ATLANTE
Cuadernos de Educación y Desarrollo (2ª Época)

Febrero 2018 - ISSN: 1989-4155

GOVERNANÇA DE TI: KEYCONTROL PROCESS

Douglas Dalapicola.

Analista de Sistemas (UNIANCHIETA).

Analista de Sistemas, Continental Automotive do Brasil.

Av. da Uva, 1585, Água Doce, Jundiaí - SP, CEP 13.213.235, 0xx11 4815-5893,

dalapicolad@gmail.com.

Juliano Schimiguel.

Professor no Centro Universitário Padre Anchieta,

na Universidade Cruzeiro do Sul, e na Universidade Nove de Julho.

schimiguel@gmail.com.

Para citar este artículo puede utilizar el siguiente formato:

Douglas Dalapicola y Juliano Schimiguel (2018): "Governança de TI: Keycontrol process.", Revista Atlante: Cuadernos de Educación y Desarrollo (febrero 2018). En línea:

https://www.eumed.net/2/rev/atlante/2018/02/keycontrol-process.html

RESUMO

O Objetivo deste trabalho éaplicar os conceitos da Governança de TI e COBIT para o gerenciamento e controle de processos dentro do âmbito corporativo de TI. A aplicação desses conceitos aliados ao Framework de COBIT e aos padrões estabelecidos nas auditorias SOX, afim de garantir a documentos e efetividade dos processos de TI dentro da Corporação.Efetuar o controle dos processos internos de TI para atendimento das Auditoria de TI, auditoria fiscais e corporativas dentro da corporação. Temos como resultados preliminares o controle de até 70% dos processos na primeira rodada de testes e controle efetuados após a elaboração dos controles internos, após esses resultados foram feitas rodadas de melhoria nos *GAPS* encontrados, e na segunda rodada de testes, os controles aqui apresentados obtiveram 100% de efetividade nos controles efetuados.

Palavras-Chave: Governança Corporativa, Governança de TI, SOX, COBIT, Documentação, Processos.

ABSTRACT

The goalof this work is to apply the concepts of IT Governance and CobiT to the management and control of processes within the corporate scope of IT. The application of these concepts allied to the COBIT Framework and the standards established in the SOX audits, in order to guarantee the documents and effectiveness of the IT processes within the Corporation.Make the control of internal IT processes to meet the IT Audit, tax and corporate audit within the corporation. We have as preliminary results the control of up to 70% of the processes in the first round of tests and control performed after the elaboration of the internal controls, after these results were made rounds of improvement in the GAPS found, and in the second round of tests, the controls presented here were 100% effective in the controls performed.

Keywords: Corporate Governance, IT Governance, SOX, COBIT, Documentation, Processes.

1.INTRODUÇÃO

Na atualidade, tem-se um cenário onde a Governança de TI e controle de processos torna-se vital para uma companhia, onde o controle de processos são definidos e seguidos para uma melhor qualidade na entrega dos serviços prestados por TI para a área de negócio da empresa. De acordo com Gil, Antônio de Loureira (1998), “Atuação em controle é a tarefa fundamental para a qualidade da segurança praticada em informática empresarial. Na realidade, o controle deve, além de apurar desvios,

isto é, apontar as diferenças entre planejamento e execução, buscando apresentar proposições a serem consideradas pelo planejamento e pela execução, para a definição de padrões exequíveis e para a melhoria/viabilização de alcance desses padrões, pela medição das execuções concretizadas".

A popularidade no estudo de Governança de TI: *KeyControl Process* atrela-se, em parte, ao interesse em um método para o controle e documentação de processo na Governança de TI, com a utilização do framework de COBIT(*Control Objectives for Information and Related Technology)* aplicadas em conjunto Lei Sarbanes-Oxley, Controles Internos.

Para a elaboração desse projeto, foram pesquisados e estudados livros, de autores como Aguinaldo Aragon Fernandes, Antônio de Loureiro Gil, WEILL, P.; ROSS, J. W, acerca da utilização de Governança de TI nas áreas de conhecimento e desenvolvimento de processos internos para TI, com a finalidade principal em controle e documentação dos processos internos de TI.

Este trabalho está organizado da seguinte maneira: Referencial teórico, uma descrição do contexto do estudo de caso; Referencial Teórico; Metodologia e Estudo de Caso; discussão dos resultados; considerações finais.

