Aderência do *framework* COBIT 5 em relação a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013

Adhesion of Cobit 5 framework in relation to information security rule ABNT NBR ISO/IEC 27002:2013

Denise da Silva Pimentel, Leandro do Anjos Tavares, Thamiris Silvestre Ferreira
Universidade Paulista - UNIP
Departamento de Exatas - Bacharelado em Sistemas da Informação
{denise.s.pimentel@hotmail.com, leandro.tavares1@hotmail.com, tham_10@hotmail.com}

Resumo. O termo "governança" ganhou um lugar de destaque no pensamento das organizações, surge à necessidade de alinhar as funções de TI e de negócios na abordagem de governança e gestão para proporcionar o equilíbrio entre a realização de benefícios, a otimização dos níveis de risco e a utilização dos recursos. Este artigo tem por objetivo apresentar uma análise capaz de demonstrar a aderência do *framework* Cobit 5 em relação à norma de segurança da informação ABNT NBR ISO/IEC 27002:2013. Para o desenvolvimento da análise foram mapeados as áreas de domínio do Cobit 5 em relação aos códigos de práticas para controles da segurança da informação descritos na norma ABNT NBR ISO/IEC 27002:2013. Por fim concluiu-se com a análise que apenas 29% dos processos do Cobit 5 são abordados na norma ABNT NBR ISO/IEC 27002:2013, no entanto os processos que não são abordados foram considerados relevantes ao *framework*.

Palavras-chave: Cobit, ABNT NBR ISO/IEC 27002, governança, segurança da informação.

Abstract. *The term "governance" gets a featured place in organizations thoughts. With IT advance, comes the necessity to align IT and business functions to governance approach and management to provide balance between benefits realization, levels risk optimization and resource use. This paper aims objective show a capable analysis to demonstrate the adhesion of Cobit 5 framework in relation to the security information rule ABNT NBR ISO/IEC 27002:2013. To develop this analysis, domain areas from Cobit 5 were mapped in relation to the practice codes for information security controls, described on ABNT NBR ISO/IEC 27002:2013 rule. Ultimately, with this analysis it concluded that only 29% of Cobit 5 process consists in ABNT NBR ISO/IEC 27002:2013, however process that not consist were considered relevant to framework.*

Key words: Cobit, ABNT NBR ISO/IEC 27002, *governance*, *information security.*

Iniciação - Revista de Iniciação Científica, Tecnológica e Artística
Edição Temática em Tecnologia Aplicada
Vol. 5 no 4 – Dezembro de 2015, São Paulo: Centro Universitário Senac
ISSN 2179-474X

Portal da revista: http://www1.sp.senac.br/hotsites/blogs/revistainiciacao/
E-mail: revistaic@sp.senac.br

1. Introdução

Um dos recursos essenciais para todas as organizações é a informação e a tecnologia que desempenha um papel significativo neste processo, pois trata a informação desde o momento de sua criação até o momento em que é destruída. A tecnologia da informação TI está cada vez mais indispensável nas organizações, ambientes sociais, públicos e corporativos e como consequência, as organizações se esforçam cada vez mais para atingir seus objetivos e obter benefícios através dos investimentos em TI (BARBOSA, A.; BARBOSA, S.; BATISTONI; LIMA; MATA; MELO; TAMAE, 2011).

Nos últimos anos, o termo "governança" ganhou um lugar de destaque no pensamento das organizações em resposta aos exemplos que demonstram a importância da boa governança frente aos desafios dos negócios globais. Governança é o conjunto de processos, regulamentos, decisões, costumes e ideias que mostram a maneira pela qual a organização é dirigida ou administrada. A governança assegura que as necessidades e posicionamentos das partes interessadas sejam avaliadas a fim de definir objetivos corporativos equilibrados, determinando a direção a ser seguida e monitorando o desempenho e a conformidade com o que foi estabelecido (ISACA, 2012).

Surge então à necessidade de alinhar as funções de TI e de negócios a fim de garantir que a TI esteja incluída na abordagem de governança e gestão para proporcionar o equilíbrio entre a realização de benefícios, a otimização dos níveis de risco e a utilização dos recursos (ISACA, 2012).

Através da combinação da governança corporativa e da governança de TI, foi desenvolvido o *Control Objectives for Information and related Technology* - COBIT, uma ferramenta reconhecida e aceita no mercado global que fornece um modelo abrangente para auxiliar as organizações a atingirem seus objetivos de governança e gestão. A última versão editada é a Cobit 5, mantida pela *Information Systems Audit and Control Foundation* - ISACA (ISACA, 2008).

O objetivo deste artigo é apresentar uma análise capaz de demonstrar a aderência do *framework* Cobit 5 em relação a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013.

