Interdisciplinary LINKSCIENCEPLACE Scientific Journal
ISSN: 2358-8411
DOI: 10.17115
Interdisciplinary Scientific Journal. ISSN: 2358-8411
Nº 3, volume 7, article nº 03, July/September 2020
D.O.I: http://dx.doi.org/10.17115/2358-8411/v7n3a3
Accepted: 01/02/2020 Published:22/09/2020

GRC COMO MECANISMO PARA IMPLANTAÇÃO E MANUTENÇÃO DE UM MODELO DE GOVERNANÇA DE TI

Arioston Cerqueira Rodrigues
Universidade Católica de Brasília
Mestre em Gestão do Conhecimento e Governança de TI para a transformação digital

João Souza Neto
Universidade Católica de Brasília
Doutor em Engenharia Elétrica pela UNB

Tomás Roberto Cotta Orlandi
Universidade Católica de Brasília
Doutor em Ciência da Informação

RESUMO
A Governança de TI – GTI nas instituições torna-se a cada dia um instrumento importante para a sobrevivência das organizações. A GTI utiliza métodos para extrair dos recursos de TI entregas que deem valor ao negócio, bem como, provoca o alinhamento dos objetivos de negócio aos objetivos de TI. Esta pesquisa apresenta a relação entre Governança de TI, Gestão de Risco e *Compliance* - GRC, por meio de uma análise conjunta, utilizando os conceitos e modelos atrelados à disciplina GRC. A primeira contribuição desta pesquisa é a apresentação de como um ciclo de GRC pode favorecer na melhoria dos direcionadores de um modelo de governança de TI de uma instituição. A segunda contribuição é a apresentação dos riscos relacionados às não conformidades encontradas no modelo de Governança de TI pesquisado. A terceira, e não menos importante contribuição, é a análise individual dos processos de um modelo de Governança de TI.

PALAVRAS-CHAVE: Governança de TI, Implementação, Riscos, *Compliance* e Modelo GRC.

ABSTRACT
IT Governance (ITG) is a fundamental practice for the survival of organizations. It uses methods to extract deliverables that value the business from IT resources,

aligning business objectives with IT objectives. This research presents the relationship between IT Governance, Risk Management and Compliance - GRC, through a joint analysis, using the concepts and models linked to the GRC discipline. The first contribution of this research is the presentation of how a GRC cycle can favor the improvement of the drivers of an IT governance model of an institution. The second contribution is the presentation of the risks related to the nonconformities found in the IT Governance model surveyed. The third and not least is the individual analysis of the processes of an IT Governance model.

KEYWORDS: IT Governance, Implementation, Risk, Compliance and GRC Framework.

INTRODUÇÃO

Uma Governança de Tecnologia da Informação (GTI) bem implementada e sustentável gera muitos benefícios para as organizações, por exemplo, maior competitividade, redução de custos operacionais, maior produtividade e garantia de que escassos recursos de Tecnologia da Informação (TI) estão sendo empregados no alcance dos objetivos mais importantes da organização (WEILL e ROSS, 2006 apud MIRANDA; LEONARDO,2014).

Apesar do conceito de Governança de TI e seus principais modelos já estarem bastante difundidos, a implantação e manutenção de práticas de Governança de TI ainda é um desafio. Ter as ações de TI alinhadas às estratégias institucionais é o pressuposto básico, mas não é uma ação fácil de ser alcançada, pois a eficiência e eficácia da implantação da Governança de TI perpassa outras disciplinas, tais como, risco e *compliance*. Segundo Racz, Weippl e Seufert (2010), tais temas, quando aplicados em silos, não trazem os mesmos resultados quando geridos conjuntamente.

A ineficiência na implantação e na manutenção da Governança de TI, bem como a ausência de um modelo, podem expor as instituições ao risco de dispêndio de recursos físicos, humanos e financeiros sem agregação de valor ao negócio, uma vez que as ações de TI não contribuirão para o alcance das metas estratégicas.

A implantação e a manutenção de um ambiente de Governança requisitam uma perfeita análise dos riscos corporativos, riscos de TI, bem como o cumprimento de aspectos legais inerentes ao negócio ou às normas institucionais. Aplicar um

modelo de Governança sob a ótica de integrar Governança, Risco e *Compliance* é uma tarefa árdua, mas se apresenta como um caminho para a efetividade da manutenção de um modelo de Governança de TI. Segundo Vicente, Racz e Silva (2009), o objetivo final do domínio GRC é identificar, integrar e otimizar processos e atividades que são comuns.

Implantar e manter uma Governança de TI requer uma interface com outros domínios, tais como gestão de risco e *compliance*, intensificando a complexidade do processo de implantação e manutenção de um modelo de GTI.

Segundo Vunk, Mayer e Matulevicius (2017), implementar e manter a Governança de TI nas organizações não têm obtido o desempenho esperado, pois não conseguem atingir as expectativas de seus patrocinadores. Os maus resultados advêm de vários fatores, entre eles, a dificuldade em demonstrar os riscos das não conformidades inerentes ao modelo de Governança de TI adotado pela Instituição, a complexidade de gerir Governança de TI, Risco e *Compliance* de forma separada e do próprio desalinhamento entre os objetivos de Negócio e de TI.

Para Smet e Mayer (2016), é claramente reconhecido que tecnologia da informação não é mais apenas uma questão técnica. Assim, a complexidade e a sua importância nas empresas envolvem uma camada de governança necessária. Tal camada de governança engloba a gestão de risco e conformidade como mecanismos de direcionamento. Para os autores, GRC é um acrônimo guarda-chuva, que abrange as três disciplinas de governança, gestão de riscos e *compliance*. Neste contexto, o principal desafio de GRC é ter uma abordagem tão integrada quanto possível para os três domínios.

Para Racz, Weipll e Seufert (2010), Governança, Risco e Conformidade (GRC) é um tópico emergente e embora haja muita pesquisa sobre as três disciplinas, como tópicos separados, há poucas discussões sobre as possíveis sinergias entre os temas. Os autores defendem, ainda, o quanto GRC pode apoiar a Governança de TI, sobretudo sob uma ótica de uma visão holística dos processos atrelados ao modelo de Governança adotado pela Instituição, sob a luz do reconhecimento dos riscos inerentes às não conformidades do modelo.

Vicente, Racz e Silva (2009) afirmam que a GRC tradicional, em silos, reforça a diminuição da transparência e, portanto, a agilidade da Governança, impactando diretamente na tomada de decisão da instituição. Os autores defendem um modelo

de GRC que pode ser traduzida por meio de um sistema de informação, onde uma arquitetura de referência pode ajudar na integração destes processos.

Essa pesquisa investigou como GRC pode contribuir na manutenção de um modelo de Governança de TI, aplicando um estudo de caso em uma instituição de âmbito Nacional, a qual possui um modelo de Governança de TI instituído desde 2012. No estudo, por meio de um autodiagnostico, foram coletadas as não conformidades inerentes ao modelo. Em seguida, um grupo focal fez a avaliação dos riscos inerentes às não conformidades da Resolução, sendo assim, foi possível gerar as principais exposições refletidas pelas falhas de *Compliance* do Modelo de GTI.

REFERENCIAL TEÓRICO

GOVERNANÇA DE TI

A Governança de Tecnologia da Informação (GTI) é cada vez mais importante na entrega de valor aos negócios das empresas. A premissa básica de qualquer modelo de governança a ser adotado é propiciar um alinhamento entre as ações desenvolvidas pela área de TI e a estratégia da empresa.

A generalização do uso da tecnologia causou dependência crítica das empresas com relação aos serviços de TI, sendo que, nos dias de hoje, os requisitos das áreas de negócio envolvem uma complexa mistura de preocupações políticas, organizacionais, técnicas e culturais (Sethibe et al., 2007). Isto exige um foco em governança de TI eficaz, que seja capaz de alinhar as demandas de TI à missão, à estratégia e à cultura da empresa. Na pesquisa de Weill e Ross (2004), os autores apresentaram uma estatística enfatizando que o retorno sobre o investimento em TI é incrementado em torno de vinte por cento quando há uma efetiva governança de TI.