2. REFERENCIAL TEÓRICO

Governança Corporativa é o conjunto de processos, pessoas, hábitos, políticas, leis, instituições etc. os quais afetam o modo como uma corporação é dirigida, administrada ou controlada. Tal conceito inclui, também, os diversos relacionamentos existentes entre as várias partes interessadas[1]da empresa, bem como os objetivos em função dos quais a mesma é governada, acionistas, comitê diretor e a gerência são as principais partes interessadas, entretanto temos como parte interessada empregados, fornecedores, clientes, bancos e também governos e outras instituições regulatórias e a comunidade como um todo.

A Governança Corporativa fundamentou-se para criar um conjunto eficiente de mecanismos para assegurar que o comportamento dos executivos esteja sempre alinhado com os interesses dos acionistas, e também para evitar fraudes, erros estratégicos e abusos de poder. De acordo com o Instituto Brasileiro de Governança Corporativa IBGC(2009), a Governança Corporativa consiste "*no sistema pelo qual as sociedades são dirigidas, monitoradas e incentivadas, envolvendo o relacionamento entre proprietários, conselho de administração, diretoria e órgãos de controle interno. As boas práticas de governança corporativa convertem princípios em recomendações objetivas alinhando interesses com*

[1] Parte interessadas: tradução do Inglês *stakeholders*

a finalidade de preservar e otimizar os valores da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade".

Ainda de acordo com o IBCG, os princípios da Governança Corporativa, temos os seguintes pontos:

- Transparência: Obrigação e desejo de informar resultados e ações.
- Equidade: Tratamento igual para todos os acionistas.
- Prestação de Contas: Os agentes da governança corporativa prestam contas e são responsáveis pelos seus atos e omissões.
- Responsabilidade corporativa: Os agentes de governança devem zelar pela sustentabilidade das organizações, visando a sua longevidade incorporando considerações de ordem social e ambiental na definição dos negócios e operações.

A figura 2.1 apresenta de acordo com o IBGC, o sistema de governança corporativa.