Neste artigo, foi realizada uma análise de como o Cobit 5 trata a segurança da informação, e o indicador desta análise foi baseado na norma ABNT NBR ISO/IEC 27002:2013, última versão da norma disponibilizada pela Associação Brasileira de Normas Técnicas - ABNT que regulamenta toda a área de segurança da informação provendo um modelo para estabelecer, implementar, operar, monitorar, analisar, manter e melhorar a gestão da segurança dos ativos de tecnologia da informação.

O artigo está organizado da seguinte forma: a Seção 2 apresenta conceitos de governança corporativa e governança de T.I., *framework* Cobit 5 e a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013, a Seção 3 apresenta o mapeamento de aderência do *framework* Cobit 5 em relação a norma ABNT NBR ISO/IEC 27002:2013 e os resultados obtidos, a Seção 4 apresenta a conclusão deste artigo.

2. Governança corporativa e T.I., Cobit 5 e ABNT NBR ISO/IEC 27002:2013

A criação de valores em uma organização possui significados variados para seus *stakeholders* e muitas vezes estes significados são incompatíveis entre si. Visando resolver estes conflitos, a governança atua essencialmente no que diz respeito à negociação, decisão e priorização dos interesses e deve considerar todas as partes interessadas ao deliberar sobre a avaliação dos riscos e oportunidades (ISACA, 2012).

A governança visa certificar que as necessidades e preferências dos *stakeholders* sejam avaliadas a fim de determinar objetivos organizacionais balanceados e direcionar as tomadas de decisão, monitorando o desempenho e a consonância com os objetivos estabelecidos. Neste contexto, a gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades conforme a direção determinada a fim de alcançar os objetivos da organização (ISACA, 2012).

Segundo o Instituto Brasileiro de Governança Corporativa - IBGC, Governança Corporativa é:

> O sistema pelo qual as organizações são dirigidas, controladas e estimuladas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa transformam princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e aperfeiçoar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.

As organizações necessitam gerir diversos ativos como recursos humanos, capital, instalações entre outros, mas a maior incerteza talvez esteja relacionada à informação e as tecnologias empregadas no recolhimento, armazenamento e disseminação das mesmas. Como os negócios estão sempre mudando, é necessário que os sistemas acompanhem essas mudanças e continuem seguros depois de implantados (WEILL; ROSS, 2006).

São necessários diversos investimentos de curto e longo prazo envolvendo as implementações de tecnologia da informação visando à obtenção de resultados difíceis de antecipar com certeza, o que torna então imprescindível fazer o alinhamento da tecnologia da informação às funções de negócio para garantir que a TI seja incluída na abordagem de gestão e de governança proporcionando o balanceamento entre o aproveitamento dos recursos, a obtenção de benefícios e a manutenção das condições de risco (WEILL; ROSS, 2006).

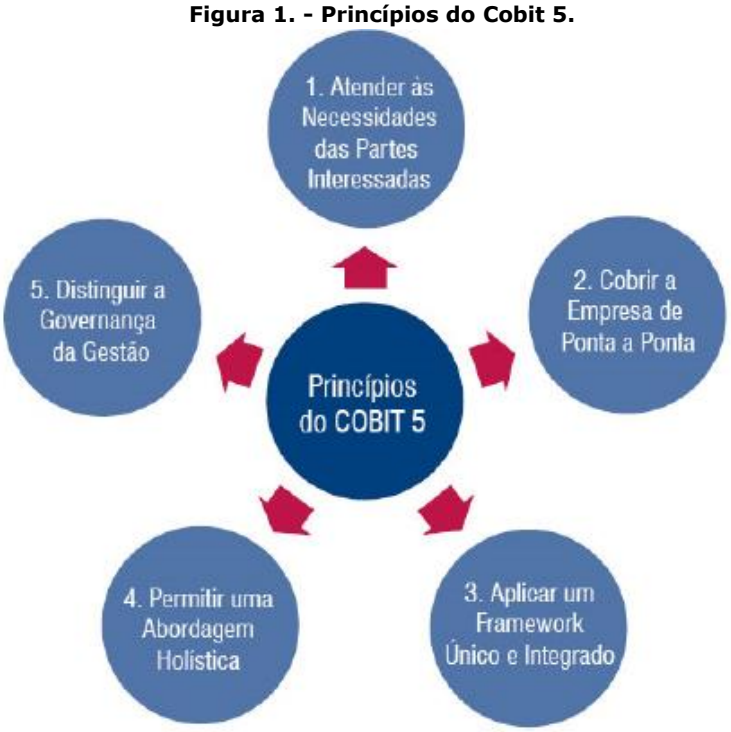
A subseção seguinte apresenta o *framework* Cobit 5, renomado como guia de boas práticas para a gestão e governança da tecnologia da informação.

***Framework* COBIT 5**

O Cobit (*Control Objectives for Information and related Technology*) é mantido pela ISACA (*Information Systems Audit and Control Association*) e provê um modelo para apoiar as organizações na gestão e gerencia da TI, e consequentemente na geração de valor aos negócios através do equilíbrio entre a geração de benefícios, a manutenção dos riscos e o uso devido dos recursos. (ISACA, 2015).