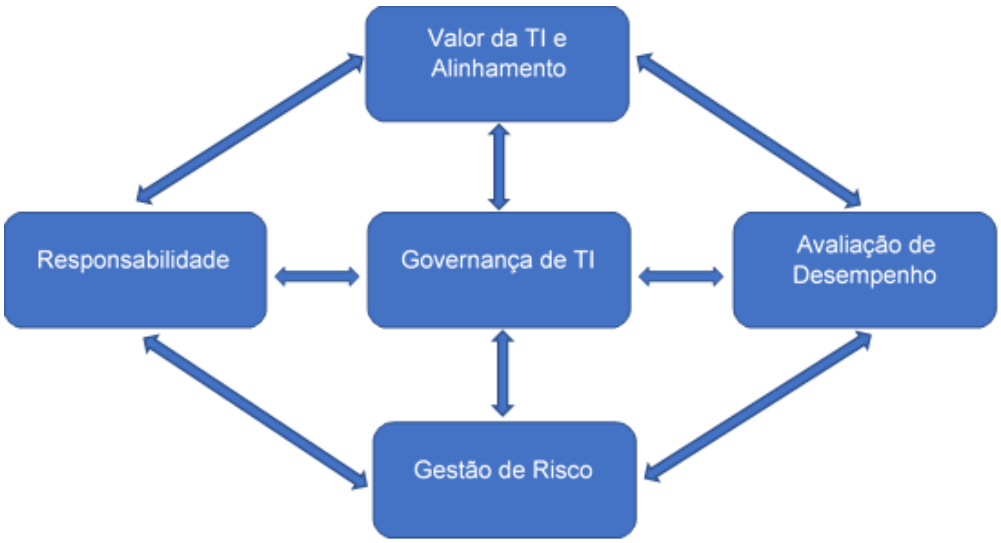
Segundo Weill e Ross (2004), a medida do desempenho é definida como a eficácia da governança de TI em entregar quatro resultados, ponderados por sua importância para a organização: o uso rentável de TI, o uso eficaz de TI para a utilização de ativos, o uso eficaz de TI para o crescimento e o uso efetivo de TI para a flexibilidade dos negócios.

A governança de TI é a estrutura de relacionamentos, processos e mecanismos usados para desenvolver, direcionar e controlar os recursos e a estratégia de TI para alcançar as metas e objetivos de uma empresa. É um conjunto de processos, que visa agregar valor a uma organização enquanto equilibra os aspectos de risco e retorno associados aos investimentos de TI.

A governança de TI é, em última instância, responsabilidade do conselho de administração e da diretoria executiva. Em um sentido mais amplo, a governança de TI engloba o desenvolvimento do plano estratégico de TI, avaliando a sua natureza, o impacto organizacional das novas tecnologias, o desenvolvimento da base de competências de TI, o alinhamento da direção e os recursos de TI, salvaguardando os interesses das partes interessadas internas e externas da TI, bem como tendo em conta a qualidade destas relações (Sethibe, T; Campbell, J; McDonald, Craig:2007).

A estrutura da função de TI e a posição da autoridade de decisão em uma organização, para muitos, determina a eficácia da governança de TI (Weill e Ross 2004). Segundo Symons (2005), existem quatro objetivos que impulsionam a governança de TI: valor e alinhamento de TI, responsabilidade, medição de desempenho e gestão de riscos. Cada um desses objetivos deve ser abordado como parte do processo de governança de TI. A Figura 1 ilustra esses objetivos.

Figura 1 - Objetivos segundo Symon



Fonte: Forrester Research, Inc.

Fundamentando a linha da importância para a Gestão de riscos, Symons (2005), reforça que os riscos associados à TI são frequentemente os mesmos que os de negócio. Portanto, gerenciar o risco de TI é primordial. Os riscos de TI incluem riscos de segurança decorrentes de hackers e ataques de negação de serviço, riscos de privacidade decorrentes de roubos de identidade, recuperação de desastres, resiliência de sistemas a interrupções e os riscos associados às falhas do projeto.

Quando as métricas sobre a gestão de risco indicam que existem grandes problemas, uma estratégia pode ser melhorar ou adequar o plano de recuperação de desastres (DRP – *Disaster Recovery Plan*) por meio da implementação das boas práticas do COBIT e do ITIL (Grembergen & Haes, 2005).

Weill e Ross (2004) afirmam que a Governança de TI reflete os princípios mais amplos de governança corporativa, focando no alcance de metas de desempenho corporativo. Os resultados, muitas vezes, são difíceis de medir.

É importante observar que Governança de TI não deve ser considerada isoladamente, porque está ligada a outras áreas-chave da empresa como, por exemplo: financeira, humana, propriedade intelectual, físico, relacionamentos, entre outros. Neste raciocínio, a Governança de TI pode compartilhar mecanismos como comitês executivos e processos de orçamento com outros processos de governança corporativa e, desse modo, apoiar a tomada de decisão empresarial. Portanto, é fundamental que a governança de TI eficaz seja visível em métricas de desempenho de negócios.

Segundo Kutsikos & Bekiaris (2007), a Governança de TI vivenciou um ponto de “viralização” com o advento do COBIT e *frameworks* relacionados que ajudaram a tornar as operações de TI mais compreensíveis e gerenciáveis por executivos de empresas.

GESTÃO DE RISCO

A definição de riscos é apontada em diversas literaturas, algumas delas até contraditórias. A maior parte das literaturas atrela risco a uma incerteza ou perda. Conforme definição de Vaughan (1997, p. 8), o risco é “uma condição na qual existe uma possibilidade de um desvio adverso de uma expectativa de resultado associado à esperança”. Muitas definições de risco estão atreladas ao ambiente financeiro, Hoji

(2001, p. 223), nesta mesma linha, manifesta que “geralmente, o risco está associado a algum fator negativo que possa impedir ou dificultar a realização do que foi planejado”.

Pode-se inferir que as definições de risco tendem a enfocar as chances de resultados sob uma ótica apenas da ocorrência de eventos prejudiciais aos resultados ou patrimônio da empresa. Entretanto, um resultado inesperado pode ter impactos tanto negativos quanto positivos. Goulart (2003, p. 74), reforça essa ideia dizendo que “o risco existe quando há probabilidade de experimentar retornos diferentes do que se espera.

A gestão do risco na definição de Brito, O. S. (2000, p. 24), “é o processo por meio do qual as diversas exposições ao risco são identificadas, mensuradas e controladas”. Brito reforça ainda que a “divulgação dos riscos” é também função a ser desempenhada no processo de gestão. Williams e Heinz apud Vaughan (1997, p. 91), corroboram esse raciocínio ao entenderem a gestão de riscos como “a minimização dos efeitos adversos do risco a um custo mínimo por meio da identificação, mensuração e controle”. Vaughan (1997) manifesta que, normalmente, os negócios possuem vários objetivos; assim, seria inadequado dizer que a gestão de riscos possui um único objetivo. Dentre os seus múltiplos objetivos, a maioria dos autores entende como dois objetivos principais: a mitigação dos efeitos dos riscos e a minimização dos custos. Aplicando-se essas definições para o ambiente das empresas não-financeiras, entende-se que a gestão de riscos não consiste em atividade voltada à eliminação dos riscos, mas, sim, à sua identificação, mensuração e controle. E, que dessa gestão, pode depender a continuidade dos negócios.

Conforme estudo realizado pela OECD (2014), após a crise financeira e uma série de falhas ou deficiências de gerenciamento de risco, as empresas suíças aumentaram o seu teste de detenção. Embora os problemas financeiros tenham sido o foco de atenção, as consequências dos riscos de reputação também estão se tornando cada vez mais claras para as empresas. Os esforços mais fortes para fortalecer o gerenciamento de risco podem ser observados em empresas que foram identificadas com diferentes problemas.

Segundo OECD (2014), fora do setor financeiro, essa atenção aumentada, no entanto, nem sempre se reflete em uma abordagem mais formal para a organização da gestão de riscos. O risco geralmente continua a ser a responsabilidade das

funções empresariais, com funções centralizadas de gerenciamento de risco desempenhando mais um papel de coordenação e apoio, bem como, produzindo relatórios que nem sempre chegam ao conselho de administração.

O COSO ERM aponta a avaliação de riscos como sendo a forma que uma organização tem de considerar até que ponto eventos em potencial podem impactar a realização dos objetivos. A administração avalia os eventos com base em duas perspectivas: probabilidade e impacto. Geralmente, se utiliza uma combinação de métodos qualitativos e quantitativos.

Segundo o COSO, os impactos positivos e negativos dos eventos em potencial devem ser analisados isoladamente ou por categoria em toda a organização. Os riscos são avaliados com base em suas características inerentes e residuais.

A ISO/IEC 31010 aponta que todas as atividades de uma organização envolvem riscos que devem ser gerenciados. O processo de gestão de riscos auxilia a tomada de decisão, levando em consideração as incertezas e a possibilidade de circunstâncias ou eventos futuros (intencionais ou não intencionais) e seus efeitos sobre os objetivos acordados.

Ainda referente a ISO/IEC 31010, define-se que o processo de avaliação de riscos é a parte da gestão de riscos que fornece um processo estruturado para identificar como os objetivos podem ser afetados, e analisa o risco em termos de consequências e suas probabilidades, antes de decidir se um tratamento adicional é requerido.

Smet e Mayer (2016), em sua pesquisa atrelam boas práticas de governança a algumas estratégias. Segundo os autores, na prática decisões sobre o tema segurança são esperadas para serem tratadas junto às decisões de investimento dos demais projetos de TI. Para Smet e Mayer a eficácia de um programa de gestão de risco de segurança da empresa está atrelado a forma em que se define os investimentos necessários. Segundo a pesquisa, os investimentos em segurança são tratados de forma similar aos investimentos gerais de TI, mas o contexto de risco de segurança é muito diferente, por esse motivo, esta parte do processo decisório na estrutura de governança de TI merece mais atenção e precisa ser repensada em uma organização que requer uma boa oferta dos serviços de TI, uma vez que estão atrelados ao negócio da empresa. Conforme os autores, a gestão

sobre estes riscos é uma forma natural de mitigação de alguns riscos inerentes as ações de TI em uma organização.