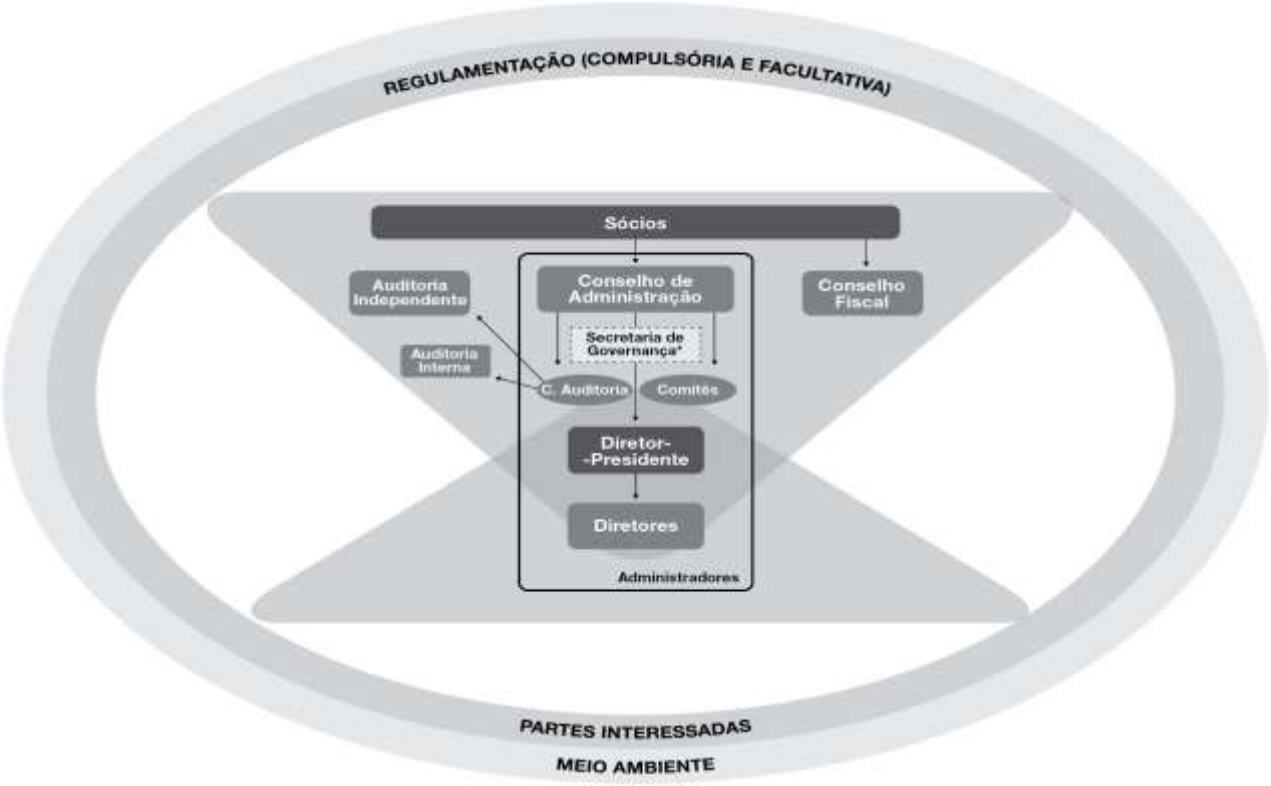

Figura 2.1 Sistema de Governança Corporativa

(http://www.ibgc.org.br/index.php/governanca/governanca-corporativa/sistema)

A empresa que opta pelo caminho dessas boas práticas adota como linhas mestras a transparência, a constante prestação de contas e a equidade. Para que essa tríade esteja presente, é preciso que o Conselho de Administração, que representa os acionistas e cotistas (proprietários do

capital), estabeleça estratégias para a empresa, eleja responsavelmente a Diretoria, fiscalize e avalie o desempenho da gestão e escolha apropriadamente a auditoria independente.

A governança de TI pode ser definida como “a especificação dos direitos decisórios e do *framework*de responsabilidade para estimular comportamentos desejáveis na utilização da TI” (WEILL, P; ROSS, J. W, Makron Books, 2006).

“Governança de TI é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, dar suporte às decisões e consequentemente alinhar TI aos negócios” (FGV Sr. João R. Peres).

De acordo com o *IT Governance Institute* (2007b), “a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e os objetivos da organização”.

Analisando essas definições, podemos concluir que a governança de TI, busca o direcionamento da TI para atender ao negócio e o monitoramento para verificar a conformidade com o direcionamento tomado pela administração da organização. Portanto a Governança de TI não é somente a implantação de modelos de melhores práticas, tais como CobiT, ITIL, CMMI, etc.

Ainda dentro dessa ótica, a Governança de TI, deve:

- Promover o alinhamento da TI ao negócio (suas estratégias e objetivos), tanto no que diz respeito a aplicações como à infraestrutura de serviços de TI.
- Promover a implantação de mecanismos que garantam a continuidade do negócio contra interrupções e falhas (manter e gerir as aplicações e a infraestrutura de serviços).
- Promover, juntamente com áreas de controle interno, *compliance* e gestão de riscos, o alinhamento da TI a marcos de regulação externos como a Sarbanes-Oxley(empresas que possuem ações ou títulos, papéis sendo negociados em bolsas de valores norte-americanas), e outras normas.