O Cobit 5 é um modelo genérico que pode ser empregado em todos os tipos e tamanhos de organizações e através dos seus princípios básicos, visa cobrir toda a extensão da organização (Figura 1).

Figura 1. - Princípios do Cobit 5.



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

1º: Atender ás necessidades das partes interessadas - Este princípio é fundamentado na geração de valor para o negócio e é aplicado através do desdobramento dos objetivos estratégicos da organização em objetivos específicos de TI, mapeados em processos característicos que possam ser gerenciados;

2°: Cobrir a Empresa de Ponta a Ponta – Tem como finalidade fazer a integração da governança de TI com a governança corporativa, considerando todos os fatores internos e externos que sejam importantes para a organização e para a gestão do negócio;

3°: Aplicar um *framework* único e integrado – Princípio que visa criar um modelo unificado para governança e gestão de TI agrupando de forma aderente todas as normas e boas práticas de TI reconhecidas internacionalmente;

4°: Permitir uma Abordagem Holística – O objetivo do quarto princípio é fornecer uma abordagem holística da governança e gestão de TI através de um tratamento eficiente e eficaz da interligação das diversas partes envolvidas, atendendo de forma única e integrada aos princípios e leis que conduzem a organização e se encontram em cada uma dessas partes;

5°: Distinguir a Governança da Gestão – Tem como objetivo diferenciar de forma explícita as atividades de governança e de gestão considerando os propósitos específicos de cada uma delas para a organização.

Os cinco princípios básicos do COBIT 5 podem ser colocados em prática através de processos habilitadores que são recursos organizacionais da governança. Esses habilitadores se apoiam em dois indicadores fundamentais para avaliação de desempenho e cumprimento das expectativas propostas em cada habilitador que são:

- Indicadores para cumprimento das metas, que têm o objetivo de verificar se as metas foram correspondidas e se as partes interessadas foram atendidas;
- Indicadores para aplicação das práticas, utilizados para verificar se as boas práticas estão sendo realizadas corretamente e se o gerenciamento do ciclo de vida está sendo aplicado.

O Cobit 5 mapeia os processos habilitadores em sete categorias, conforme a definição oferecida na documentação, Cobit 5 (ISBN 978 – 1 – 60420 – 284 - 7) Modelo Corporativo para Governança e Gestão de TI da organização:

- Princípios, políticas e modelos: São os meios de comunicação utilizados para transmitir para todos os níveis da organização as orientações e instruções da administração e do órgão de governança;
- Processos: Um conjunto de atividades influenciadas pelas políticas da organização que recebe entradas de diversas origens e as trabalha para produzir resultados;
- Estrutura organizacional: Habilitador que envolve todos os membros da organização, entidades organizacionais, clientes e fornecedores para atingir um modelo de estrutura organizacional;
- Cultura, ética e comportamento: Se refere ao conjunto de comportamentos individuais e coletivos da organização;
- Informação: Trata das informações importantes para a organização sendo elas automatizadas ou não e que podem ser classificadas como estruturadas ou desestruturadas; formalizadas ou não formalizadas;
- Serviços, infraestrutura e aplicativos: se refere aos recursos que tem foco na prestação de serviços de TI;
- Pessoas, habilidades e competências: Envolve as partes interessadas internas ou externas à organização e visa dimensionar as metas das habilidades e competências relacionadas, como níveis de qualificação, habilidades técnicas, níveis de experiência e conhecimento necessários para desenvolver as atividades do processo e os papéis organizacionais.

Para que o Cobit seja implementado em uma organização é recomendado que todos os profissionais envolvidos no negócio conheçam as suas funções e responsabilidades, partindo do nível estratégico e desdobrando-se do nível tático para o nível operacional (ISACA, 2012).

A subseção seguinte apresenta a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013 que foi projetada com o intuito de auxiliar todos os tipos e tamanhos de organização a estabelecer um controle efetivo da segurança da informação, a norma é utilizada como referência de boas práticas a serem seguidas no gerenciamento da segurança de todo e qualquer tipo de informação e ativos da organização (ABNT, 2013).

Norma de segurança da informação ABNT NBR ISO/IEC 27002:2013

A informação deve ser compreendida como todo tipo de representação de um conhecimento, seja ele falado, escrito ou em forma de imagens ou signos. Estas formas de conhecimento são consideradas ativos da organização e possuem grande importância para o negócio devendo então ser devidamente protegidos (ABNT, 2013).

Segundo a Associação Brasileira de Normas Técnicas – ABNT NBR ISO/IEC 27002:2013:

> É possível alcançar a segurança da informação colocando em prática um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para garantir que os objetivos do negócio e a segurança da informação da organização sejam alcançados.

