XX SEMEAD
Seminários em Administração

novembro de 2017
ISSN 2177-3866

BOAS PRÁTICAS DE GOVERNANÇA DE TI ADOTADAS PELOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA

MÁRCIA NÉA OLIVEIRA PASCOAL
UNIVERSIDADE DE FORTALEZA (UNIFOR)
marcianea@bnb.gov.br

ODERLENE VIEIRA DE OLIVEIRA
UNIVERSIDADE DE FORTALEZA (UNIFOR)
oderlene@hotmail.com

BOAS PRÁTICAS DE GOVERNANÇA DE TI ADOTADAS PELOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA

1 INTRODUÇÃO

A cada ano tem crescido a preocupação com a vulnerabilidade das instituições públicas e privadas à instabilidade e à crise. Para remediar possíveis falhas essas instituições vêm se utilizando de boas práticas de governança corporativa (ABBOTT; SNIDAL, 2000). A adoção de boas práticas de governança corporativa é fator chave de crescimento corporativo sustentável e vantagem competitiva a longo prazo, pois gera valor para o acionista, além de posicionar a empresa como líder de mercado quando esta possui acesso rápido e fácil a informações confiáveis sobre seu negócio (MADHANI, 2008). Estas práticas devem ser introduzidas na organização, normatizadas para que possam ser legitimadas (ROSSONI; MACHADO-DA-SILVA, 2010).

Quando o assunto é boas práticas de governança corporativa não se pode deixar de mencionar um momento-chave na história da governança corporativa, que foi a publicação, em 1992, do Relatório *Cadbury*, tido como o melhor modelo de boa prática no Reuno Unido (KEAY, 2014) como também no mundo (HENRY, 2008; JORDAN, 2013). De acordo com Jones e Pierce (2013) o Relatório Cadbury serviu de inspiração para o desenvolvimento dos códigos de boas práticas de governança corporativa em todo o mundo. Vale também destacar a iniciativa da África do Sul com o lançamento de seu III Código de Governança, em setembro de 2009, conhecido como King III, que trouxe pela primeira vez a importância da Governança de TI para as boas práticas de governança corporativa. A TI passou a ser vista como uma parceira estratégica que pode criar oportunidades e aumentar a competitividade da organização (MASSON et al., 2014). Gheorghe (2011) explana que a Governança de TI surgiu dos esforços do Conselho de Administração no intuito de obter um melhor desempenho em um ambiente de elevada competição e garantir uma melhor transparência.

A Tecnologia da Informação foi considerada por muito tempo pela Administração Pública como uma ferramenta auxiliar, uma variável mediadora na análise do desempenho da administração pública e dos governos (CEPIK; CANABARRO; POSSAMAI, 2010). Com o passar dos anos, a TI assumiu a responsabilidade não somente de gerar, mas gerenciar o conteúdo das informações, mantendo a eficiência, e assim, desempenhando um papel fundamental na transformação da administração pública, passando de gestão de objeto para objeto de governança (HOLDEN, 2007).

Assim, observa-se que as práticas de governança estão presente nos setores público e privado aos quais são aplicados os mesmos princípios de governança corporativa: *accountability* (responsabilização), transparência e conduta ética empresarial. As principais diferenças entre estes setores residem no fato que o valor agregado pela governança deve atingir o setor privado por meio de lucro, totalmente voltado para a parte financeira, enquanto que o setor público, visa principalmente a maximização do bem-estar da sociedade considerando seus interesses e necessidades. E sobre as metas, devido a limitação de *stakeholders*, papéis bem definidos, o setor privado consegue esclarecer melhor suas metas; sobre o setor público, a meta é complexa, pois há variedade de *stakeholders* (sociedade) e dificuldade em mensurar a meta e se o alcance foi satisfatório (MADHANI, 2014).

Devido a essas diferenças entre os setores público e privado é que o Comitê do Setor Público (PSC) da Federação Internacional de Contadores (IFAC) dedica-se à coordenação mundial das necessidades do setor público pertinente a governança e a gestão pública. Nesse sentido, em 2001, o PSC/IFAC publicaram um estudo que define princípios e recomendações com o objetivo de promover, orientar e auxiliar o grupo de governantes a aplicar ou rever as práticas de governança, visando uma gestão mais capacitada e conseguintemente mais efetiva, eficiente e transparente (SILVEIRA; GOULART, 2016).

Observa-se também um movimento, nas duas últimas décadas, no desenvolvimento de modelos de boas práticas de governança de TI, que parecem ajustar-se às aspirações dos acionistas e do mercado, em geral, de garantir que as ações de TI estejam alinhadas com a estratégia das organizações, contribuindo para o atingimento dos objetivos (TAROUCO; GRAEML, 2011). Tendo como base todas estas referências que apóiam a realização da governança de TI nas organizações, o Tribunal de Contas da União (TCU) elaborou o Referencial Básico de Governança, aplicável a órgãos e entidades da Administração Pública (TCU, 2014), tido como um código de boas práticas de governança de TI para a administração pública.

Assim, na presente investigação definiu-se a seguinte questão de pesquisa: Quais as boas práticas de Governança de TI que estão sendo adotadas pela Administração Pública Federal Brasileira? Assim, o objetivo geral consistiu em identificar as boas práticas de Governança de TI adotadas pelos órgãos da Administração Pública Federal Brasileira.

Em pesquisa realizada por Pascoal e Oliveira (2017) com o objetivo de identificar a adoção de boas práticas em governança corporativa nos órgãos da APFB foi evidenciado que dentre as variáveis de assunto específico do questionário do ano de 2014, havia uma menor adoção de práticas referentes à Gestão de Risco e Gestão de Continuidade, o que motivou inicialmente a realização da presente investigação. Outra justificativa foi o fato de as práticas de governança de TI envolver a gestão de riscos e esta, por sua vez, trata dos riscos relacionados à segurança da informação. Nesse sentido, estudos sobre a adoção de boas práticas de governança de TI é de grande interesse por parte dos gestores e demais envolvidos na definição de boas práticas de gestão de riscos de segurança da informação por proporcionar maior controle quanto às incertezas e o impacto destas no objetivo do negócio (SOUZA et al., 2016).

2 REFERENCIAL TEÓRICO

2.1 Boas práticas de governança de TI

Nas duas últimas décadas, vêm surgindo vários modelos de boas práticas de governança de TI, que parecem ajustar-se às aspirações dos acionistas e do mercado, em geral, de garantir que as ações de TI estejam alinhadas com a estratégia das organizações, contribuindo para o atingimento dos objetivos Os modelos de boas práticas de governança de TI apontados como os de utilização mais frequente nas empresas são: ITIL, COBIT, PMBok, BS 7799, ISO/IEC 17799 e ISO/IEC 27001 (TAROUCO; GRAEML, 2011). Considerando que o COBIT 5 integra todos os demais modelos citados, a seguir foca-se na descrição apenas desse modelo.

Ao mencionar o termo Boas Práticas de Governança Corporativa na área de Tecnologia da Informação, a referência que os profissionais e gestores de TI conhecem ou já ouviram falar é o documento *Control Objectives for Information and related Technology* (COBIT) desenvolvido e publicado pelo *Information System Audit and Control* (ISACA), atualmente na versão 5, de 2012. É considerado um Modelo Corporativo para Governança e Gestão de TI da Organização, também é conhecido como guia de boas práticas de gestão e governança dos processos de TI e tido como referência para os gerentes e auditores.