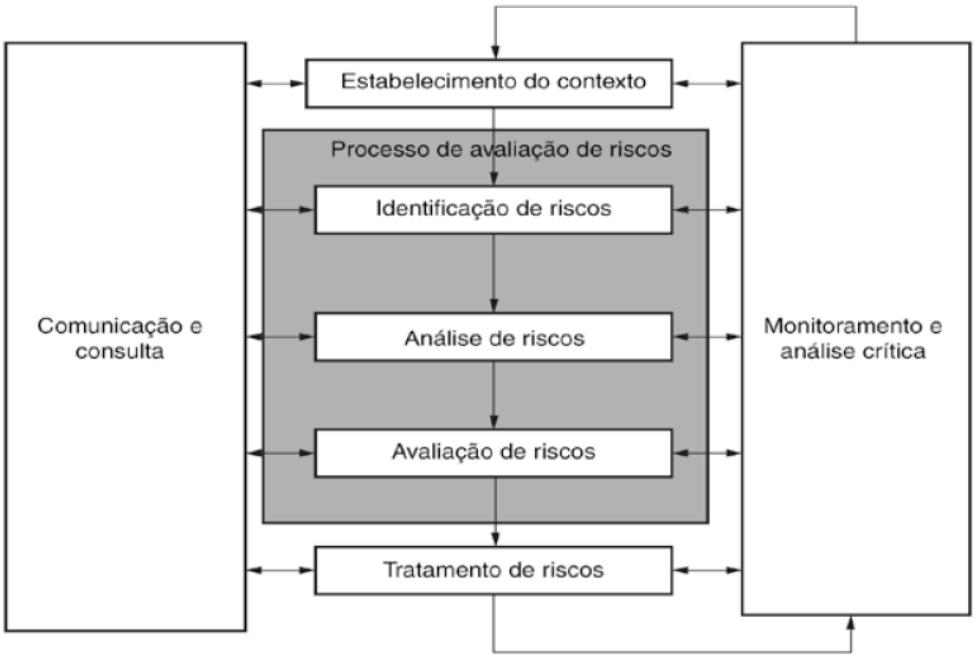
Segundo a ABNT NBR/ISSO 31000:2009, O sucesso da Gestão de Riscos irá depender da eficácia da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la através de toda a organização, em todos os níveis. A estrutura auxilia a gerenciar riscos eficazmente através da aplicação do processo de gestão de riscos em diferentes níveis e dentro de contextos específicos da organização. A estrutura assegura que a informação sobre riscos proveniente desse processo seja adequadamente reportada e utilizada como base para a tomada de decisões e a responsabilização em todos os níveis organizacionais aplicáveis.

A ISO/IEC 31010 apresenta ainda que o processo de avaliação de riscos fornece aos tomadores de decisão e às partes responsáveis um entendimento aprimorado dos riscos que poderiam afetar o alcance dos objetivos, bem como a adequação e eficácia dos controles em uso. Isto fornece uma base para decisões sobre a abordagem mais apropriada a ser utilizada para tratar os riscos. A saída do processo de avaliação de riscos é uma entrada para os processos de tomada de decisão da organização.

Ao se estabelecer o contexto, os objetivos do processo de avaliação de riscos, os critérios de risco e o programa para o processo de avaliação de riscos são determinados e acordados.

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos conforme figura 2. A maneira como este processo é realizado é dependente não somente do contexto do processo de gestão de riscos, mas também dos métodos e técnicas utilizados para conduzir o processo de avaliação de riscos.

Figura 2 - Processo avaliação de Riscos



Fonte: ISO/IEC 31010

COMPLIANCE

A ISO 19600:2014, *Compliance* é a consequência de uma organização cumprir as suas obrigações, e é feito de forma sustentável, incorporando-o na cultura da organização e no comportamento e atitude de pessoas que trabalham para ela. Apesar de manter a sua independência, é preferível que a gestão de *compliance* seja integrada aos processos de gestão financeira, de risco, da qualidade, ambiental, de saúde e segurança da organização e aos seus requisitos e procedimentos operacionais.

Um sistema de gestão de *Compliance* eficaz abrangendo toda a organização permite que uma organização demonstre seu comprometimento com o cumprimento das leis pertinentes, incluindo requisitos legislativos, códigos da indústria e normas organizacionais, bem como as normas de boa governança corporativa, boas práticas, ética e expectativas da comunidade.

A avaliação de riscos envolve a comparação do nível de risco de *compliance* encontrado durante o processo de análise com o nível de risco de *compliance* que a organização pode e está disposta a aceitar. Com base nesta comparação, as prioridades podem ser definidas como uma base para determinar a necessidade de implementação de controles e a extensão destes controles

Para a implantação de *Compliance*, segundo a ISO 19600, convém que a organização determine as questões externas e internas, como as relacionadas aos riscos de *compliance*, que são pertinentes para a sua finalidade e que afetam sua capacidade de atingir o(s) resultado(s) pretendido(s) de seu sistema de gestão de *compliance*. Ao fazer isto, convém que a organização considere uma ampla série de aspectos externos e internos, como os contextos regulamentares, sociais e culturais, a situação econômica, as políticas e os procedimentos.

Outro ponto que é evidenciado para o sucesso da implantação do *compliance* é o comprometimento da liderança. Segundo a ISO 19600, recomenda-se que o conselho de administração e a Alta Direção demonstrem liderança e comprometimento com relação ao sistema de gestão de *compliance.*

Para que todos da organização e a liderança possam ter um instrumento que demonstre as diretrizes quanto ao *compliance*, a ISO 19600 recomenda também a criação de um Política de *Compliance* que seja apropriada ao propósito da organização, fornecendo uma estrutura para definir os objetivos de *compliance.*

Segundo a ISO 19600, para um sistema de gestão de *compliance* ser eficaz, o conselho de administração e a Alta Direção precisam dar o exemplo, aderindo e apoiando ativamente o *compliance* e o sistema de gestão de *compliance*.

GRC

Racz, Weipll e Seufert (2008), definem GRC como uma abordagem holística integrada à governança, risco e conformidade em toda a organização, assegurando que uma organização atue de forma eticamente correta e de acordo com sua apetência pelo risco, políticas internas e regulamentos externos através do alinhamento da estratégia, processos, tecnologia e pessoas, melhorando assim a eficiência e a eficácia.

Vicente, Racz e Silva (2009), denominam GRC como uma forma de entendimento mais amplo das políticas internas, regras e riscos, dentro de uma visão holística da organização. Essa visão pode ser realizada pela integração de processos e atividades comuns em todas as funções do GRC, como avaliações de risco ou funções que funcionam melhor em conjunto, tal como atrelar riscos mais significativos ou compilar uma lista consensual dos critérios mais críticos de problemas de GRC. Para Vicente, Racz e Silva (2009), o objetivo final do domínio GRC é identificar, integrar e otimizar processos e atividades que são comuns.

Os 5 processos de *Compliance*: análise de requisitos, análise de desvios, gerenciamento de desvios, relatórios/documentação e análise de desvio promovem gatilhos para o Gerenciamento de Risco, dentro de uma análise de ambiente interno. Os sete processos inerentes ao COSO ERM:2004 mostram o tratamento dado na disciplina risco no que se refere à definição, identificação e avaliação de risco para que haja uma resposta ao risco e um controle das atividades relacionadas a cada evento controlado. Esses processos, por sua vez, também contribuem para a disciplina governança, para que a avaliação o direcionamento, o relato e o monitoramento sejam efetivos e possam retroalimentar o ciclo do modelo proposto.

Vunk, Mayer e Matulevicius (2017), reforçaram o estudo elaborado por Racz, Weipll e Seufert (2010), onde, por meio de revisão sistemática de literatura, apresentaram um modelo integrado de GRC. Os autores apresentam um modelo de processos dividido verticalmente em três domínios GRC, ainda separados em seus respectivos fluxos. Os fluxos principais vão de *Compliance* ao Risco e do Risco para a Governança de TI, resumindo o estudo demonstrando o modelo de Racz et al.(2010).

Tanto Racz, Weipll e Seufert (2008), quanto Vunk, Mayer e Matulevicius (2017) concluem que a ideia de um conceito integrado é amplamente suportada e que GRC é mais do que um termo geral para governança, risco e conformidade, mas sim uma forma de convergir ações em prol das três disciplinas.

METODOLOGIA DE PESQUISA

Esta seção descreve a metodologia adotada neste trabalho. Segundo Gil (2007), o método científico é um conjunto de procedimentos intelectuais e técnicas adotadas para se atingir o conhecimento. A pesquisa foi desenvolvida com natureza quantitativa e qualitativa, com fins exploratórios. Para a avaliação dos riscos foi utilizado o método grupo focal, na fase 3.