Apesar de oferecer os meios técnicos necessários, os controles e processos contidos na norma são limitados por dependerem da gestão e da colaboração de todas as partes interessadas, internas ou externas, e a problemática da segurança da informação não pode ser solucionada apenas com a implantação desses controles. O código de boas práticas apresentado foi elaborado para aplicação em diversos tipos de negócios e desta forma, alguns controles e diretrizes podem não ser aderentes a todas as organizações podendo não suprir todas as necessidades de segurança da informação da organização sendo necessária a aplicação de controles adicionais e recomendações não contidas na norma (ABNT, 2013).

O capítulo seguinte apresenta o mapeamento e a análise de aderência do *framework* Cobit 5 em relação a norma ABNT NBR ISO/IEC 27002:2013.

3. Mapeamento de aderência do *framework* COBIT 5 em relação a norma ISO/IEC 27002:2013

A análise consiste em estabelecer um comparativo sobre como o *framework* Cobit 5 adere a normativa da segurança da informação de acordo com os padrões internacionais da ABNT NBR ISO/IEC 27002:2013.

Para o desenvolvimento da análise foram mapeados as áreas de domínios do Cobit 5 e a última norma vigente de segurança da informação ABNT NBR ISO/IEC 27002:2013. Este mapeamento é um guia comparativo que aborda os códigos de práticas para controles de segurança da informação relacionados aos domínios e processos compostos na última versão do *framework* Cobit 5.

A cobertura da segurança da informação é abordada em quatro áreas domínios, em consonância com as áreas responsáveis por planejar, construir, executar e monitorar (*Plan, Build, Run and Monitor* - PBRM).

Os domínios no mapeamento são descritos em sua forma abreviada (ISACA, 2012):

- Alinhar, Planejar e Organizar (*Align, Plan and Organise* – (APO);
- Construir, Adquirir e Implementar (*Build, Acquire and Implement* – (BAI);
- Entregar, Serviços e Suporte (*Deliver, Service and Support* - (DSS);
- Monitorar, Avaliar e Analisar (*Monitor, Evaluate and Assess* – (MEA).

Cada área de domínio possui processos que estão associados aos objetivos de T.I.. No mapeamento desenvolvido foram analisados todos os processos e objetivos contidos em cada domínio. O mapeamento de domínios foi segregado em tabelas padronizadas para auxiliar na interpretação da análise.

A tabela de mapeamento de domínios possui o seguinte *layout*: na posição esquerda foram descritos todos os processos em sua forma abreviada, na posição central estão descritos os objetivos de T.I. referentes a área de domínio e na posição direita foram descritos os códigos de práticas e controle de segurança da informação. Para compreensão do mapeamento, na coluna de processos a demarcação "x", significa que os processos demarcados referentes ao objetivo de T.I. ao qual está associado, possui aderência em um ou mais código de prática e controle de segurança da informação. Os códigos de

práticas para controles de segurança da informação são apresentados em tópicos e a descrição dos tópicos pode ser visualizada na Tabela 5.

- Mapeamento domínio APO (Tabela 1), consiste em analisar todos os processos e objetivos de T.I. contidos no domínio APO e demonstrar o relacionamento existente de cada processo e objetivo com o código de práticas para controles de segurança da informação ABNT NBR ISO/IEC 27002:2013. O domínio é composto por 13 processos (APO01 - Gerenciar a estrutura de Gestão de TI, APO02 - Gerenciar a estratégia, APO03 - Gerenciar Arquitetura da Organização, APO04 - Gerenciar Inovação, APO05 - Gerenciar portfólio, APO06 - Gerenciar orçamento e custo, APO07 - Gerenciar Recursos Humanos, APO08 - Gerenciar Relacionamentos, APO09 - Gerenciar Contratos de Prestação de Serviços, APO10 - Gerenciar Fornecedores, APO11 - Gerenciar Qualidade, APO12 - Gerenciar Riscos, APO13 - Gerenciar Segurança):

Tabela 1. Mapeamento domínio APO.

COBIT 5													Objetivos de TI	ABNT ISO/IEC ISO27002:2013
APO01	APO02	APO03	APO04	APO05	APO06	APO07	APO08	APO09	APO10	APO11	APO12	APO13		Código de Prática e Controle de Segurança de Informação
x	x	x	x	x	x	x	x	x		x			Alinhamento da estratégia de TI e negocios	6.1. / 6.1.2. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1.
x						x			x	x	x	x	Conformidade de TI e apoio para conformidade de negócio com leis e regulamentos externos	5. / 5.1.1. / 5.1.2. / 6.1.2. / 6.1.5. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x		x	x	x	x						Compromisso da gerencia executiva com a tomada de decisão de TI	6.1. / 6.1.2. / 7. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x	x	x	x	x	x	x	x	x	x	x	Gestão de risco organizacional de TI	5. / 5.1.1. / 5.1.2. / 6.1. / 6.1.2. / 6.1.5. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
	x	x	x	x	x		x	x	x	x			Beneficios obtidos pelo investimento de TI e portifólio de serviços	6.1. / 6.1.2. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
		x		x	x		x	x	x		x	x	Transparência dos custos, beneficios e riscos de TI	5. / 5.1.1. / 5.1.2. / 6.1.2. / 6.1.5. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x		x	x	x	x	x	x	x	x	x	Prestação de serviços de TI em consonância com os requisitos de negócio	5. / 5.1.1. / 5.1.2. / 6.1. / 6.1.2. / 6.1.5. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
	x	x	x	x	x		x	x	x	x	x	x	Uso adequado de aplicativos, informações e soluções tecnologicas	5. / 5.1.1. / 5.1.2. / 6.1. / 6.1.2. / 6.1.5. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x	x	x		x		x	x	x	x		Agilidade de TI	6.1. / 6.1.2. / 6.1.5. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.