É um modelo abrangente que apóia as empresas no atingimento de seus objetivos de governança e gestão de TI, criando valor por meio da TI equilibrando a realização de benefícios e a otimização dos níveis de risco e uso de recursos. Também permite visibilidade da TI por toda a organização, compreendendo todo o negócio, considerando os interesses internos e externos vinculados com a TI. Este modelo, COBIT 5, por ser genérico, pode ser utilizado por organizações de qualquer porte, comerciais, sem fins lucrativos ou públicas (DOURADO, 2015). Este *framework*, atendendo o princípio de ser uma base para integrar modelos, padrões e práticas como modelo único, fez uso de conceitos e princípios divulgados pelo ISACA (ISACA, 2012): a) COBIT 4.1; b) Val IT, conjunto de princípios direcionadores

e de processos e boas práticas para apoiar e ajudar a gestão executiva em nível empresaria, mas também, pode ser utilizado para criar valor para o negócio por meio de investimentos de TI; c) Risk IT, auxilia na gestão de risco de TI; d) *Business Model for Information Security* (BMIS), oferece uma abordagem ampla e orientada ao negócio para a gestão de segurança da informação; e) *IT Assurance Framework* (ITAF), modelo orientador sobre a concepção, execução e relatório de auditoria de TI, possui termos e conceitos específicos para a garantia de TI; e f) *Board Briefing on IT Governance*, um livreto de referência para disciplinar, de forma abrangente, o *board* e gestão executiva quanto aos conceitos de governança de TI.

Ainda dentro do arcabouço de ferramentas, o *Taking Governance Forward (TGF)* é um recurso que fornece um portal de acesso a todos os assuntos relacionados a governança (ISACA, 2012). E quando há necessidade, o COBIT 5 conecta-se também com outros padrões e modelos de mercado mundialmente conhecidos com o objetivo de apoiar as partes interessadas a compreender como que todo este conjunto de boas práticas se inter-relacionam e como podem ser usadas ao mesmo tempo (ISACA, 2012). São estas: *Information Technology Infraestructure Library* (ITIL); *The Open Group Architecture Framework* (TOGAF); *Project Management Body of Knowledge* (PMBOK); *PRojects IN Controlled Environments 2* (PRINCE2); *Committee of Sponsoring Organizations of the Treadway Comission* (COSO); e *International Organization for Standardization* (ISO).

De acordo com Dourado (2015, p. 6) "o COBIT 5 auxilia as organizações na criação de valor para TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos." Tem como objetivos: a) oferecer um *framework* abrangente que auxilia as organizações a otimizar o valor gerado pela TI; b) permitir que a TI seja governada e gerenciada de forma holística para toda a organização; e c) criar uma linguagem comum entre TI e negócios para a governança e gestão de TI corporativa.

O COBIT 5 (ISACA, 2012) fundamenta-se em cinco princípios básicos para governança e gestão de TI na organização, conforme exposto na Figura 1.

Figura 1 - Princípios do COBIT 5

Fonte: COBIT 5 (ISACA, 2012, p.15).

Tendo todas estas referências que apóiam a realização da governança de TI nas organizações, o Tribunal de Contas da União (TCU) elaborou o Referencial Básico de Governança, aplicável a órgãos e entidades da Administração Pública (TCU, 2014), tido como um código de boas práticas de governança de TI para a administração pública.

O Referencial Básico de Governança do TCU, trata-se

> [...] de documento que reúne e organiza boas práticas de governança pública que, se bem observadas, podem incrementar o desempenho de órgãos e entidades públicas.

> Além de esclarecer e incentivar os agentes públicos na adoção de boas práticas de governança, este Referencial se torna um guia para as ações do próprio TCU na melhoria de sua governança interna. Com efeito, algumas de nossas ações se pautaram nas referidas boas práticas ou mesmo inspiraram a sua definição (TCU, 2014, p. 6).

A adoção de modelos de boas práticas de governança de TI repercute positivamente no aumento da visibilidade dos executivos sobre o retorno de investimentos em TI e no aumento do controle e da qualidade dos serviços prestados pela TI (TAROUCO; GRAEML, 2011).

Determinar qual o modelo adequado para implementar a Governança de TI em uma organização é uma missão crítica, pois uma abordagem que se adapta a uma organização não necessariamente funcionará em outra (PATEL, 2004). De Haes e Van Grembergen (2006) ressaltam que conceber o modelo de Governança de TI é o primeiro passo e que o desafio seguinte é implementá-lo na organização como uma solução sustentável.

Os fatores determinantes para a adoção de modelos de boas práticas de governança de TI estão relacionados à crescente demanda por monitoramento e controle organizacional, à exigência de transparência pelos acionistas e pelo mercado, ao aumento da complexidade da tecnologia, e ao fato de as áreas de negócio estarem cada vez mais dependentes da TI (TAROUCO; GRAEML, 2011).

2.2 Gestão de Riscos de TI

Risco é a possibilidade ou probabilidade de perigo, um inconveniente, algo que ameaça (AURÉLIO, 2017). No mesmo contexto, risco poderá levar a um prejuízo ou insucesso no alcance de um objetivo decorrente de uma incerteza e que independe de ações dos envolvidos (MICHAELIS, 2017). Juridicamente, risco é a "possibilidade de evento futuro e incerto em sua extensão, somente provável depois de ocorrido, e capaz de acarretar prejuízo e consequente responsabilidade pela reparação" fundamentado no Código Civil Brasileiro, art. 492 e Código Comercial, art. 667 (SIDOU, 2016). E, conforme a norma ABNT ISO 73:2009 (ABNT, 2009a), risco representa "efeito das incertezas nos objetivos", ou seja, um impacto direto ou indireto, positivo ou negativo, que desvia do caminho planejado para o alcance dos objetivos.

Consolidando, risco é a possibilidade da ocorrência de uma incerteza que impacta direta ou indiretamente, positiva ou negativamente, o alcance de um objetivo e que independe da vontade dos envolvidos, porém, requer responsabilidade na reparação do prejuízo ocasionado por esta ocorrência. Tendo em vista a questão da incerteza e a "impotência" dos envolvidos diante os riscos, a gestão dos riscos é uma resposta para que a organização seja munida de controles que monitorem as incertezas, conhecidas ou não, a fim de evitar e se posicionar respondendo de forma a mitigar, evitar, transferir ou eliminar o risco (SANTOS; SILVA, 2014).

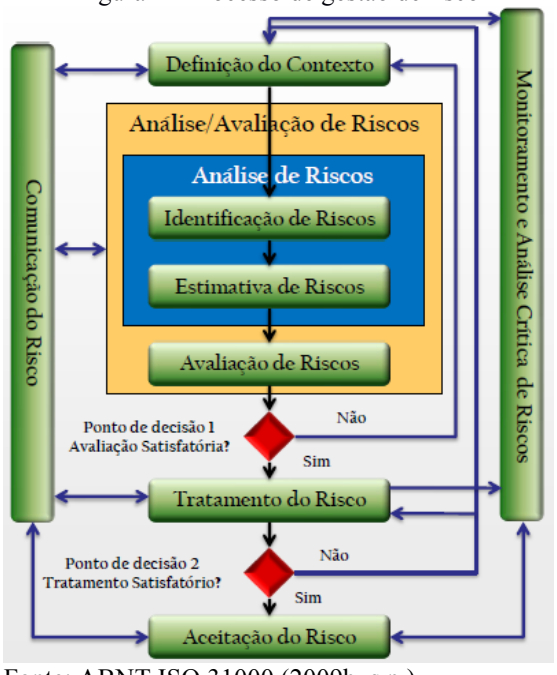
Em se tratando de TI, os processos incorporam riscos específicos e devem ser devidamente abordados para que os dirigentes não incorram em violações de: normas de segurança da informação, legislação de privacidade, legislação de *spam*, legislação de práticas de comércio, direito de propriedade intelectual (incluindo acordos de licenças de *software*), exigências de registro de informações, legislação e regulamentações ambientais, legislação de saúde e segurança, legislação de acessibilidade, e normas de responsabilidade social, em acordo com a norma ABNT ISO 31000:2009 (ABNT, 2009b).