A metodologia empregada nesta pesquisa envolveu quatro fases: a revisão de literatura, um autodiagnostico sob a perspectiva da *compliance* do modelo pesquisado, uma avaliação sob a ótica de gestão de risco e, por último, foi aplicado o modelo GRC de RACZ, et al.

ESTUDO DE CASO

A pesquisa foi direcionada aos gestores de TI do Sistema Indústria, representando os 26 Estados e o Distrito Federal, além da CNI. Alguns Estados podem ser segmentados por instituição, ou seja, em alguns casos, a pesquisa foi respondida no mesmo Estado por mais de um gestor, representantes das entidades SESI, SENAI, FEDERAÇÃO DA INDÚSTRIA e/ou IEL. A pesquisa foi encaminhada pela Superintendência de Tecnologia da Informação da CNI, uma vez que os resultados serão aproveitados em um trabalho futuro. Na investigação, foi coletado o nível de implantação de cada um dos dez processos de Governança de TI que compõem a Resolução 563/2012, para uma análise de conformidade.

A ferramenta *SurveyMonkey* foi o instrumento utilizado para elaboração dos questionários e respectivas coletas. Os gestores de TI do Sistema Indústria deram suas contribuições, respondendo as questões que foram classificadas dentro de uma escala Likert.

A pesquisa coletou dos gestores de TI do Sistema Indústria informações quanto ao grau de implantação dos artefatos inerentes à resolução 563/2012, trazendo, como resultado, o índice de conformidade de cada processo por instituição investigada.

Organização estudada

O Sistema Indústria foi a organização estudada, sendo uma instituição criada para atender o segmento industrial no país. É formado por um conjunto de entidades, encabeçadas pela Confederação Nacional da Indústria (CNI).

A CNI é o órgão máximo do sistema sindical patronal da indústria e, desde a sua fundação, em 1938, defende os interesses da indústria nacional e atua na articulação com os poderes Executivo, Legislativo e Judiciário, além de diversas entidades e organismos no Brasil e no exterior.

As Federações de indústrias estão presentes nos 26 estados e no Distrito Federal e defendem e representam as indústrias locais perante os governos estaduais e municipais. Além disso, fazem a conexão das empresas de sua região ou localidade com a CNI, por meio do oferecimento de informações sobre o cenário de atuação das indústrias, indicação de demandas e expectativas e execução de iniciativas e projetos conjuntos.

Para a manutenção de todas as linhas de negócio das entidades do Sistema Indústria, é fundamental que a Tecnologia da Informação (TI) seja a principal aliada

para superar os desafios e, por consequência, manter as entidades competitivas, sobretudo com serviços que fortaleçam a indústria brasileira.

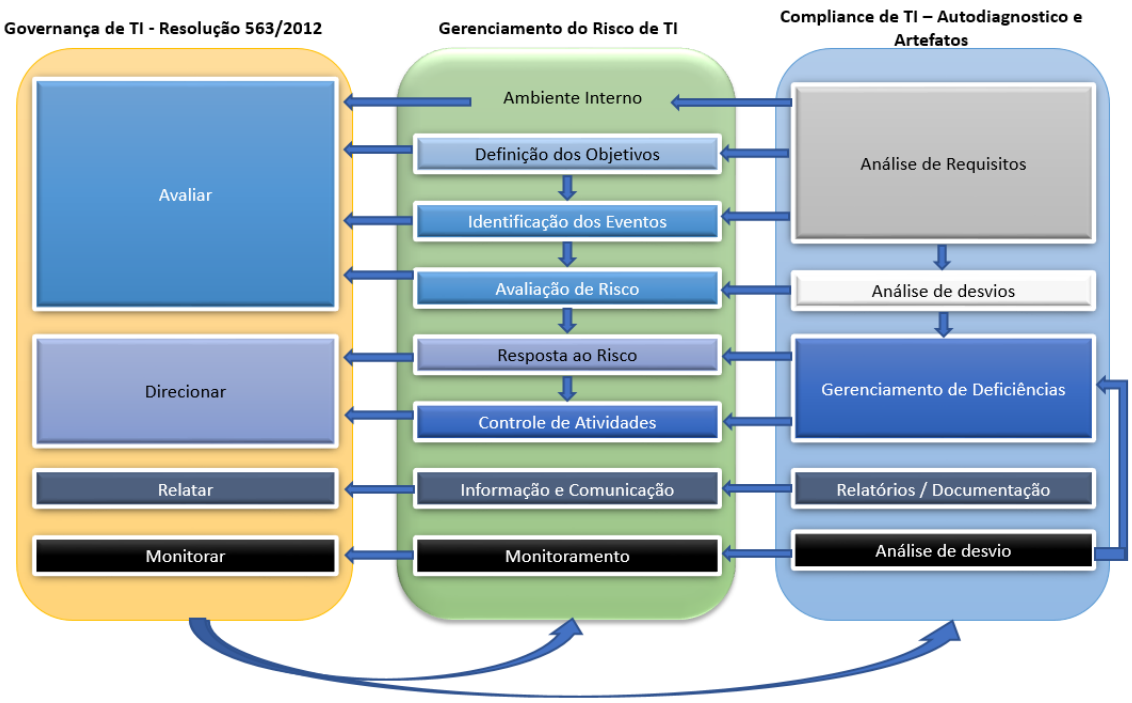
GRC PARA A ORGANIZAÇÃO

Se considerarmos que as boas práticas de Governança de TI tendem a mitigar os riscos institucionais, sobretudo os dos negócios, a não implantação dos processos apontados pela resolução 563/2012 pode gerar uma exposição a riscos substancial, com alguns deles não avaliados e não mitigados, promovendo a ocorrência de incidentes relacionados a estes processos, que trarão prejuízos aos serviços e processos de negócios do Sistema.

Segundo Vunk, Mayer e Matulevicius (2017), domínios como governança de TI, gerenciamento de riscos e conformidade são essenciais para orientar a TI. Embora tenha havido algumas melhorias, esses domínios são geralmente considerados separadamente, gerando, em consequência, menos valor de negócio, devido à complexidade dos fluxos dos processos.

O Modelo de Racz, Weippl e Selfort (2008), figura 3, foi adotado para aplicar o ciclo GRC no Sistema Indústria, utilizando a Resolução 563/2012 da CNI como modelo de Governança de TI. Esses processos de Governança são entradas para a avaliação de conformidade realizada por meio de pesquisa, gerando um autodiagnostico do grau de conformidade dos processos da Resolução. Em continuidade, a identificação e avaliação dos riscos fecharam o ciclo GRC, com a apresentação das exposições críticas quanto ao não cumprimento do modelo de Governança de TI.

Figura 3 – Modelo utilizado para o ciclo GRC no sistema Indústria



Fonte: Racz, Weippl e Seufert (2008) – Adaptada

A figura 3 reflete a adaptação do modelo de Racz, Weippl e Seufert (2008), uma vez que a revisão de literatura apontou para novos *frameworks*, também usados como modelo de governança, gerenciamento de risco e *compliance*.

Na ótica da Governança de TI, foi utilizada a resolução 563/2012, modelo de governança da instituição pesquisada, enquanto o modelo de Racz, Weippl e Seufert (2008), adotaram a ISO/IEC 38.500 que é a norma que trata a governança corporativa.

Quanto ao modelo adotado para o gerenciamento de Risco, esse estudo adaptou também o modelo de Racz, Weippl e Seufert (2008), que utilizou o COSO ERM:2004. O COSO ERM foi projetado para criar uma "consciência sobre riscos e controles" por toda a empresa e tornar-se um modelo comum para a discussão e avaliação de riscos organizacionais - *Enterprise Risk Management Framework* (ERM), neste estudo foi usado como referência a ISO/IEC 31000:2009 e a 31010:2011. A ISO/IEC 31000:2009 é a norma internacional para gestão de risco e a ISO/IEC 31010:2011 é uma das normas de suporte da ISO 31000, de Gestão de Riscos e fornece orientação sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos.

Ainda quanto a adaptação do modelo de Racz, Weippl e Seufert (2008), o modelo usado pelos autores para a defesa do modelo de GRC na disciplina *compliance* foi o modelo de Rath e Sponholz (2009), enquanto na defesa deste trabalho o modelo adotado foi a ISO/IEC 19600:2014, que fornece orientações para o estabelecimento, desenvolvimento, implementação, avaliação, manutenção e melhoria do sistema de gestão de *compliance*.

Na Figura 3, foram retratados os insumos para a elaboração desta pesquisa, tendo como parâmetro para um modelo de Governança de TI a Resolução da CNI 563/2012, o Gerenciamento de riscos, com base em estudo e análise de grupo focal e, finalizando, o audiagnostico que apresentou o nível de conformidade à resolução 563/2012, gerando o ciclo GRC para a instituição pesquisada.