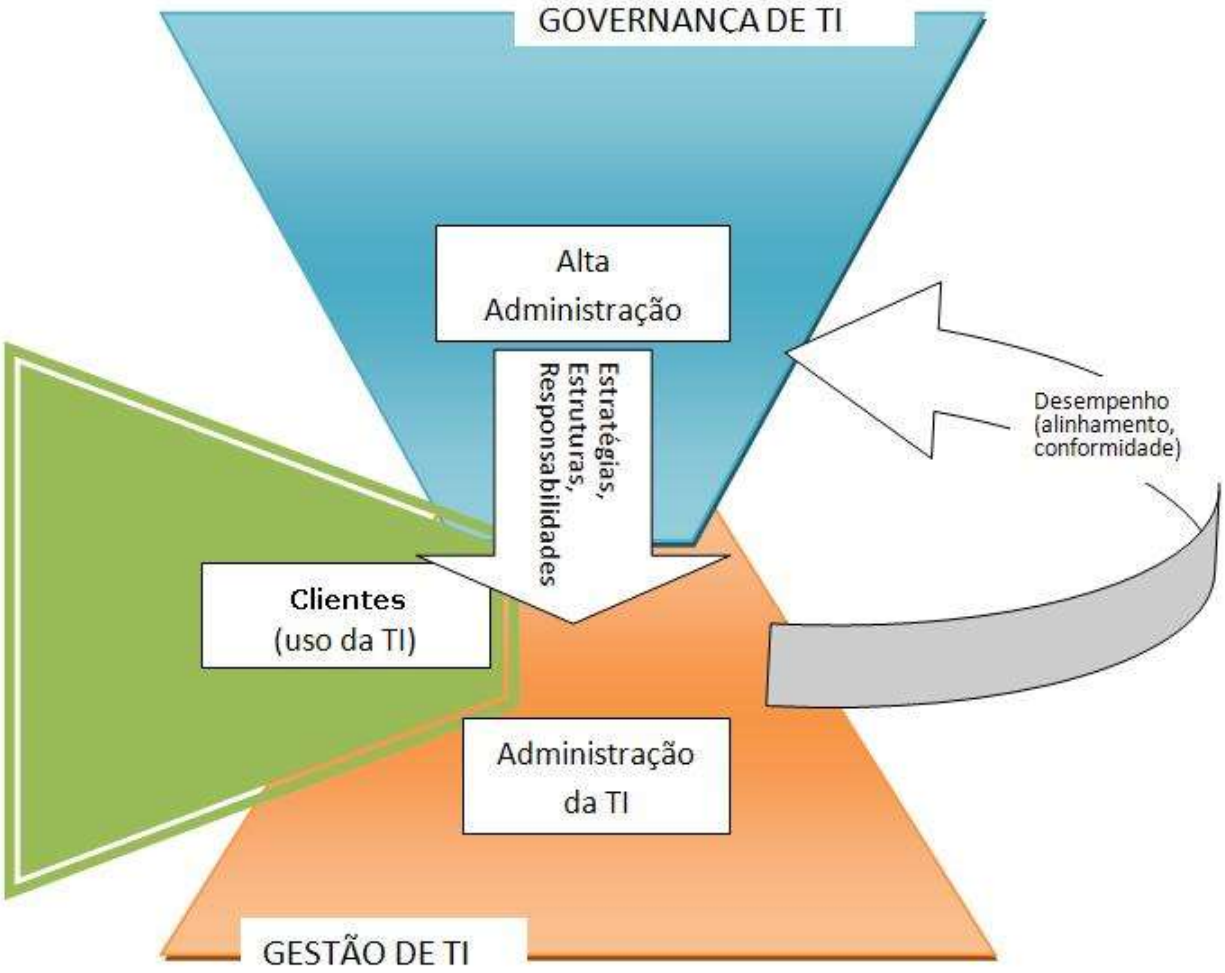

Figura 2.2 Governança de TI – Ciclo de estratégia e Decisão

(http://portal.tcu.gov.br/comunidades/governanca-de-ti/entendendo-a-governanca-de-ti/)

A governança de TI pode ser representada pelo que chamados de **"Ciclo da Governança de TI"**.