Partindo destas premissas, a gestão de risco faz-se necessária sob o ponto de vista de uma empresa que preza pela boa governança a fim de garantir o alcance dos objetivos definidos na instância estratégica pelo Conselho de Administração com o intuito de se obter resultados, sejam financeiros ou não, em busca de sua sustentabilidade no mercado. Inferindo-se que, não tem como dissociar a governança da gestão de risco como seu principal meio de dirigir uma empresa (COSTA, 2012).

A norma supracitada defende a empresa por meio de princípios que devem permear todos os níveis hierárquicos para que este processo alcance sua eficácia. Então, a gestão de riscos (ABNT, 2009b): a) cria e protege valor - melhora o desempenho da empresa sobre à segurança física e conformidade legal e regulatório; b) é parte integrante de todos os processos organizacionais - a gestão de riscos é de responsabilidade da alta administração e é parte dos processos organizacionais, principalmente o planejamento estratégico, como todos os processos de gestão de projetos e gestão de mudanças; c) é parte da tomada de decisões - auxilia nas escolhas conscientes e na priorização de ações, pois distingue entre várias alternativas reconhecendo as consequências de cada uma; d) aborda explicitamente a incerteza - a gestão de riscos explicita a consideração da incerteza, a natureza dela e como pode ser tratada; e) é sistemática, estruturada e oportuna - contribui para a eficiência e os resultados consistentes, comparáveis e confiáveis; f) baseia-se nas boas informações disponíveis - para melhor gerenciar os riscos, faz-se uso de várias fontes de informação, como dados históricos, experiências, retroalimentação dos stakeholders, observações, previsões e outros. Considerando a possibilidade de divergência entre as fontes como limitações existentes; g) é feita sob medida - a gestão de risco deve estar alinhada com o contexto interno e interno da organização e com o perfil de risco inerente ao produto ou serviço oferecido; h) considera fatores humanos e culturais - reconhece capacidades, percepções e intenções de todos os stakeholders, internos e externos, em todos os níveis da organização que colaboram ou dificultam a realização dos objetivos estabelecidos; i) é transparente e inclusiva - envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis hierárquicos, pois todas as opiniões são consideradas na determinação dos critérios de risco, assegura que a gestão de riscos permaneça consistente e atualizada; j) é dinâmica, iterativa e capaz de reagir à mudanças - a gestão de risco está em constante mudança provocada por eventos de naturezas adversas e precisa reagir diante as adversidades e adaptar os planos de resposta, porque outros riscos aparecem, outros desaparecem, e necessita de constante atualizações; e k) facilita a melhoria contínua da organização - à medida que a gestão de riscos se desenvolve e implementa estratégias para melhorar a maturidade em riscos, toda a organização é impactada positivamente.

A Figura 2 demonstra o fluxo da gestão de risco com as atividades inerentes às boas práticas:

Figura 2 - Processo de gestão de risco



Fonte: ABNT ISO 31000 (2009b, s.p.).

O processo de gestão de risco proposto pode ser utilizado em todos os processos organizacionais, inclusive aplicado sobre os processos de TI, aos quais o trabalho se propõe a identificar a existência destas práticas na APFB.

Como resposta ao risco, a norma ABNT NBR ISO 15999-1:2008 (ABNT, 2008) estabelece que a Alta Administração deverá definir uma política de continuidade de negócio alinhado ao propósito da organização, estabelecendo e atendendo requisitos e manter a melhoria contínua do Sistema de Gestão de Continuidade de Negócio (SGCN).

Figura 3 - Relacionamento da Gestão de Risco e demais disciplinas tratadas neste trabalho

Fonte: Adaptado pela autora com base em Prado Júnior (2013, s. p.).

Para facilitar o que foi explanado, apresenta-se a interligação da gestão de risco com as disciplinas de Continuidade de negócio e Segurança da Informação na Figura 3.

3 METODOLOGIA

A pesquisa caracteriza-se, quanto ao tipo, como descritiva e documental (BRYMAN; BELL, 2011), e quanto ao método, como quantitativa (NEUMAN, 1997).

A coleta de dados foi realizada com base em dados secundários do TCU levantados em 2010, 2012 e 2014, mediante a aplicação de questionários, em 301, 349 e 372 órgãos classificados em segmentos, respectivamente, e abrangeu os temas relacionados à governança de TI em órgãos públicos da APFB, conforme exposto no Quadro 1.

Quadro 1: Segmentos das empresas participantes do Levantamento de Governança de TI 2014

Segmento	Descrição
EXE-Dest	Empresas públicas federais e as sociedades de economia mista
EXE-Sisp	Organizações que fazem parte do Sistema de Administração dos Recursos de Informação e Informática (SISP)
JUD	Organizações do Poder Judiciário
LEG	Organizações do Poder Legislativo
MPU	Organizações que constituem o Ministério Público da União (MPU)
Terceiro Setor	Organizações que não se enquadrem em nenhum dos segmentos anteriores

Fonte: elaborada pela autora com base nos dados do TCU (2014).

Assim, foram selecionadas variáveis por meio de consulta às palavras “risco” e “continuidade” sobre as questões e seus subitens para que se identificassem práticas relacionadas à disciplina de risco constante nos questionários dos anos estudados: 2010, 2012 e 2014. As variáveis foram agrupadas em áreas: Corporativa, Segurança da Informação e TI. Apesar da Segurança da Informação constar de uma disciplina da TI, ela é peculiar quanto aos seus processos e geralmente tem tratamento diferenciado na literatura. Após esta análise, as variáveis foram identificadas entre os anos a fim de viabilizar a comparação entre elas. Desta forma, apresentam-se 19 variáveis presentes nos questionários analisados, que foram organizadas conforme exposto no Quadro 2.

Os itens selecionados para a análise na pesquisa aferem objetivamente os aspectos relativos à Governança TI amparados no Referencial Básico de Governança (TCU, 2014), ABNT NBR ISO 15999-1:2008 (ABNT, 2008), ABNT NBR ISO 31000:2009 (ABNT, 2009b) e outros modelos e boas práticas de governança de TI.