MODELO DE GOVERNANÇA DA ORGANIZAÇÃO

A resolução 563/2012 foi assinada em 31 de julho de 2012, com a indicação de ser implantada inicialmente no Departamento Nacional do SENAI. A Resolução resolve "Aprovar o modelo de Governança de Tecnologia da Informação para as Entidades do Sistema Indústria", tendo como primeira etapa a implantação no SENAI, a partir de janeiro de 2013. O presidente do Conselho Nacional do SENAI, Sr. Robson Braga de Andrade, utiliza termos enfáticos na assinatura da Resolução: "Registre-se, dê-se ciência e cumpra-se". Tal ênfase destaca a preocupação da instituição maior do Sistema Indústria quanto à adoção de um modelo de Governança para as entidades que o compõem.

O Modelo de Governança de TI para as entidades do Sistema Indústria apresenta informações acerca dos processos de planejamento, aquisição de bens e serviços de TI, de segurança da informação, auditoria dos processos de TI e de gestão de recursos humanos de TI. Além disso, o documento reúne princípios e diretrizes que norteiam as ações relacionada à Governança de TI.

Os princípios que orientaram a elaboração da proposta de um modelo de Governança de TI foi o foco no negócio, orientação a processos, melhoria contínua e alinhamento sistêmico. Na Resolução, estes foram definidos da seguinte forma:

- Foco no negócio - trata do alinhamento das ações de TI com os objetivos estratégicos das entidades do sistema Indústria;

• Orientação a processos - trata das estruturas, relacionamentos e comunicação, necessários para a organização e alcance das metas;

• Melhoria contínua - trata do aperfeiçoamento contínuo dos processos de TI, apoiado por mecanismos de controle eficazes e métricas objetivas e rastreáveis.

• Alinhamento sistêmico - trata de consolidação do uso das práticas de Governança de TI entre as áreas de TI dos entes do Sistema indústria.

Independentemente de como a área de TIC esteja estruturada, fundamentalmente o que precisa ser avaliado é o quanto os esforços em TIC podem estar contribuindo para as linhas de negócio das entidades do Sistema Indústria. Nesse sentido, a CNI propõe, por meio da Resolução 563/2012, um modelo de Governança de TI (GTI) como balizador para todas as entidades do Sistema Indústria, por entender que a GTI é evidentemente fundamental para o atingimento das metas institucionais.

COMPLIANCE DA RESOLUÇÃO - CNI 563/2012

O questionário aplicado aos gestores de TI do Sistema Indústria, em todos os Estados da Federação, foi restrito às instituições que compõem o SESI, SENAI, FIBRA e IEL, em âmbito nacional. Essas instituições podem ser geridas pela mesma área de TI ou serem geridas de forma independente, por isso, alguns estados possuem mais de um representante.

Por meio do autodiagnostico realizado, foi possível avaliar as conformidades da TI das entidades à Resolução 563/2012. A pesquisa apontou, numa escala Likert, o grau de conformidade avaliado por cada gestor, gerando, ao final, um *score* representando o nível de conformidade à Resolução na percepção do entrevistado.

A escala Likert gerada para cada item da resposta foi:

– Totalmente Implantado - 85 a 100% – O indicador direto está presente e é considerando adequado. Existe ao menos um indicador indireto e/ou afirmação confirmando a implementação.

– Largamente Implantado - 50 a 85% – O indicador direto está presente e é considerando adequado. Existe ao menos um indicador indireto e/ou afirmação confirmando a implementação.

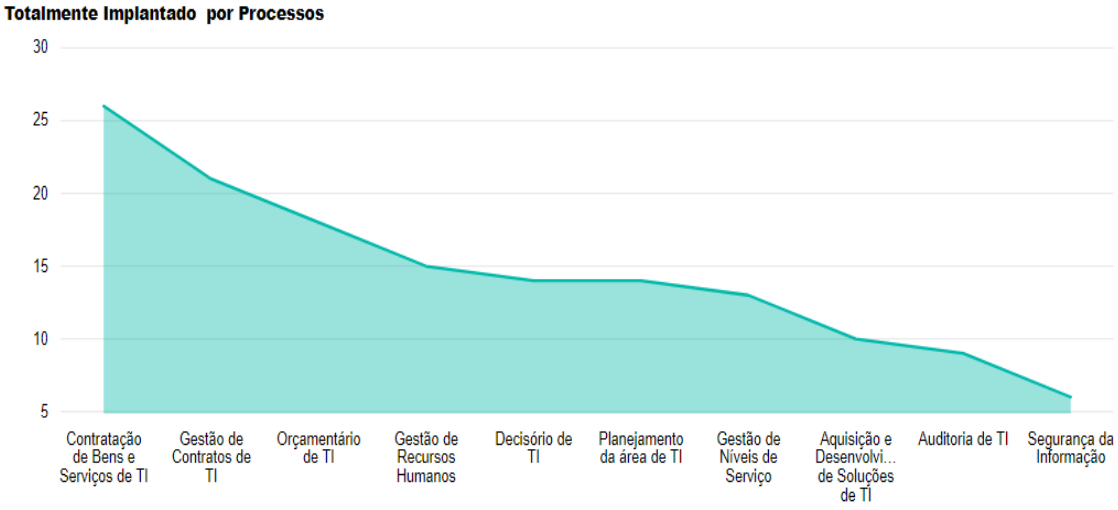
– Parcialmente Implantado - 15 a 50% – O indicador direto não está presente ou é julgado inadequado. Pode existir ao menos um indicador indireto e/ou afirmação que confirmando a implantação;

– Não implantado - 0 a 15% – O indicador direto não está presente ou é julgado inadequado. Não existe um indicador indireto e/ou afirmação que confirme a implantação.

A consolidação dos resultados de cada processo da resolução 563/2012, permitiu comparar o grau de implantação de cada processo, que os gestores classificaram entre totalmente implantado, largamente implantado, parcialmente implantado e não implantado.

A figura 4, destaca, dentre todos os processos, *Contratação de Bens e Serviços de TI* que é reconhecido como um processo totalmente implantado em 26 das 30 instituições do Sistema Indústria que participaram da pesquisa, seguido de *Gestão de Contratos de TI* com 21 instituições, *Orçamento de TI* com 17, *Gestão de RH* com 15 e o *processo decisório de TI*.

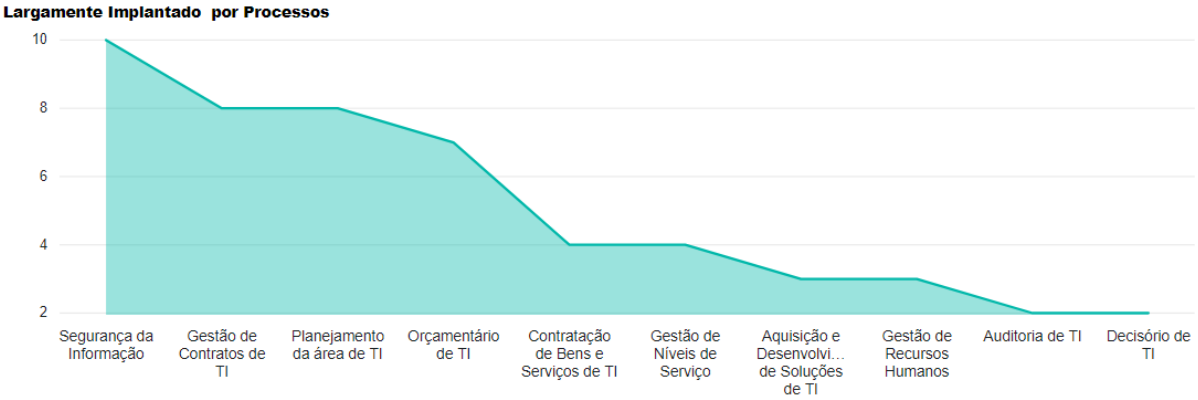
Figura 4 - Totalmente Implantado



Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria (2018)

Quanto aos processos considerados como largamente implantados, podemos observar à sequência representada na figura 5.

Figura 5 - Largamente Implantado

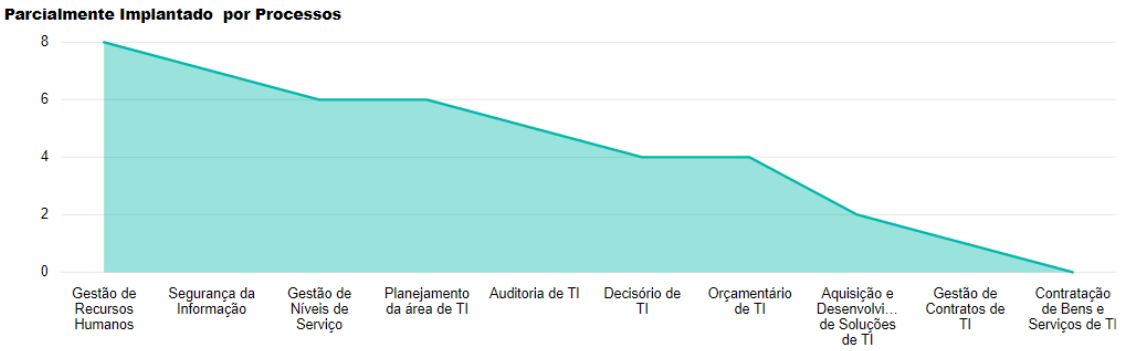


Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria

Segurança da informação foi considerado um processo largamente implantado por 10 instituições pesquisadas, seguido *de Gestão de Contratos, Planejamento da área de TI, Orçamentário de TI* e *Contratação de Bens e serviços*.

