). Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa. Recuperado em: http://periodicos.unifacef.com.br/index.php/resiget/issue/view/129.

Omar, O., Rolt, C. R. (2015). A Governança de TIC no Processo de Modernização das Serventias Extrajudiciais do Brasil. III Encontro de Internacionalização do Conpedi – *1* n. 9 Madrid, 2015. Recuperado de: http://portaltutor.com/index.php/conpedireview/article/view/33/30.

Pestana, M. H, Gageiro, J. N. (2005). Análise de Dados para Ciências Sociais – A complementaridade do SPSS (4a ed.). Lisboa: Editora Sílabo.

Pereira, C., Ferreira, C. (2015). Identificação de Práticas e Recursos de Gestão do valor das TI no Cobit 5. Revista lbérica de Sistemas e Tecnologias de Informação, Portugal,2015, nº 15, jun, p. 17-33.

Ramos, K. H. C., Vieira, T. P. B., Costa, J. P. C., Sousa, R. T. S. (2014). Multidimensional analysis of critical success factors for it governance within the brazilian federal public administration in the light of external auditing data 12th international conference on information systems & technology management – contecsi. Recuperado de: http://www.contecsi.fea.usp.br/envio/index.php/contecsi/12contecsi/paper/viewfile/3086/2402.

Sampieri, R. H. Collado, C. F. Lucio, P. B. (2013). Metodologia de Pesquisa Científica (5a ed). Porto Alegre: Penso.

Sethibe, T., Campbell, J., Mcdonald, C. (2007). IT Governance in Public and Private Sector Organisations: Examining the Differences and Defining Future Research Directions. Recuperado de https://periodicos.ufsc.br/index.php/adm/issue/view/1576.

Siegel, S., Castellan, N. (2006). Estatística não-paramétrica para Ciências do Comportamento (2ª ed.). Porto Alegre: Artmed.

STF. (2011). Sistema Judiciário Brasileiro: Organização e Competências. Recuperado de: http://www.stf.jus.br/portal/cms/vernoticiadetalhe.asp?idconteudo=169462.

Teodoro, N. A., Przeybilovicz, E., Cunha, M. A. Governança de tecnologia da informação: Uma investigação sobre a representação do conceito. Revista de Administração – Rausp *49*, são paulo, 2014, (abr./maio/jun.), p. 307-321. Recuperado de: http://www.scielo.br/pdf/rausp/v49n2/08.pdf.

Tribunal de Contas da União – TCU. (2016). Referências do questionário de governança de ti 2016. Recuperado de: http://portal.tcu.gov.br/comunidades/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/.

Van Grembergen, W., de Haes, S., Guldentops, E. (2004) Structures, Processes and Relational Mechanisms for IT Governance. Idea Group Publishing, 2004. Recuperado de: http://www.antwerpmanagementschool.be/media/287503/it%20gov%20theories%20and%20practices.pdf.