Quadro 2 - Classificação das variáveis quanto à natureza

Grupo	Área	Prática	Variável
Continuidade	Corparativa	Institucionalizar política corporativa de gestão de continuidade do negócio	ProcGestContin
	TI	Institucionalizar o processo gestão da continuidade dos serviços de TI	ProcGestContinTI
		Executar processo de gestão da continuidade dos serviços de TI conforme plano pré-definido	PlanContinTI
Risco	Corporativa	Institucionalizar política corporativa de gestão de riscos	GestRiscoCORP
	Segurança da Informação	Institucionalizar o processo de gestão de riscos de segurança da informação	ProcGestRiscoSEGINF
		Executa processo de gestão de vulnerabilidades técnicas de TI	ExVulneraSEGINF
		Executar o processo de gestão de riscos de segurança da informação	AnaRiscoCritNegSEGINF
	TI	Analisar dos riscos quanto à contratação	AnaRiscoContrato
		Apetite ao risco	ApetiteRisco
		Auditoria Interna avalia a gestão de risco instituída	AuditAvalRG
		Auditoria Interna avalia os riscos críticos ao negócio	AuditRisco
		Avaliar os riscos de TI críticos ao negócio	AvRiscoTI
		Definir diretrizes de gestão de riscos de TI	DiretrGR
		Executar processo de gestão de riscos de TI	ExRiscoTI
		Identificar riscos de TI de processos críticos de negócio	IdRiscoTI
		Institucionalizar papéis e responsabilidades pela gestão de riscos de TI	P&R-GR
		Institucionalizar o processo de gestão de risco de TI	ProcGestRiscoTI
		Realizar tomada de decisões estratégicas com base no apetite ao risco de TI definidos	TomDecGR
		Trata os riscos de TI dos processos críticos de negócio seguindo o plano de tratamento de risco	TrRiscoTI

Para analisar os dados foi aplicada estatística descritiva, com o uso da média e contagem de frequência das respostas (MORETTI; CAMPANARIO, 2009); posteriormente foi feito uma análise horizontal entre as variáveis coincidentes dos anos de 2010, 2012 e 2014 complementada com uma análise horizontal destas variáveis com as demais do ano de 2014 (que apresenta maior detalhamento quanto às práticas), concluindo esta análise com uma inferência da autora demonstrando as variações e as suposições envolvidas com base nos dados. E por fim, aplicou-se regressão linear múltipla (CORRAR *et al*., 2007; GUJARATI, 2000) para a base de dados de 2014 a fim de se mostrar a fórmula relacionada à base de dados que explica a adoção das práticas de governança corporativa por meio das práticas adotadas nos setores de TI dos órgãos públicos. Para a obtenção dos resultados estatísticos foram utilizados os *softwares Microsoft Excel* e *STATA*.

4 RESULTADOS E ANÁLISE

Utilizando-se estatística descritiva, foi realizado a contagem da frequência e percentual das respostas quanto à adoção das práticas relacionadas no Quadro 4 (exposto na seção de metodologia) por ano consultado, conforme exposto na Tabela 1.

Do exposto na Tabela 1, observa-se que a cada ciclo (bienal) da aplicação dos questionários, o assunto "Risco" e "Continuidade" tem se tornado mais relevante em acordo com a evolução quantitativa da presença de 3 variáveis em 2010, 6 em 2012 e 19 em 2014.

A análise será iniciada pela comparação dos resultados da contagem das frequências das variáveis de adoção de práticas que coincidem nos três anos e dois últimos anos do

questionário (coluna "Análise Horizontal"), entre variáveis afins de 2014 com as da Análise Horizontal (coluna "Análise Vertical"), e por fim, a coluna "Inferência" com a consolidação dos achados e pressupostos que ocasionaram os resultados elaborado pela autora.

Tabela 1 - Adoção de Práticas - média e frequência das respostas prática por ano

Grupo	Área	Variável	2010		2012		2014	
			Qtd	%	Qtd	%	Qtd	%
Continuidade	Corparativa	ProcGestContin					99	26,61
	TI	ProcGestContinTI	21	6,98	60	17,19	38	10,22
		PlanContinTI	10	3,32	20	5,73	110	29,57
Risco	Corporativa	GestRiscoCORP					82	22,04
	Segurança da Informação	ProcGestRiscoSEGINF					56	15,05
		ExVulneraSEGINF					163	43,82
		AnaRiscoCritNegSEGINF	49	16,28	33	9,46	94	25,27
	TI	AnaRiscoContrato					254	68,28
		ApetiteRisco					53	14,25
		AuditAvalRG					69	18,55
		AuditRisco			52	14,90	102	27,42
		AvRiscoTI					128	34,41
		DiretrGR			27	7,74	93	25,00
		ExRiscoTI					76	20,43
		IdRiscoTI					139	37,37
		P&R-GR					96	25,81
		ProcGestRiscoTI			16	4,58	51	13,71
		TomDecGR					79	21,24
		TrRiscoTI					76	20,43

A seguir, as análises do grupo de práticas de governança de "Continuidade" entre os três anos de variáveis coincidentes (Análise horizontal - AH) e a comparação das mesmas variáveis deste grupo (Análise vertical - AV) para o ano de 2014, conforme apresentado na Tabela 1 - Adoção de práticas - média e frequência das respostas por prática por ano:

1. AH - Variável/prática ProcGestContinTI (Institucionalizar o processo de gestão da continuidade de serviços de TI) - Na análise dos dados observou-se que 21 órgãos públicos da APFB, equivalente a aproximadamente 7% dos respondentes, afirmaram a existência deste processo na TI em 2010. Em 2012, esta prática teve um crescimento de 300% na quantidade de respondentes, representando 17% do total de órgãos públicos que afirmaram adotar esta prática. Em 2014, há um decréscimo de adoção a referida prática.
2. AH - Variável/prática PlanContinTI (Executar o processo de gestão da continuidade dos serviços de TI conforme plano pré-definido) - Quanto à existência do Plano de Continuidade de serviços de TI em órgãos públicos, registra-se que, em 2010 e 2012, há adoção do processo de gestão de continuidade de serviços na TI, mas somente alguns órgãos elaboraram um plano. Ainda assim, é observado uma evolução na adoção de Plano de Continuidade, mesmo que esta mesma curva de evolução não seja acompanhada pela instituição da prática, como visto na análise da variável anterior.
3. AV - Comparando a adoção da prática de Gestão de Continuidade do negócio de forma corporativa (ProcGestContin) com a adoção deste mesmo processo na área de TI, foi realizada uma análise vertical considerando as duas variáveis mencionadas nos itens anteriores somente para o ano de 2014. Conforme os dados apresentados nas respostas, de 372 órgãos públicos da APFB que fizeram parte deste questionário, 99 possuem o processo de gestão de continuidade de negócio corporativo, 38 possuem o processo de gestão de continuidade de serviço de TI e 110 afirmaram executar o processo de gestão continuidade conforme um plano pré-definido. E assim, para a variável/prática "Continuidade", infere-se que, apesar

da baixa adesão em se institucionalizar um processo de continuidade corporativo ou de TI, existe um plano a seguir em casos de resposta aos riscos pelos quais a instituição está exposta.

A seguir, as análises do grupo de práticas de governança de "Risco" entre os três e dois anos de variáveis coincidentes (AH) e a comparação das mesmas variáveis deste grupo (AV) para o ano de 2014 conforme apresentado na Tabela 1 - Adoção de práticas - média e frequência das respostas por prática por ano:

1. AH - Variável/prática AnaRiscoCritNegSEGINF (Executar o processo de gestão de riscos de segurança da informação) - Ressalte-se que em 2010, do total de 301 órgãos respondentes, 49 órgãos apreendem que realizam a análise dos riscos sobre as informações críticas para o negócio, considerando-se que não basta armazenar e prover soluções automatizadas, a TI também precisa assegurar a integridade das informações e a disponibilidade destas para a tomada de decisão e outras necessidades em tempo hábil com a devida confiabilidade. Ocorre que em 2012, de 349 respondentes, 33 órgãos validaram esta afirmação. Já em 2014, 25,27% dos órgãos apresentaram a adoção desta prática, superando mais do dobro dos anos anteriores, reconhecendo a necessidade de se analisar a exposição das informações ao risco.
2. AH - Variável/prática AuditRisco (Auditoria interna avalia os riscos críticos ao negócio) - quanto à existência de um plano de auditoria interna para avaliar os riscos considerados críticos para o negócio e a eficácia dos respectivos controles, entende-se que, se a instituição deve ou é recomendado possuir processos definidos e executados voltados a gestão de risco, faz-se necessário auditar a eficácia destes controles dentro do órgão. Quase 15% dos respondentes elaboravam um plano de auditoria interna baseada em riscos em 2012, e em 2014, este número duplicou. Ou seja, cada vez mais a equipe da auditoria interna considera os riscos em seus trabalhos.
3. AH - Variável/prática DiretrGR (Definir diretrizes de gestão de risco de TI) - Diretriz é uma norma, indicação ou instrução que serve de orientação (AURÉLIO, 2017). Em 2012, apenas 7,74% dos respondentes definiram suas diretrizes de gestão de risco de TI, e em 2014, 25% passou a adotar esta prática, levando a crer que há um entendimento por parte dos órgãos públicos quanto às diretrizes de gestão de risco de TI.
4. AH - Variável/prática ProcGestRiscoTI (Institucionalizar o processo de gestão de risco de TI) - Em 2012, apenas 4,58% dos respondentes possuem processo de gestão de risco de TI, e em 2014, esta prática teve uma maior adesão apresentando 13,71%.
5. AV - Variáveis/práticas agrupadas sobre Segurança da Informação que se apresentam em 2014 (ProcGestRiscoSEGINF - institucionalizar o processo de gestão de risco da Segurança da Informação; ExVulneraSEGINF - executar o processo de gestão de vulnerabilidades técnicas de TI; e, AnaRiscoCritNegSEGINF - executar o processo de gestão de riscos de segurança da informação) - analisando as práticas para a área de Segurança da Informação no ano de 2014, 15% dos órgãos da APFB possui um processo de gestão de risco voltado para a segurança da informação, por outro lado, ratifica-se a execução de um processo de gestão de vulnerabilidades técnicas de TI, com quase 44% de adesão à prática, como resposta de mitigar os riscos relativos a esta área, como também, executa uma parte do processo de gestão de riscos quanto à análise dos riscos da exposição das informações críticas de negócio.

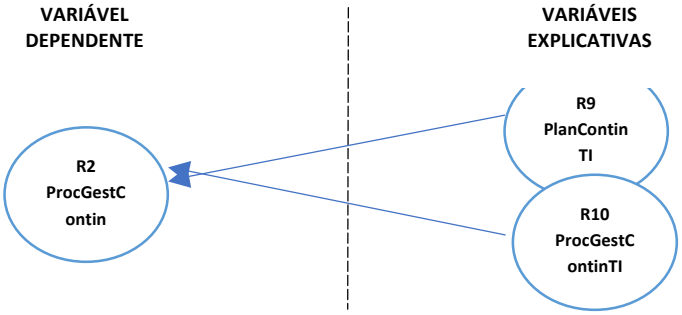
6. AV - Variáveis/práticas agrupadas sobre TI que se apresentam em 2014 (AnaRiscoContrato - analisar dos riscos quanto à contratação; ApetiteRisco - apetite ao risco; AuditAvalGR - auditoria avalia a gestão de risco instituída; AuditRisco - auditoria interna avalia os riscos críticos ao negócio; AvRiscoTI - avaliar riscos de TI críticos ao negócio; DiretrGR - definir diretrizes de gestão de riscos de TI; ExRiscoTI - executar processo de gestão de risco de TI; IdRiscoTI - identificar riscos de TI de processos críticos de negócio; P&R_GR - institucionalizar papéis e responsabilidades pela gestão de riscos de TI; ProcGestRiscoTI - institucionalizar processo de gestão de risco de TI; e, TomDecGR - realizar tomada de decisões estratégicas com base no apetite ao risco de TI definidos) - Comparando as práticas ApetiteRisco, AuditAvalGR e AuditRisco, apesar de todas apresentarem percentual muito baixo quanto à adoção, é perceptível que há um plano de auditoria para a instituição em maior número para as áreas de negócio (AuditRisco), mas para a TI (AuditAvalGR) tem-se um número menor, e, há uma definição, em poucos órgãos, do nível de risco que possa assumir, subsidiando a auditoria de parâmetros para seu trabalho. Concluindo que ainda é necessário ampliar esta prática a fim de garantir a eficácia da execução dos processos de gestão de risco. Quanto às demais práticas de governança de Risco, analisou-se que de 2012 para 2014 há um crescimento na adoção de processo de gestão de risco de TI e definição de diretrizes que norteiam a gestão de TI, ainda assim, foi observado que em 2014, nas demais variáveis, existem atividades em realização sem um processo de gestão de risco de TI mapeado, ou seja, existem ações isoladas sem um processo que as suporte.

Conforme posição de 2014 tem-se que 82 órgãos possuem o processo de Gestão de Risco Corporativo instituído. Vale ressaltar que, independente da adoção da prática corporativa, a área de Segurança da Informação considera e executa meios para evitar as vulnerabilidades que atingem a informação crítica de negócio e, na esfera de TI, apresenta-se uma preocupação que perpassa a maioria dos órgãos no tocante à análise dos riscos inerentes à contratação. Ratifica-se a adoção de práticas de gestão de risco de TI independente das iniciativas corporativas, quando da identificação e avaliação dos riscos de TI apresentam maior número de órgãos que afirmam adotar tais práticas, mesmo estes que não possuam um processo de gestão de risco próprio de TI, há atividades em realização de forma isolada. Quanto às diretrizes da gestão de riscos, considerando-se a quantidade de órgãos que adotaram o processo de gestão de risco corporativo, a TI buscou as diretrizes que norteiam a sua gestão de risco, provavelmente, alinhada aos preceitos do processo corporativo.

Posteriormente, a fim de ampliar a exploração dos dados desta pesquisa, foram realizadas duas regressões lineares múltiplas usando isoladamente a base de 2014, devido a existência de 5 níveis de respostas (domínios) qualitativos (CORRAR et al, 2007; GUJARATI, 2000). Conforme as classificações da Tabela 1, foram selecionadas as duas variáveis das área corporativas "Continuidade" e "Risco", Gestão de Risco Corporativo (GestRiscoCORP) e Gestão de Continuidade do Negócio (ProcGestContin), para identificar a influência da existência destes processos sobre os relacionados à TI, tendo em vista que o fato da Alta Administração não possuir um processo corporativo referencial, não quer dizer que uma outra área, seja TI ou negócio, não possua meios de realizar uma governança setorial adotando práticas sem alinhamento estratégico.

Para a primeira regressão linear múltipla foi selecionada como variável dependente para o grupo "Continuidade", Gestão de Continuidade do Negócio (ProcGestContin) pertencente à área corporativa como primeira hipótese, conforme exposto na Figura 4.

Figura 4 - Hipótese 1- as respostas para a existência de um plano de continuidade corporativa NÃO influencia a existência de um Processo de Gestão de Continuidade de TI e de um Plano de Continuidade de TI.



Fonte: elaborado pelas autoras.

A fim de testar a hipótese 1, foi feito uso de técnica estatística de econometria para modelos de escolhas qualitativas para variáveis *dummies* (binárias) gerando uma regressão linear múltipla devido a hipótese sugerir mais de uma variável explicativa. Dentre os modelos que suportam esta técnica, o Logit apresentou-se mais adequado devido se trabalhar com dados individuais (por órgão).

A disposição dos dados da variável "ProcGestContin" da base de dados de 2014, foi transformada para binária, representando a variável regressando (y na equação), sendo: "0" - não adota a prática, agrupando as respostas "não se aplica", "não adota", e "iniciou plano"; e, "1" - adota a prática, agrupando as repostas "adota parcialmente" e "adota integralmente" (parcialmente ou integralmente, pois ambas as respostas dependem da realidade do órgão e a customização do processo fica sob o critério do órgão público). As variáveis explicativas (independentes) foram mantidas com os 5 níveis de resposta a fim de apresentar as probabilidades do órgão público adotar a prática "ProcGestContin", ou seja, a variável dependente *dicotômica* (y) igual a 1; com base nas respostas para as variáveis explicativas "PlanContinTI" e "ProcGestContinTI".