Processos que foram interpretados como Parcialmente Implantados teve o seu máximo em 8 instituições. A figura 6 exibe o processo *Gestão de Recursos Humanos* como sendo o mais avaliado como Parcialmente Implantado, seguido de *Segurança da informação*, *Gestão de Níveis de Serviço*, *Planejamento da área de TI* e *Auditoria de TI*.

Figura 6 - Parcialmente implantado

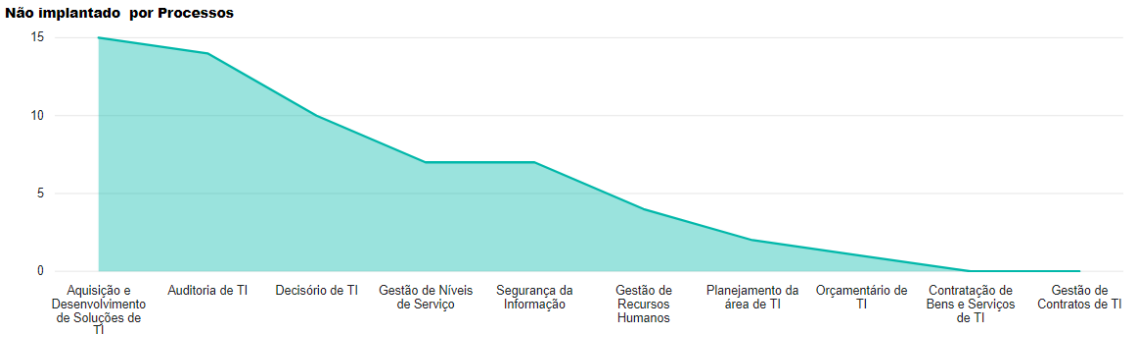


Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Quanto à análise dos processos Não Implantados, a figura 7 mostra que o processo *Aquisição e Desenvolvimento de soluções de TI* não está implantado em

metade das instituições participantes, seguido do processo *Auditoria de TI, Processo Decisório de TI, Gestão de Níveis de Serviço e Segurança da Informação.*

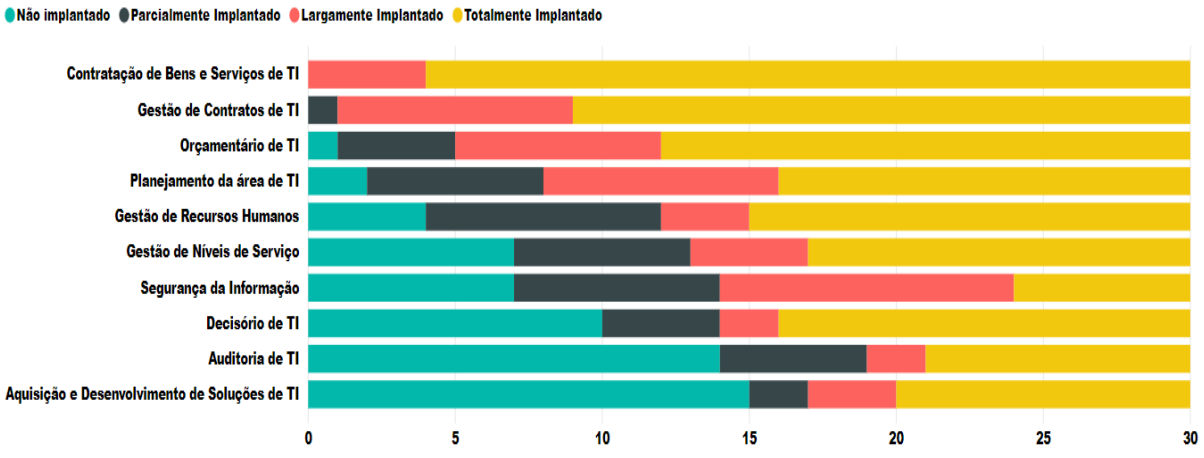
Figura 7 - Não implantado



Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Uma outra visão pode ser observada na Figura 8. Nesta figura, os dados apresentados anteriormente podem ser observados também por meio de uma visão onde os processos estão organizados por capacidade, mostrando primeiramente os com status de Totalmente Implantado e, em sequência, Largamente Implantado, Parcialmente implantado até o Não Implantado.

Figura 8 - Análise por processos em linhas



Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Análise Individual dos Processos

Os processos da Resolução 563/2012, quando analisados individualmente, exibem alguns pontos de atenção. A tabela 1 mostra a consolidação do autodiagnostico, apresentando os processos na sequência definida pela resolução 563/2012.

Tabela 1 – Análise por processo ordenados pela sequência da resolução

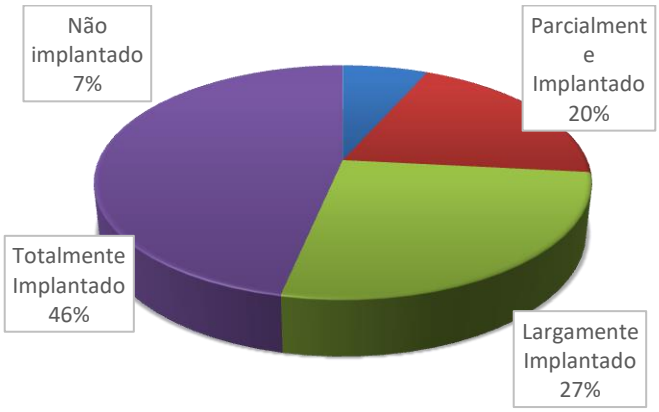
Número	Processos	Totalmente Implantado	Largamente Implantado	Parcialmente Implantado	Não implantado
1	Planejamento da área de TI	14	8	6	2
2	Decisório de TI	14	2	4	10
3	Gestão de Recursos Humanos	15	3	8	4
4	Segurança da Informação	6	10	7	7
5	Aquisição e Desenvolvimento de Soluções de TI	10	3	2	15
6	Gestão de Níveis de Serviço	13	4	6	7
7	Contratação de Bens e Serviços de TI	26	4	0	0
8	Gestão de Contratos de TI	21	8	1	0
9	Orçamentário de TI	18	7	4	1
10	Auditoria de TI	9	2	5	14

Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

1 - Planejamento de TI

Esse é um processo que, predominantemente, foi diagnosticado entre Totalmente Implantado ou Largamente Implantado, demonstrando alta aderência. Apenas 7% das regionais não exercem o planejamento de TI, conforme exibido no gráfico da figura 9:

Figura 9 - Processo Planejamento de TI

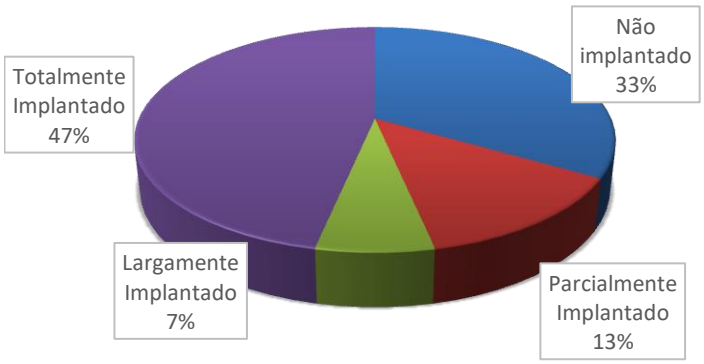


Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

2 - Decisório de TI

Das Instituições pesquisadas, conforme exibido na figura 10, 47% declararam ter este processo Totalmente Implantado, entretanto, entre Não Implantado e Parcialmente Implantado totaliza-se 46%. Analisando os dados, percebe-se que o processo decisório é um processo que requer atenção em grande parte das instituições diagnosticadas, aproximando os 50%.

Figura 10 - Processo Decisório

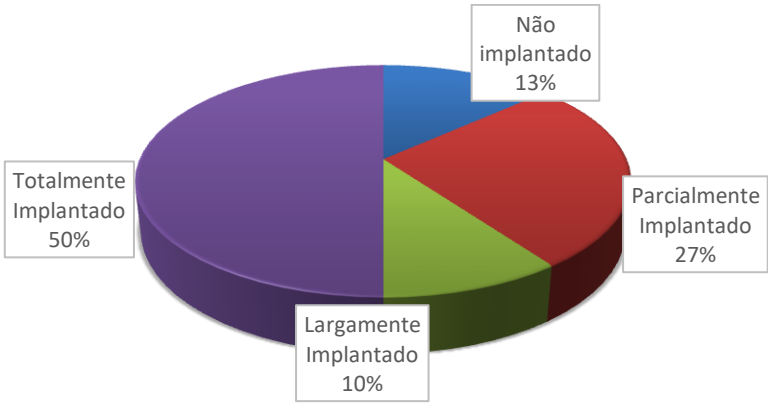


Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

3 - Gestão de Recursos Humanos

Esse processo está Amplamente Implantado nas Regionais. Ao somarmos Totalmente Implantado a Largamente Implantado, temos uma declaração de implantação na ordem de 60%. Apenas 13% das instituições declararam não gerir RH, conforme exibido na figura 11.