x		x				x		x	x		x	x	Segurança da informação, infraestrutura de processamento e aplicativos.	5. / 5.1.1. / 5.1.2. / 6.1.2. / 6.1.5. / 7. / 7.1.1. / 7.1. / 7.1.2. /7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x	x	x	x	x	x	x	x	x			Otimização de ativos, recursos e capacidades de TI	6.1. / 6.1.2. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. /13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x	x				x						Capacitação e apoio aos processos de negócio atraves da integração de aplicativos e tecnologia nos processos de negócio	6.1. / 6.1.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. .
x	x			x	x	x	x	x	x	x	x		Entrega de programas fornecendo beneficios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	6.1. / 6.1.2. /6.1.5. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x	x	x					x	x	x	x	x	Disponibilidade de informações uteis e confiaveis para tomada de decisão	5. / 5.1.1. / 5.1.2. / 6.1. / 6.1.2. / 6.1.5. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x					x	x	x	x	x	x		Conformidade de TI com as políticas internas	6.1. / 6.1.2. / 6.1.5. / 7. / 7.1.1. / 7.1. / 7.1.2. / 7.2. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.
x	x					x	x			x	x		Equipes de TI e negócios motivadas	6.1. / 6.1.2. / 6.1.5. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1.
x	x	x	x	x		x	x		x	x	x		Conhecimento, expertise e iniciativas para inovação dos negócios	6.1. / 6.1.2. / 6.1.5. / 12.1.2. / 13. / 13.1. / 13.1.2. / 14. / 14.1.1. / 15.2. / 15.2.1. / 15.2.2.

- Mapeamento domínio BAI (Tabela 2), consiste em analisar todos os processos e objetivos de T.I. contidos no domínio BAI e demonstrar o relacionamento existente de cada processo e objetivo com o código de práticas para controles de segurança da informação ABNT NBR ISO/IEC 27002:2013. O domínio é composto por 10 processos (BAI01 - Gerenciar Programas e Projetos, BAI02 - Gerenciar Definição de Requisitos, BAI03 - Gerenciar Identificação e Desenvolvimento de Soluções, BAI04 - Gerenciar Disponibilidade e Capacidade, BAI05 - Gerenciar Capacidade de Mudança Organizacional, BAI06 - Gerenciar Mudanças, BAI07 - Gerenciar Aceitação e Transição da Mudança, BAI08 - Gerenciar Conhecimento, BAI09 - Gerenciar Ativos, BAI10 - Gerenciar Configuração):

Tabela 2. Mapeamento domínio BAI.

COBIT 5										ABNT ISO/IEC 27002:2013
BAI01	BAI02	BAI03	BAI04	BAI05	BAI06	BAI07	BAI08	BAI09	BAI10	Objetivos de T.I.	Código de Prática e Controle de Segurança de Informação
X	X	X		X			X		X	Alinhamento da estratégia de TI e negocios	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 7.2.2. / 11. / 11.2.3. / 11.2.4. / 11.2.6. / 14. / 14.1.
	X							X	X	Conformidade de TI e apoio para conformidade de negócio com leis e regulamentos externos	14.1.1. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 11. / 11.2.3. / 11.2.4. / 11.2.6. / 14. / 14.1.
X	X			X	X					Compromisso da gerencia executiva com a tomada de decisão de TI	6.1.5. / 14.1.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 14. / 14.1.
X	X	X	X		X	X		X	X	Gestão de risco organizacional de TI	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 17.2.1. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 14. / 14.1.
X	X	X	X	X	X	X	X			Beneficios obtidos pelo investimento de TI e portifólio de serviços	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 12.1.2. / 7.2.2. / 14. / 14.1.
X								X	X	Transparência dos custos, beneficios e riscos de TI	6.1.5. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 11. / 11.2.3. / 11.2.4. / 11.2.6.
X	X	X	X	X	X	X	X	X		Prestação de serviços de TI em consonância com os requisitos de negócio	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 17.2.1. / 12.1.2. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 7.2.2. / 14. / 14.1.
X	X	X	X	X	X	X	X		X	Uso adequado de aplicativos, informações e soluções tecnologicas	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. 12.1.3. / 17.2.1. / 12.1.2. 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 7.2.2. / 11. / 11.2.3. 11.2.4. / 11.2.6. / 14. / 14.1.
	X		X	X	X	X	X	X	X	Agilidade de TI	14.1.1. / 12.1.3. / 17.2.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 11. / 11.2.3. / 11.2.4. / 11.2.6. / 14. / 14.1.
	X				X		X	X	X	Segurança da informação, infraestrutura de processamento e aplicativos.	14.1.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 7.2.2. / 11. / 11.2.3. / 11.2.4. / 11.2.6. / 14. / 14.1.
X	X	X	X	X	X		X	X	X	Otimização de ativos, recursos e capacidades de TI	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 17.2.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 7.2.2. / 11. / 11.2.3. / 11.2.4. / 11.2.6. / 14. / 14.1.
	X	X		X	X	X				Capacitação e apoio aos processos de negócio atraves da integração de aplicativos e tecnologia nos processos de negócio	14.1.1. / 14.2.5. / 14.2.6. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 14. / 14.1.
X	X	X	X	X	X	X				Entrega de programas fornecendo beneficios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 17.2.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 14. / 14.1.
	X	X	X		X	X	X	X	X	Disponibilidade de informações uteis e confiaveis para tomada de decisão	14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 17.2.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 7.2.2. / 11. / 11.2.3. / 11.2.4. / 11.2.6. / 14. / 14.1.