Tabela 2 - Dados da regressão linear múltipla da variável dependente Processo de Continuidade de Negócio Corporativa com previsão de confiabilidade (P) até 5%. Modelo Logit.

Variáveis	Coeficiente	Erro Padrão	Z	P>|Z|
Constante	-3,803941	0,4870328	-7,81	0,010
PlanContinTI	0,4222172	0,1632388	2,59	0,001
ProcGestContinTI	0,5595819	0,1762026	3,18	0,000

Fonte: Dados gerados pela autora por meio da ferramenta STATA/SE 14.2

Nesta situação, a função *logit* expressa a seguinte probabilidade:

$$P(X) = \frac{1}{1 + e^{-(\alpha + \beta_1 * PlanContinTI + \beta_2 * ProcGestContinTI)}}$$

Como ambas as variáveis apresentaram coeficientes dentro da previsão de confiabilidade esperada, as estimativas obtidas são: α = -3,803941, β_1= 0,4222172 e β_2= 0,5595819 (TABELA 2). Assim, para cada órgão que adote parcialmente a prática de executar um plano de contingência de serviço de TI (4), e que possua um plano iniciado para adotar o processo de gestão de continuidade de serviço de TI (3), temos a seguinte probabilidade do órgão possuir o processo de continuidade de negócio instituído corporativamente:

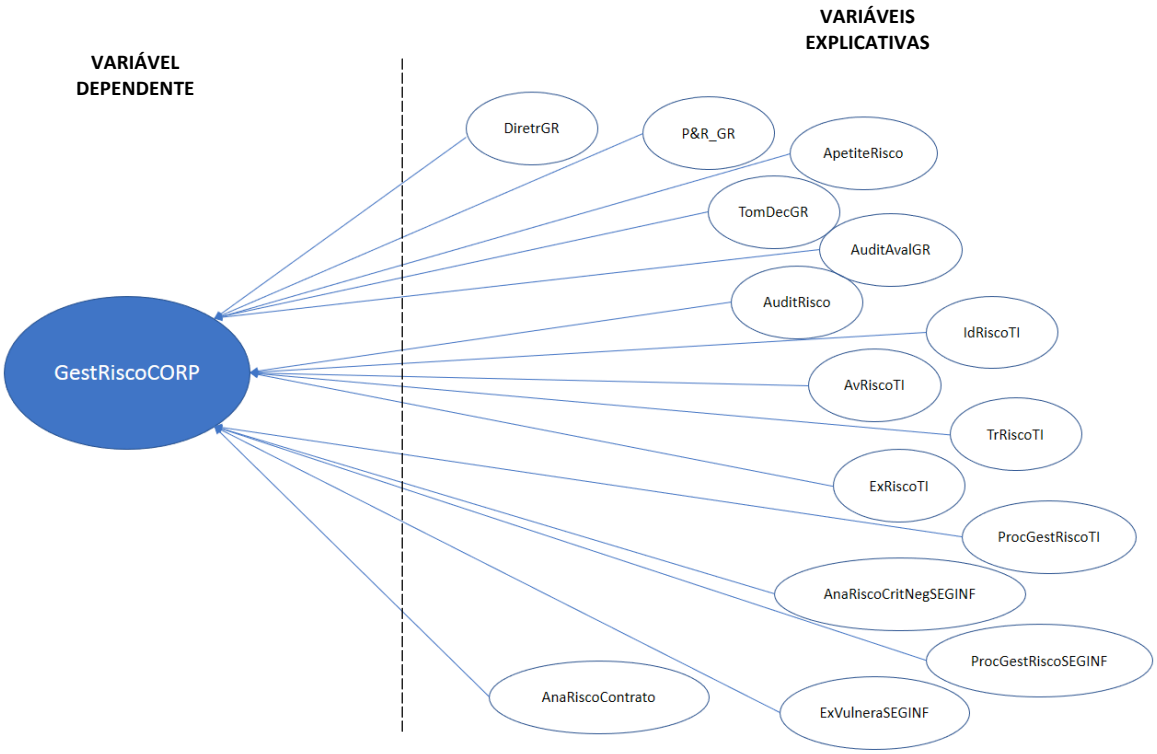
$$P(X) = \frac{1}{1 + e^{-(-3{,}803941 + 0{,}4222172 * 4 + 0{,}5595819 * 3)}}$$

$$P(X) = \frac{1}{1 + 1{,}54701381}$$

$$P(X) = \mathbf{39{,}26\%}$$

Para a segunda regressão linear múltipla foi selecionada como variável dependente para o grupo "Risco", Gestão de Risco Corporativo (GestRiscoCORP) também pertencente à área corporativa. E como segunda hipótese, tem-se (Figura 5):

Figura 5 - Hipótese 2- as respostas para a existência de um processo de gestão de risco corporativo NÃO influenciam a existência de outras práticas relativas a risco em outros setores do órgão público.



Fonte: elaborada pelas autoras (2017).

Similarmente à técnica utilizada para as variáveis referentes a "Continuidade", utilizou-se a mesma disposição das variáveis e lógica para o teste da hipótese 2. A disposição dos dados da variável "GestRiscoCORP" da base de dados de 2014 foi transformada para binária, representando a variável regressando (y na equação), sendo: "0" - não adota a prática, agrupando as respostas "não se aplica", "não adota", e "iniciou plano"; e, "1" - adota a prática, agrupando as repostas "adota parcialmente" e "adota integralmente" (parcialmente ou integralmente, pois ambas as respostas dependem da realidade do órgão e a customização do processo fica sob o critério do órgão público). As variáveis explicativas (independentes) foram mantidas com os 5 níveis de resposta a fim de apresentar as probabilidades do órgão público adotar a prática "GestRiscoCORP", ou seja, a variável dependente *dicotômica* (y) igual a 1; com base nas respostas para as variáveis explicativas "PlanContinTI" e "ProcGestContinTI".

Tabela 3 - Dados da regressão linear múltipla da variável dependente Gestão de Risco Corporativo com previsão de confiabilidade (P) até 5%. Modelo Logit

Variáveis	Coeficiente	Erro Padrão	Z	P>|Z|	[95% Conf.	Interval]
DiretrGR	.1469802	.3087041	0.48	0.634	-.4580687	.752029
P&R_GR	.2536714	.3165953	0.80	0.423	-.3668439	.8741867
ApetiteRisco	-.026241	.2895083	-0.09	0.928	-.5936668	.5411848
TomDecGR	.4072659	.2532793	1.61	0.108	-.0891524	.9036843
AuditAvalGR	-.217332	.2185209	-0.99	0.320	-.6456251	.2109612
AuditRisco	.733167	.1778941	4.12	0.000	.384501	1.081.833

IdRiscoTI	.2767925	.4186898	0.66	0.509	-.5438244	1.097.409
AvRiscoTI	-.2545183	.45143	-0.56	0.573	-1.139.305	.6302682
TrRiscoTI	.150257	.2928856	0.51	0.608	-.4237883	.7243022
ExRiscoTI	.2902896	.3043849	0.95	0.340	-.3062939	.8868731
ProcGestRiscoTI	-.1124026	.2552067	-0.44	0.660	-.6125986	.3877934
AnaRiscoCritNegSEGINF	-.4602053	.2996783	-1.54	0.125	-1.047.564	.1271534
ProcGestRiscoSEGINF	.7106937	.2769764	2.57	0.010	.16783	1.253.557
ExVulneraSEGINF	.2240513	.1976516	1.13	0.257	-.1633386	.6114412
AnaRiscoContrato	.0870103	.1734558	0.50	0.616	-.2529569	.4269775
Constante	-8,078412	.9988295	-8.09	0.000	-1003608	-6120742

Fonte: Dados gerados pela autora por meio da ferramenta STATA/SE 14.2.