Figura 11 - Processo Gestão de Recursos Humanos

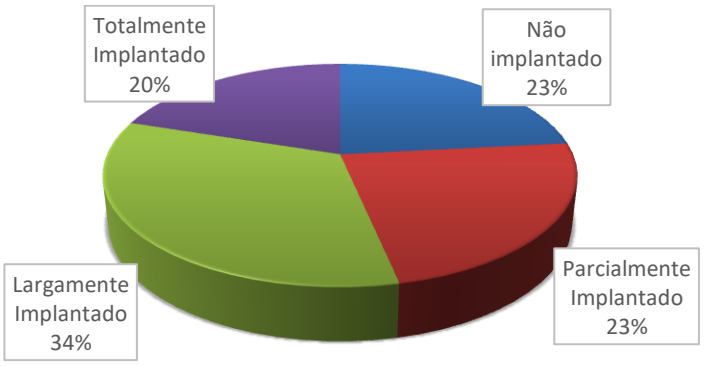


Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

4 - Segurança da Informação

De todos os processos da resolução 563/2012, Segurança da Informação foi o que mais dividiu o status de implantação. Não Implantado e Parcialmente Implantado apresentam 23%, totalizando 46%, enquanto, Largamente Implantado com 34% e Totalmente Implantado com 20% totalizam 54%, conforme exibido na figura 12.

Figura 12 - Processo Segurança da Informação



Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

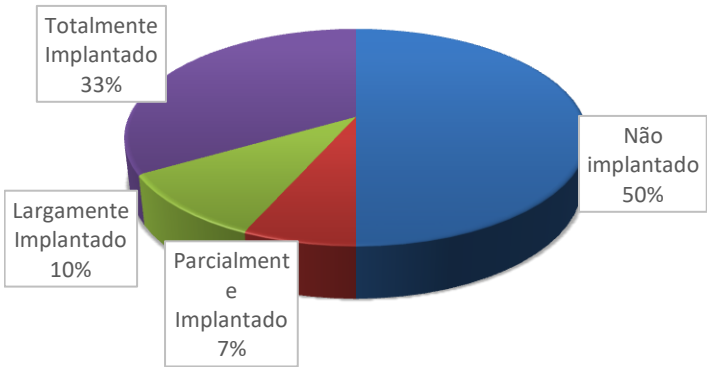
Considerando a criticidade deste processo, bem como, a quantidade de artefatos exigidos pela resolução para o mesmo, cabe fazer uma análise crítica da

situação uma vez que 46% com baixa aderência desperta pontos de atenção quanto aos riscos envolvidos.

5 - Aquisição e Desenvolvimento de Soluções de TI

Conforme pesquisa, 50% das instituições do Sistema Indústria declararam não ter implantado este processo, conforme exibido na figura 13.

Figura 13 - Processo Aquisição e Desenvolvimento de Soluções de TI



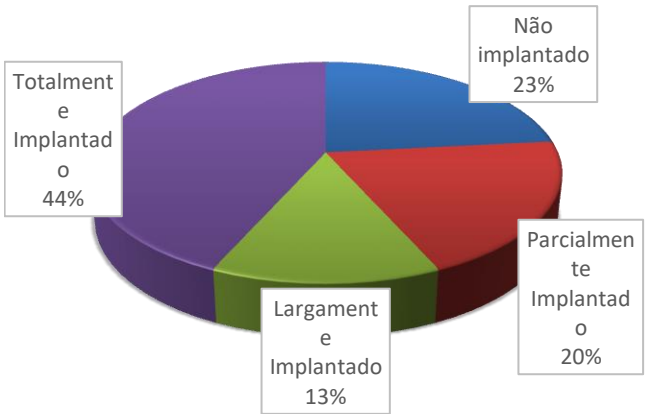
Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Ainda observando a Figura 13, se somado os Não Implantados aos que consideram Parcialmente Implantado totaliza-se 57%. Evidentemente esse número gera um ponto de atenção quanto aos riscos inerentes à não implantação.

6 - Gestão de Níveis de Serviço

Este processo foi declarado como Totalmente Implantado e Largamente Implantado, totalizando 57%, conforme exibido na figura 14.

Figura 14 - Processo Gestão de Níveis de Serviços



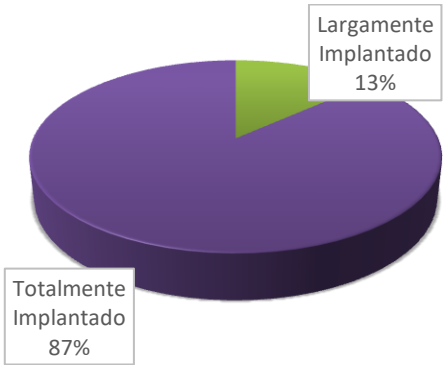
Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Somando Não implantado com Parcialmente Implantado, totaliza-se 46%, sendo que 23% representa 7 de 30 estados que não possuem gestão sobre os níveis de serviço.

7- Contração de Bens e Serviços de TI

Esse processo basicamente concentrou-se entre Totalmente Implantado e Largamente Implantado, conforme exibido na figura 15.

Figura 15 - Processo Contratação de Bens e Serviços



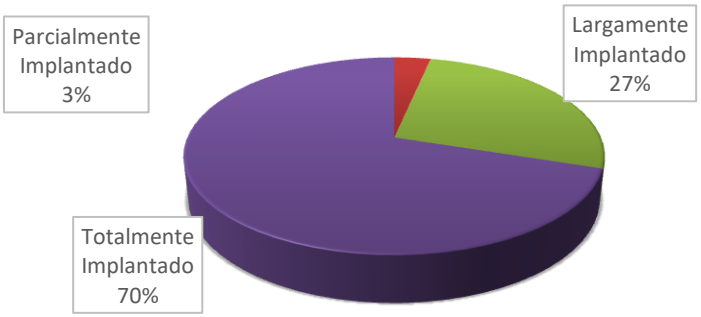
Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Esse resultado representa uma excelente aderência ao processo, demonstrando que apenas 4 instituições precisam gerar seus artefatos para migrar para Totalmente Implantado. Esse processo é o melhor estruturado dentre todos os diagnosticados.

8 - Gestão de Contratos

Esse processo destaca-se por ser amplamente implantado. Nenhuma instituição declarou não ter implantado e apenas 3% declarou ter Parcialmente Implantado, conforme apresentado na Figura 16.

Figura 16 - Processo Gestão de Contratos



Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

É também um processo que apresenta uma boa adesão por parte das instituições pesquisadas.

9 - Orçamentário de TI

Observa-se, neste processo, uma alta aderência à Resolução 563/2012. Apenas 3% das instituições demonstraram não gerir este processo e 14% declaram tê-lo feito parcialmente. A Figura 17 expõe este resultado.

Figura 17 - Processo Orçamentário de TI

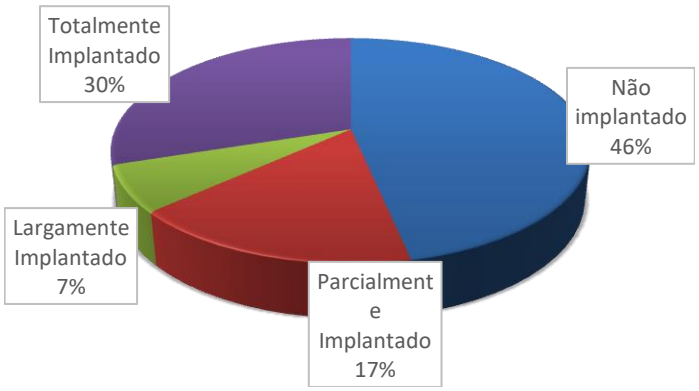
Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Predominantemente, no país, o processo está Implantado ou Largamente Implantado, totalizando 83%.

10 - Auditoria de TI

Este processo traz um dos piores resultados quanto à não implantação. Tem-se que 46% das instituições pesquisadas declararam não ter este processo implantado e 17 % possuem apenas parcialmente, conforme exibido na figura 18.

Figura 18 - Processo Auditoria de TI



Fonte: autodiagnostico aplicado aos Gestores do Sistema Indústria - 2018

Totalmente Implantado e Largamente Implantado totalizam 37%, entretanto, considerando a predominante ausência de implantação em nível nacional, cabe atenção aos riscos inerentes à não implantação do processo.