					X	X		X	X	Conformidade de TI com as políticas internas	12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 8. / 8.1. / 8.1.1. / 8.1.2. / 8.1.3. / 8.1.4. / 8.2.3. / 11. / 11.2.3. / 11.2.4. / 11.2.6.
X							X			Equipes de TI e negócios motivadas	6.1.5. / 7.2.2.
X	X	X	X	X	X	X	X			Conhecimento, expertise e iniciativas para inovação dos negócios	6.1.5. / 14.1.1. / 14.2.5. / 14.2.6. / 12.1.3. / 17.2.1. / 12.1.2. / 7.3. / 7.3.1. / 14.2.2. / 14.2.3. / 7.2.2. / 14. / 14.1.

- Mapeamento domínio DSS (Tabela 3), consiste em analisar todos os processos e objetivos de T.I. contidos no domínio DSS e demonstrar o relacionamento existente de cada processo e objetivo com o código de práticas para controles de segurança da informação ABNT NBR ISO/IEC 27002:2013. O domínio é composto por 6 processos (DSS01 - Gerenciar Operações, DSS02 - Gerenciar Solicitações e Incidentes de Serviços, DSS03 - Gerenciar Problemas, DSS04 - Gerenciar Continuidade, DSS05 - Gerenciar Serviços de Segurança, DSS06 - Gerenciar Controles de Processos de Negócio):

Tabela 3. Mapeamento domínio DSS.

COBIT 5							**ABNT ISO/IEC 27002:2013**
DSS01	**DSS02**	**DSS03**	**DSS04**	**DSS05**	**DSS06**	**Objetivos de T.I.**	**Código de Prática e Controle de Segurança de Informação**
			x	x		Alinhamento da estratégia de TI e negocios	17. / 5.
x		x	x	x	x	Conformidade de TI e apoio para conformidade de negócio com leis e regulamentos externos	12. / 17. / 5. / 9.1.
						Compromisso da gerencia executiva com a tomada de decisão de TI	
x	x	x	x	x	x	Gestão de risco organizacional de TI	12. / 16. / 17. / 5. / 9.1.
x		x	x			Beneficios obtidos pelo investimento de TI e portifólio de serviços	12. / 17.
						Transparência dos custos, beneficios e riscos de TI	
x	x	x	x	x	x	Prestação de serviços de TI em consonância com os requisitos de negócio	12. / 16. / 17. / 5. / 9.1.
x	x	x	x	x	x	Uso adequado de aplicativos, informações e soluções tecnologicas	12. / 16. / 17. / 5. / 9.1.
x		x	x			Agilidade de TI	12. / 17.
x	x		x	x	x	Segurança da informação, infraestrutura de processamento e aplicativos.	12. / 16. / 17. / 5. / 9.1.
x		x	x	x	x	Otimização de ativos, recursos e capacidades de TI	12. / 17. / 5. / 9.1.
		x	x	x	x	Capacitação e apoio aos processos de negócio atraves da integração de aplicativos e tecnologia nos processos de negócio	17. / 5. / 9.1.
						Entrega de programas fornecendo beneficios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	
x	x	x	x	x	x	Disponibilidade de informações uteis e confiaveis para tomada de decisão	12. / 16. / 17. / 5. / 9.1.
x	x	x	x	x	x	Conformidade de TI com as políticas internas	12. / 16. / 17. / 5. / 9.1.
x			x	x	x	Equipes de TI e negócios motivadas	12. / 5. / 9.1.
x	x	x	x	x	x	Conhecimento, expertise e iniciativas para inovação dos negócios	12. / 16. / 17. / 5. / 9.1.