Para a prática de governança de Gestão de Risco, foram obtidas somente 2 variáveis de 15 dentro do parâmetro de confiabilidade de 5%, AuditRisco e ProcGestRiscoSEGINF. Resultando na função *logit* com a seguinte probabilidade:

$$P(X) = \frac{1}{1 + e^{-(\alpha + \beta_1 * AuditRisco + \beta_2 * ProcGestRiscoSEGINF)}}$$

As estimativas obtidas são: α = -8,078412, β_1= 0,733167 e β_2= 0,7106937. Assim, para cada órgão que tenha um plano iniciado com a Auditoria Interna avaliando os riscos críticos ao negócio (3), e que adote parcialmente o processo de gestão de risco da segurança da informação (4), temos a seguinte probabilidade de o órgão possuir o processo de gestão de riscos instituído corporativamente:

$$P(X) = \frac{1}{1 + e^{-(-8{,}078412 + 0{,}733167 * 3 + 0{,}7106937 * 4)}}$$

$$P(X) = \frac{1}{1 + 20{,}82462540}$$

$$P(X) = \mathbf{4{,}58\%}$$

Ou seja, tem-se coeficientes positivos para as práticas citadas de forma que, ao se fazer uso da função *logit*, esta poderá fornecer a probabilidade pela qual a prática gestão de riscos corporativa poderá ser adotada num órgão da APFB. Neste exemplo, a probabilidade é de 4,58% caso o órgão possua um plano iniciado para a adoção de auditorias com avaliação focado em avaliação de riscos e um processo parcialmente adotado de Gestão de Riscos de Segurança da Informação.

5 CONCLUSÃO

Este artigo teve como objetivo analisar as boas práticas de governança de TI adotada pelos órgãos no âmbito da Administração Pública Federal Brasileira por meio de aplicação de análises descritivas, horizontal e vertical; e regressão linear múltipla no banco de dados das variáveis de Risco e Continuidade do Negócio.

Na análise foram utilizados dados de três bases de dados secundárias referentes aos anos de 2010, 2012 e 2014 do TCU, depois selecionadas 17 variáveis relacionadas a Risco e Continuidade. Para que fosse possível a comparação entre os anos, os dados das variáveis foram transformados no mesmo formato de resposta, binário. E aplicado a estatística descritiva fazendo uso de média e frequência.

Com a estatística descritiva foi possível identificar para as práticas de continuidade de negócio que, o Processo de Gestão de Continuidade Corporativo (ProcGestContin) em 2014 apresentou um contingente de adoção em 26,6% de 372 órgãos da APFB; o Processo de Gestão de Continuidade de Serviços de TI (ProcGestContinTI) tinha uma baixa adesão (7%) em 2010, 21 órgãos públicos da APFB, equivalente a aproximadamente 7% dos respondentes, afirmaram a existência deste processo na TI em 2010. Em 2012, esta prática teve um

crescimento de 300% na quantidade de respondentes, representando 17% do total de órgãos públicos que afirmaram adotar esta prática. Em 2014, há um decréscimo de adoção a referida prática; Quanto à existência do Plano de Continuidade de serviços de TI em órgãos públicos, registra-se que, em 2010 e 2012, há adoção do processo de gestão de continuidade de serviços na TI, mas somente alguns órgãos elaboraram um plano. Então, Comparando a adoção da prática de Gestão de Continuidade do negócio de forma corporativa (ProcGestContin) com a adoção deste mesmo processo na área de TI, foi realizada uma análise vertical considerando as duas variáveis mencionadas nos itens anteriores somente para o ano de 2014. Conforme os dados apresentados nas respostas, de 372 órgãos públicos da APFB que fizeram parte deste questionário, 99 possuem o processo de gestão de continuidade de negócio corporativo, 38 possuem o processo de gestão de continuidade de serviço de TI e 110 afirmaram executar o processo de gestão continuidade conforme um plano pré-definido. E assim, para a variável/prática "Continuidade", infere-se que, apesar da baixa adesão em se institucionalizar um processo de continuidade corporativo ou de TI, existe um plano a seguir em casos de resposta aos riscos pelos quais a instituição está exposta.

Para as práticas de governança relacionadas a Risco, tem-se: o processo de gestão de riscos de segurança da informação que em 2010, do total de 301 órgãos respondentes, 49 órgãos apreendem que realizam a análise dos riscos sobre as informações críticas para o negócio, considerando-se que não basta armazenar e prover soluções automatizadas, a TI também precisa assegurar a integridade das informações e a disponibilidade destas para a tomada de decisão e outras necessidades em tempo hábil com a devida confiabilidade. Ocorre que em 2012, de 349 respondentes, 33 órgãos validaram esta afirmação. Já em 2014, 25,27% dos órgãos apresentaram a adoção desta prática, superando mais do dobro dos anos anteriores, reconhecendo a necessidade de se analisar a exposição das informações ao risco. Quanto à existência de um plano de auditoria interna para avaliar os riscos considerados críticos para o negócio e a eficácia dos respectivos controles, entende-se que, se a instituição deve ou é recomendada a possuir processos definidos e executados voltados à gestão de risco, faz-se necessário auditar a eficácia destes controles dentro do órgão. Quase 15% dos respondentes elaboravam um plano de auditoria interna baseada em riscos em 2012, e em 2014, este número duplicou. Ou seja, cada vez mais a equipe da auditoria interna considera os riscos em seus trabalhos.

Vale ressaltar que na análise de regressão múltipla esta é uma das duas variáveis que apresentou significância influenciando na adoção do Processo de Gestão de Risco Corporativo. A outra refere-se ao Processo de Gestão de Risco de Segurança da Informação que também influencia na adoção da Gestão de Risco Corporativo. A adoção da Análise de Risco Crítico de Negócio (AnaRiscCritNegSEGINF) também apresentou evolução quantitativa, de forma que pode-se inferir que é uma prática que está dentre as prioridades dos órgãos da APFB. E quanto ao contingente de adoção das práticas de risco, a Análise dos Riscos dos Contratos tem apresentado mais de 60% de adesão por parte dos órgãos, o que se coaduna com a atual realidade vivenciada do poder público brasileiro quanto aos escândalos envolvendo empresas contratadas. E a segunda variável com maior adoção é a prática de executar o processo de gestão de vulnerabilidades técnicas de TI.

Em geral, conforme posição de 2014 tem-se que 82 órgãos possuem o processo de Gestão de Risco Corporativo instituído. Vale ressaltar que, independente da adoção da prática corporativa, a área de Segurança da Informação considera e executa meios para evitar as vulnerabilidades que atingem a informação crítica de negócio e, na esfera de TI, apresenta-se uma preocupação que perpassa a maioria dos órgãos no tocante à análise dos riscos inerentes à contratação. Ratifica-se a adoção de práticas de gestão de risco de TI independente das iniciativas corporativas, quando da identificação e avaliação dos riscos de TI apresentam maior número de órgãos que afirmam adotar tais práticas, mesmo estes que não possuam um

processo de gestão de risco próprio de TI, há atividades em realização de forma isolada. Quanto às diretrizes da gestão de riscos, considerando-se a quantidade de órgãos que adotaram o processo de gestão de risco corporativo, a TI buscou as diretrizes que norteiam a sua gestão de risco, provavelmente, alinhada aos preceitos do processo corporativo.