IDENTIFICAÇÃO E AVALIAÇÃO DOS RISCOS DE COMPLIANCE

Nesta seção, são apresentados os riscos inerentes a não-conformidades com a resolução 563/2012. Esses riscos foram apontados por meio de um levantamento em grupo focal.

Considerando as múltiplas finalidades dos grupos focais, pode-se dizer que um dos passos mais importantes ao se planejar um grupo focal é estabelecer o propósito da sessão (BARBOUR; KITZINGER, 1999). Neste sentido, houve o convite a 6 gestores de TI do Sistema Indústria para que participassem de uma

sessão via Skype, para avaliação dos riscos eminentes as não conformidades da resolução 563/2012.

O grupo de gestores do Sistema Indústria que foi escolhido para participar do grupo focal foi caracterizado como um grupo de caráter exploratório, ou seja, todos estavam centrados na produção de conteúdo; a sua orientação teórica estava voltada para a geração de hipóteses.

Foram realizados 3 encontros de 1h, para que os riscos avaliados pelo grupo focal. O resultado deste processo de avaliação de riscos foi fornecer informações baseadas em evidências e análise para tomar decisões informadas sobre como tratar riscos específicos. A ISO/IEC 31010:2011, aponta os principais objetivos de uma avaliação de riscos, aos quais parte deles estão correlacionados como resultado desta avaliação de risco, gerada pelo grupo focal. Dentre elas cito:

• Entender o risco e seu potencial impacto sobre os objetivos Institucionais do Sistema Indústria;

• Fornecer informações aos tomadores de decisão;

• Contribuir para o entendimento dos riscos a fim de auxiliar na seleção das opções de tratamento;

• Identificar os principais fatores que contribuem para os riscos e os elos fracos em sistemas e organizações;

• Comparar riscos em sistemas, tecnologias ou abordagens alternativas;

• Comunicar riscos e incertezas;

• Auxiliar no estabelecimento de prioridades;

• Fornecer informações que ajudarão a avaliar a conveniência da aceitação de riscos quando comparados com critérios pré-definidos.

CONCLUSÕES

O resultado da pesquisa evidenciou que implementar GTI adequadamente não é tarefa trivial. Todos os dez processos relacionados ao Modelo de Governança instituído por meio da resolução 563/2012 não estão totalmente implantados em todos as trinta e uma instituições pesquisadas.

Evidencia-se que os processos que estão com maior nível de implantação, ao exemplo de *Contratação de Bens e Serviços de TI, Gestão de Contratos e Orçamentário de TI,* são processos que estão relacionados ao cumprimento de aspectos legais, onde os riscos institucionais já são conhecidos e difundidos dentro das instituições. Além disso, são processos frequentemente auditados pelos órgãos reguladores do Sistema Indústria.

O modelo GRC proposto por Racz, Weippl e Seufert (2008), adequado aos *frameworks* atuais nesta pesquisa, permitiu identificar os riscos inerentes às não conformidades na implantação do modelo de governança previsto na resolução 563/2012, para as instituições do Sistema Indústria.

Os resultados obtidos evidenciam o comportamento de GRC como um fluxo que deve ser ininterrupto em busca de melhoria contínua, uma vez que o fundamento de GRC é apoiar a ação de Governança, Risco e *Compliance* de TI, tanto na implantação quanto na manutenção dos *frameworks* utilizados na gestão de tais disciplinas.

As características de um modelo GRC geram uma visão ampla sobre o que está acontecendo em cada processo, bem como, apontam para a necessidade de estruturação de planos de ação para a mitigação dos riscos e cumprimento das regras de *compliance*.

Essa pesquisa teve como objetivo geral, *contribuir para o aprimoramento da governança de TI sob a ótica da integração dos processos de GRC*. As características de um modelo GRC supracitadas cumprem esse objetivo, uma vez que dão uma visão ampla de todos os “gargalos” inerentes a um modelo já implantado, bem como apoiam a implantação do modelo, permitindo que todos os atores envolvidos tenham uma visão dos impactos das não conformidades inerentes ao modelo de Governança.

A adaptação do modelo de Racz, Weipll e Seufert (2008) aos *frameworks* atuais demonstrou, por meio do estudo de caso, uma contribuição como instrumento de implantação e manutenção de um modelo de Governança de TI.

As questões respondidas por este trabalho, objetivadas pelo aprimoramento da Governança de TI, levam à conclusão de que um ciclo GRC é um forte mecanismo para apoio e manutenção de um modelo de Governança de TI, uma vez que é capaz de dar uma visão mais ampla dos riscos relacionados às não conformidades dos processos de um modelo de Governança.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas - International Organization for Standardization. ABNT ISO 19600:2014 - **Sistema de gestão de *compliance* – Diretrizes,** ISBN 978-85-07-06228-8. 2014

Associação Brasileira de Normas Técnicas - International Organization for Standardization ABNT ISO 31000:2009 – **Gestão de Riscos - Princípios e diretrizes.** 2009

Associação Brasileira de Normas Técnicas - International Organization for Standardization / International Electrotechnical Commission ABNT ISO/IEC 31010:2009 - **Ferramentas e Técnicas para Avaliação de Riscos**. 2009

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. **Institucional**. Disponível em: <http://www.portaldaindustria.com.br/cni/institucional/2012/07/1,1826/sistema-industria.html>Acesso em: 30 de nov. 2016.

EDEPHONCE N. NFUKA, LAZAR RUSU, (2011) "**The effect of critical success factors on IT governance performance",** Industrial Management & Data Systems, Vol. 111 Issue: 9, pp.1418-1448, doi: 10.1108/02635571111182773

GIL, A. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

GRANBERGEN, V; HAES, S. **Measuring and Improvind IT Governance Through the Balanced Scorecard**. Information Systems Control Journal, Volume 2, 2005

HOJI, M. **Administração Financeira**: Uma abordagem prática: matemática financeira aplicada, estratégias financeiras, análise; planejamento e controle financeiro. 2. ed. São Paulo: Atlas, 2000

International Organization for Standardization / Publicly Available Specification ISO/PAS 17005: **Conformity assessment - Use of management systems - Principles and requirements.** 2008

ISACA. **COBIT 5 Control Objectives for Information and related Technology**: Enabling Processes (versão 5). Rolling Meadows: IT Governance Institute, 2012.

ISACA. **COBIT 5 For Risk**: Enabling Processes (versão 5). Rolling Meadows: IT Governance Institute, 2013.

KREY, M; FURNELL, S. **Approach to the Evaluation of a Method for the Adoption of Information Technology Governance, Risk Management and Compliance in the Swiss Hospital Environment.** Centre for Security, Communications & Network Research University of Plymouth, Plymouth, United Kingdom. 2012

KUTSIKOS, K; BEKIARIS, M. **Perspectives and Challenges for IT Governance.** Department of Business Administration University of the Aegean, MIBES,2007

MIRANDA, L.G. **Uso da Simulação para Implantação da Governança da Tecnologia da Informação**. 2014. 138 fls. Dissertação de Mestrado – Universidade Católica de Brasília. Brasília, 2014.

NIST Special Publication 800-100. **Information Security. *Handbook*: *A Guide for*. *Managers***. 2007. Disponível em: < http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>. Acesso em: 02 ago 2016.

OECD (2014), Risk Management and Corporate Governance, Corporate Governance, OECD Publishing. http://dx.doi.org/10.1787/9789264208636-en.

RACZ, N; WEIPPL, E; SEUFERT, A. **A Process Model For Integrated It Governance, Risk, And Compliance Management.** Institute for Software Technology and Interactive Systems, Favoritenstr. 9-11 1040, Vienna, Austria, 2008

RACZ, N., WEIPPL, E. & SEUFERT, A.: **A frame of reference for research of integrated governance, risk, and compliance (GRC).** In: Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (2010)

SETHIBE, T; CAMPBELL, J, MCDONALD, C. **IT Governance in Public and Private Sector Organisations: Examining the Differences and Defining Future Research Directions.** School of Information Sciences and Engineering University of Canberra, Canberra, Australia, 2007.

SILVA, E.; MENEZES, E. **Metodologia da pesquisa e elaboração de dissertação**. Florianópolis: UFSC, 4. ed. 2005. Disponível em: < https://projetos.inf.ufsc.br/arquivos/Metodologia

SMET, D; MAYER, N. **Integration of IT Governance and Security Risk Management: a Systematic Literature Review.** Institute of Science and Technology 5, avenue des Hauts-Fourneaux, Luxembourg. 2016

SYMONS, C; CACERE, M; YOUNG, O; Lambert, N. **IT Governance Framework**. 2005

VAUGHAN, E. **Risk Management (Hardcover).** 1997

VUNK, M; MAYER, N; AND MATULEVIČIUS, R. **Framework for Assessing Organisational IT Governance, Risk and Compliance.** Institute of Computer Science, University of Tartu, Estonia; Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg, 2017

WEILL, P; ROSS, J. **IT Governance on One Page.** CISR WP. 349 and Sloan.