- Mapeamento domínio MEA (Tabela 4), consiste em analisar todos os processos e objetivos de T.I. contidos no domínio MEA e demonstrar o relacionamento existente de cada processo e objetivo com o código de práticas para controles de segurança da informação ABNT NBR ISO/IEC 27002:2013. O domínio é composto por 3 processos (MEA01 – Desempenho e Conformidade, MEA02 - Sistema de Controle Interno, MEA03 - Conformidade com Requisitos Externos):

Tabela 4. Mapeamento domínio MEA.

COBIT 5				ABNT ISO/IEC 27002:2013
MEA01	MEA02	MEA03	Objetivos de T.I.	Código de Prática e Controle de Segurança de Informação
x			Alinhamento da estratégia de TI e negocios	18. / 18.2.3.
x	x	x	Conformidade de TI e apoio para conformidade de negócio com leis e regulamentos externos	18. / 18.2.3. / 5. / 6.1.
x			Compromisso da gerencia executiva com a tomada de decisão de TI	18. / 18.2.3.
x	x	x	Gestão de risco organizacional de TI	18. / 18.2.3. / 5. / 6.1.
x		x	Beneficios obtidos pelo investimento de TI e portifólio de serviços	18. / 18.2.3.
x	x		Transparência dos custos, beneficios e riscos de TI	18. / 18.2.3. / 5. / 6.1.
x	x	x	Prestação de serviços de TI em consonância com os requisitos de negócio	18. / 18.2.3. / 5. / 6.1.
x	x		Uso adequado de aplicativos, informações e soluções tecnologicas	18. / 18.2.3. / 5. / 6.1.
x			Agilidade de TI	18. / 18.2.3.
x	x	x	Segurança da informação, infraestrutura de processamento e aplicativos.	18. / 18.2.3. / 5. / 6.1.
x			Otimização de ativos, recursos e capacidades de TI	18. / 18.2.3.
			Capacitação e apoio aos processos de negócio atraves da integração de aplicativos e tecnologia nos processos de negócio	
x			Entrega de programas fornecendo beneficios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	18. / 18.2.3.
x	x		Disponibilidade de informações uteis e confiaveis para tomada de decisão	18. / 18.2.3. / 5. / 6.1.
x	x	x	Conformidade de TI com as políticas internas	18. / 18.2.3. / 5. / 6.1.
x			Equipes de TI e negócios motivadas	18. / 18.2.3.
x	x	x	Conhecimento, expertise e iniciativas para inovação dos negócios	18. / 18.2.3. / 5. / 6.1.

A norma ABNT NBR ISO/IEC 27002:2013 apresenta 14 seções de controles de segurança da informação de um total de 35 objetivos de controles e 114 controles, totalizando 163 processos.

Através da análise, foram mapeados os códigos de práticas para controles de segurança da informação da ABNT NBR ISO/IEC 27002:2013, que são aderidos em uma ou mais área(s) de domínio do Cobit 5 (Tabela 5).

Tabela 5. Mapeamento descritivo de códigos de práticas para controles de segurança da informação ABNT NBR ISO/IEC 27002:2013 associados ao Cobit 5.

ABNT NBR ISO/IEC 27002:2013	COBIT 5
5. Políticas de segurança da informação	APO, DSS, MEA, BAI
5.1.1. Políticas para segurança de informação	APO
5.1.2. Análise crítica das políticas para segurança da informação	APO
6.1. Organização interna	APO, MEA
6.1.2. Segregação de funções	APO
6.1.5. Segurança da informação no gerenciamento de projetos	APO, BAI
7. Segurança em recursos humanos	APO
7.1. Antes da contratação	APO
7.1.1. Seleção	APO
7.1.2. Termos e condições de contratação	APO
7.2. Durante a contratação	APO
7.2.2. Conscientização, educação e treinamento em segurança da informação	BAI
7.3. Encerramento e mudança da contratação	BAI
7.3.1. Responsabilidades pelo encerramento ou mudança da contratação	BAI
8. Gestão de ativos	BAI
8.1. Responsabilidade pelos ativos	BAI
8.1.1. Inventário dos ativos	BAI
8.1.2. Proprietário dos ativos	BAI
8.1.3. Uso aceitável dos ativos	BAI
8.1.4. Devolução dos ativos	BAI
8.2.3. Tratamento dos ativos	BAI
9.1. Requisitos do negócio para controle de acesso	DSS
11. Segurança física e do ambiente	APO, BAI
11.2.3. Segurança do cabeamento	APO, BAI
11.2.4. Manutenção dos equipamentos	APO, BAI
11.2.6. Segurança de equipamentos e ativos fora das dependências da organização	APO, BAI
12. Segurança nas operações	DSS
12.1.2. Gestão de mudanças	APO, BAI
12.1.3. Gestão de capacidade	BAI
13. Segurança nas comunicações	APO
13.1. Gerenciamento da segurança em redes	APO
13.1.2. Segurança dos serviços de rede	APO
14. Aquisição, desenvolvimento e manutenção de sistemas	APO, BAI
14.1. Requisitos de segurança de sistemas de informação	BAI
14.1.1. Analise e especificação dos requisitos de segurança da informação	APO, BAI
14.2.2 Procedimentos para controle de mudanças de sistema	BAI
14.2.3. Análise crítica técnica das aplicações após mudanças na plataforma operacional	BAI
142.5. Princípios para projetar sistemas seguros	BAI
14.2.6. Ambiente seguro para desenvolvimento	BAI
15.2. Gerenciamento da entrega do serviço do fornecedor	APO
15.2.1. Monitoramento e analise critica de serviços com fornecedor	APO
15.2.2. Gerenciamento de mudanças para serviços com fornecedor	APO
16. Gestão de incidentes de segurança da informação	DSS
17. Aspectos da segurança da informação na gestão da continuidade do negócio	DSS
17.2.1. disponibilidade dos recursos de processamento da informação	BAI
18. Conformidade	MEA
18.2.3 Análise crítica da conformidade técnica	MEA