Portanto conclui-se que, há necessidade dos órgãos da APFB investirem em práticas de Gestão de Risco e Gestão de Continuidade do Negócio como forma de garantir boas respostas às incertezas e por consequência, valorizar o órgão para melhor empregar os investimentos e gerar bons resultados para a sociedade.

REFERÊNCIAS

ABBOTT, K. W.; SNIDAL, D. Hard and soft law in international governance. **International Organization**, v. 54, n. 3, p. 421–456, 2000.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 15999-1**. Gestão de Continuidade do Negócio - Parte 1: código de prática. International Organization for Standardization - ISO. Rio de Janeiro, 2008.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 73.** Risk Management - Vocabulary. International Organization for Standardization - ISO. Rio de Janeiro, 2009a.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 31000.** Risk Management - Principles and Guidelines. *International Organization for Standardization* - ISO. Rio de Janeiro, 2009b.

AURÉLIO. **Dicionário do Aurélio Online - Dicionário Português**. 2017. Disponível em: <https://dicionariodoaurelio.com/>. Acesso em: 20 abr. 2017.

BRYMAN, Alan; BELL, Emma. **Business research methods.** 3. ed. New York: Oxford University Press, 2011.

BUSHMAN, Robert M.; SMITH, Abbie J. Financial accounting information and corporate governance. **Journal of accounting and Economics**, v. 32, n. 1, p. 237-333, 2001.

CEPIK, M. A. C.; CANABARRO, D. R.; POSSAMAI, J. **Do Novo Gerencialismo Público à Governança da Era Digital - Governança de TI:** Transformando a Administração Pública no Brasil. PORTO ALEGRE: WS, v. 20, 2010. Disponivel em: <http://hdl.handle.net/10183/78940>. Acesso em: 27 ago. 2016.

COSTA, S. C. O compliance como um novo modelo de negócio nas sociedades empresárias. **CIENTÍFICA DR: Revista Científica da Faculdade Darcy Ribeiro,** n. 3, p. 51-60, jul./dez. 2012 – ISSN 2236-8949.

DE HAES, Steven; VAN GREMBERGEN, Wim. IT Governance Structures, Processes and Relational Mechanisms: achieving IT/Business alignment in a Major Belgian Finantial Group. In: Hawaii International Conference on System Sciences, 39th, 2006, Hawaii. **Proceedings**. IEEE.Computer Society Digital Library, 2006.

DOURADO, Luzia. **COBIT 5:** Framework de Governança e Gestão Corporativa de TI. Jan. 2015. Disponível em: <http://www.neutronica.com.br/wp-content/uploads/COBIT-5-Framework-de-Governanca-e-Gestao-Corporativa-de-TI-v1.2.pdf>. Acesso em: 10 jan. 2017.

FONSECA, Camila Veneo Campos; SILVEIRA, Rodrigo Lanna Franco da. Corporate governance and cost of debt: evidences among brazilian listed companies. **Read. Revista Eletrônica de Administração,** Porto Alegre, v. 22, n. 1, p. 106-133, 2016.

GHEORGHE, Mirela. Risk Management in IT Governance Framework. Fonte: **Economia: Seria Management**, v. 14, n. 2, p. 545, 2011.

GUJARATI, Damodar N. **Econometria básica**. 3. ed. São Paulo: Makron Books, 2000. 846p.

HENRY, A. **Understanding Strategic Management**. New York: Oxford University Press, 2008.

HOLDEN, Stephen H. The Evolution of Federal Information Technology Management Literature: Does IT Finally Matter?. **Modern Public Information Technology Systems:** Issues and Challenges. IGI Publishing, 2007.
ISACA - Information Systems Audit and Control Association. **COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.** USA, 2012.
JONES, V.; PIERCE, C. **Corporate Governance in the United Kingdom**. Orpington: Global Governance Services, 2013.
JORDAN, C. Cadbury twenty years on. **Villanova Law Review**, v. 58, n. 1, p. 1–24, 2013.
LA PORTA, R. et al. Investor protection and corporate valuation. **Journal of Finance,** Oxford, v. 57, n. 3, 2002.
MADHANI, P. M. Corporate Governance from compliance to competitive advantage. **The Accounting World**, v. 7, n. 8, p. 26-31, 2008.
MADHANI, P. M. Corporate Governance and Disclosure: Public Sector vs Private Sector. **SCMS Journal of Indian Management**, v. 11, n. 1, p. 5-20, mar. 2014.
MASSON, E.; JUNIOR, E. C. M.; PEREIRA, J. N.; NETO, J. S. A governança de TI autônoma na Administração Pública Federal. In: SIMPÓSIO DE EXCELÊNCIA E GESTÃO E TECNOLOGIA, XI, Resende. **Anais…** Resende/RJ: SEGeT, 2014.
MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa.** São Paulo: Melhoramentos, 2017.
MORETTI, S. L. DO A.; CAMPANARIO, M. DE A. **A Produção Intelectual Brasileira em Responsabilidade Social Empresarial Empresarial–RSE sob a Ótica da Bibliometria**. 2009.
NEUMAN, L. W. **Social research methods:** qualitative and quantitative approaches. 3. ed. Boston: Allyn & Bacon, 1997.
PASCOAL, M. N.O.; OLIVEIRA, O. V. Adoção de Melhores Práticas de Governança Corporativa na Administração Pública Federal Brasileira. In: ENCONTRO DA ANPAD, XLI, EnAPAD, 2017, São Paulo, **Anais…** São Paulo/SP: ANPAD, 2017.
PATEL, Nandish V. An emerging strategy for E-business IT Governance. In: VAN GREMBERGEN, Win (ed.). **Strategies for Information Technology Governance**. Hershey, PA, USA: Idea Group Publishing, 2004.
PRADO JÚNIOR, H. R. **Gestão de Risco.** 2013. Disponível em: < https://qualidadeonline.wordpress.com/2013/01/21/a-gestao-da-continuidade-dos-negocios-gcn-parte-1/%3E.>. Acesso em: 30 maio 2017.
ROSSONI, Luciano; MACHADO-DA-SILVA, Clóvis L. Organizational Institutionalism and Corporate Governance (Institucionalismo Organizacional e Práticas de Governança Corporativa - Portuguese). **Revista de Administração Contemporânea**, v. 14, p. 173-198, 2010.
SANTOS, H. F.; SILVA, R. A. **Gestão de Projetos:** plano de reposta ao risco. 2014.
SIDOU, J.M. Othon. **Dicionário Jurídico:** Academia Brasileira de Letras Jurídicas. 11. ed. Rio de Janeiro: Forense, 2016.
SILVEIRA, Nádia Sulene Moreira; GOULARTE, Jeferson Luís Lopes. Práticas de Governança no Setor Público Municipal: uma análise a partir do estudo 13 do PSC/IFAC. **RAGC,** v. 4, n. 9, 2016.
SOUZA, Jackson Gomes Soares et al. Gestão de riscos de segurança da informação e governança de TI no setor público. In: ENGEMA, 2016, **Anais…** São Paulo: USP, 2016.
TAROUCO, H. H.; GRAEML, A. R. Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. **RAUSP,** v. 46, n. 1, p.7-18, 2011.
TCU - Tribunal de Contas da União. **Referencial Básico de Governança do TCU** – 2014. 2014.