A tabela pode ser visualizada na íntegra na própria norma ABNT NBR ISO/IEC 27002:2013.

Através da análise do mapeamento foi constatado que dos 163 processos apresentados na norma de segurança de informação ABNT NBR ISO/IEC 27002:2013, apenas 47 processos são abordados no Cobit 5, o que representa um total de 29% de aderência dos processos da ABNT NBR ISO/IEC 27002:2013 em relação às áreas de domínio do Cobit 5, no entanto os processos que não são abordados foram considerados relevantes ao *framework* Cobit 5, por serem processos inerentes ao ambiente, controle de acesso, orientação e utilização de dispositivos.

O capítulo seguinte apresenta a conclusão e as considerações finais deste artigo.

4. Conclusão

O objetivo deste artigo foi apresentar uma análise capaz de demonstrar a aderência do *framework* Cobit 5 em relação a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013, última versão da norma disponibilizada pela Associação Brasileira de Normas Técnicas - ABNT.

Para o desenvolvimento da análise foram mapeados as áreas de domínios do Cobit 5 em relação aos códigos de práticas para controles de segurança da informação descritos na norma ABNT NBR ISO/IEC 27002:2013 estabelecendo um guia comparativo dos domínios e processos abordados.

O artigo apresentou conceitos referentes à governança corporativa, governança de T.I., *Framework* Cobit 5, norma de segurança da informação ABNT NBR ISO/IEC 27002:2013 e por fim, a análise de aderência do Cobit 5 em relação aos processos de segurança de informação.

Através da análise elaborada foi concluído que a ABNT NBR ISO/IEC 27002:2013 apresenta 14 seções de controles de segurança da informação de um total de 35 objetivos de controles e 114 controles, totalizando 163 processos, no mapeamento foi constatado que desses 163 processos apenas 47 processos são abordados no Cobit 5.

Por fim concluiu-se que apenas 29% dos processos do Cobit 5 são abordados na ABNT NBR ISO/IEC 27002:2013, no entanto os processos que não são abordados foram considerados relevantes ao *framework* Cobit 5, por serem processos inerentes ao ambiente, controle de acesso, orientação e utilização de dispositivos.

É possível simplificar a implementação prática do *framework* Cobit 5 em conjunto com a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013, obtendo um ganho de tempo, custo e evitando a duplicidade na implantação de processos.

O mapeamento foi suficiente para atingir o objetivo.

A contribuição mais importante foi apresentar a intersecção d*o framework* Cobit 5 em relação a norma de segurança da informação ABNT NBR ISO/IEC 27002:2013, ressaltando os principais processos de segurança da informação baseados nos objetivos de T.I., e também evidenciar os processos que estão fora da intersecção, demonstrando se os mesmos são relevantes ao *framework* Cobit 5.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013**, 2013. Disponível em: < http://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 04 mar. 2015.

ISACA - INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. **Cobit 5**, 2012. Disponível em: < http://www.isaca.org/portuguese/Pages/default.aspx>. Acesso em: 04 mar. 2015.

IBGC - INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Disponível em: < http://www.ibgc.org.br/inter.php?id=18161>. Acesso em: 29 mar. 2015.

WEILL, P.; ROSS, J. W. **Governança de TI Tecnologia da Informação**. São Paulo: M.Books, 2006.

ISACA. INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. **Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit: A Management Briefing From ITGI and OGC**, 2008. Disponível em: < http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf>. Acesso em: 27 abr. 2015.

BARBOSA, Andressa Munhoz; BARBOSA, Sonia Rosangela E.; BATISTONI, Vander; LIMA, Valter Belo de; MATA, Joana Rodrigues da; MELO, Izabellitta Ap.; TAMAE, Rodrigo. **Governança em TI: Cobit; Itil.** São Paulo: FAEF, 2011.