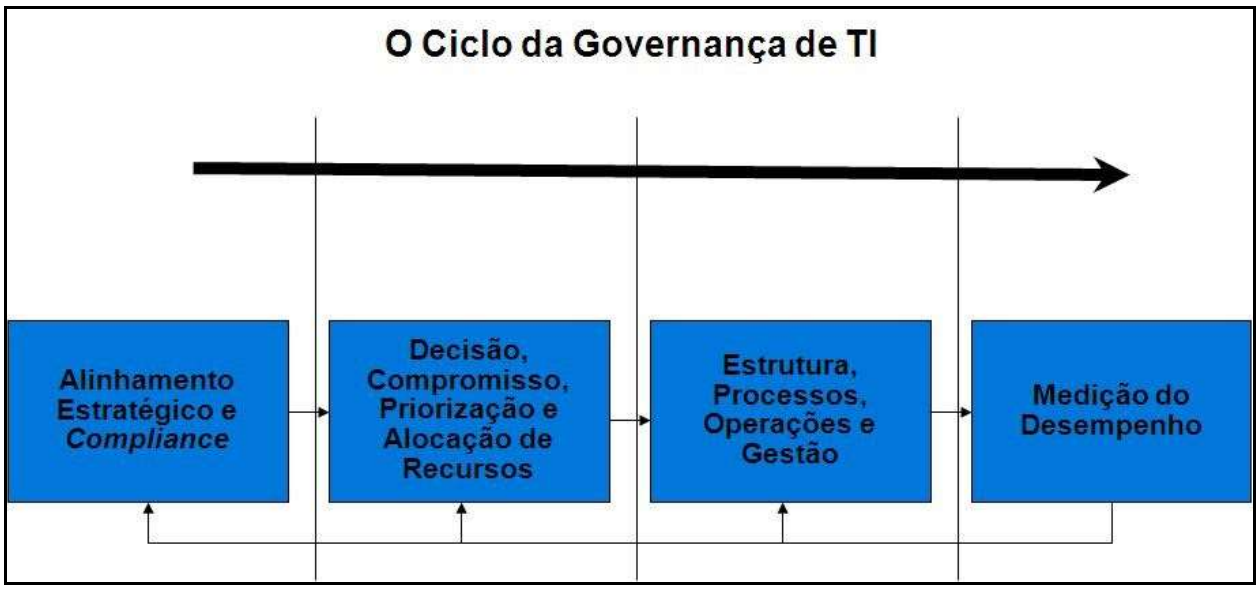

Figura 2.3 O Ciclo da Governança de TI (http://inovaemgestao.blogspot.com.br/2009/12/ciclo-de-governanca-de-ti.html)

O alinhamento estratégico e *compliance*refere-se ao planejamento estratégico da tecnologia da informação, que leva em consideração as estratégias da empresa para seus vários produtos e segmentos de atuação, assim como os requisitos de *compliance* externos, tais como *Sarbanes-Oxley act* e o Acordo da Basiléia.

A etapa de decisão, compromisso, priorização e alocação de recursos refere-se às responsabilidades pelas decisões relativas à TI em termos de: Arquitetura de TI, serviços de infraestrutura, investimentos, necessidade de aplicações, etc., assim como à definição dos mecanismos de decisão, ou seja, em que fóruns da empresa são tomadas essas decisões.

A etapa de estrutura, processos, operações e gestão refere-se à estrutura organizacional e funcional de TI, aos processos de gestão e operação dos produtos e serviços de TI, alinhados com as necessidades estratégicas e operacionais, infraestrutura, suporte técnico, segurança da informação, governança de TI e outras funções auxiliares ao CIO etc.

A etapa de gestão do valor e do desempenho**,** refere-se à determinação coleta e geração de indicadores de resultados dos processos, produtos e serviços de TI, à sua contribuição para estratégias e os objetivos do negócio e à demonstração do valor da TI para o negócio.

A lei Sarbanes-Oxley, SOX como é conhecida no mundo dos negócios, foi criada após uma série de escândalos financeiros que aconteceram em companhias de capital aberto no Estados Unidos, que minaram a confiança dos investidores no mercado de capital americano. Os principais objetivos dessa lei

é proteger os investidores do mercado de ações Americano de fraudes contábeis e financeiras de companhias abertas, assim como instituir uma sério de penalidades contra crimes relacionados, seu foco é os controles internos sobre relatórios financeiros.

Em TI, temos um grande impacto, pois todos os processos da empresa estão ligados diretamente a software que são desenvolvidos ou mantidos pela estrutura de TI da companhia, com isso a Governança de TI, acaba sendo impactada em alguns aspectos, como: Novos Controles em aplicações legadas devem ser implantadas, Novas aplicações, processos existentes em TI devem ser ajustados e melhorados para mitigar os riscos, novos processos de TI devem ser implantados e projetados, alteração da estrutura organizacional de TI, e os riscos devem ser monitorados constantemente.

O CobiT (*Control Objectives for Information and Related Technology)* foi criado em 1994 pela ISACF a partir do seu conjunto inicial de objetivos de controle e vem evoluindo através da incorporação de padrões internacionais técnicos, profissionais e específicos para processos de TI. O modelo de CobiT é genérico, com isso pode representa todos os processos normalmente encontrado nas funções de TI e decifrável tanto para a operação como para os gerentes de negócios, pois cria uma ponte entre o que a pessoal operação precisa executar e a visão dos executivos necessitam para “Governar”.

O CobiT concentra seu foco na Governança, no gerenciamento da informação e da tecnologia relacionadas onde quer que elas estejam, cobrindo a empresa de ponta-a-ponta. No CobiT 5, possuímos cinco domínios de processos:

- Governança (Avaliar, Dirigir e Monitorar);
- Alinhar, Planejar e Organizar;
- Construir, Adquirir e Implementar;
- Entregar, Reparar e Suportar;
- Monitorar, Avaliar e Medir.

E juntos esses domínios possuem 37 processos de TI, conforme abaixo.

	Processos de TI
EDM (Avaliar, Dirigir e Monitorar	- EDM01 -> Assegurar o estabelecimento e a manutenção do framework de Governança - EDM02 -> Assegurar a entrega dos benefícios - EDM03 -> Assegurar a otimização dos riscos - EDM04 -> Assegurar a otimização dos recursos - EDM05 -> Assegurar a transparência para as partes interessadas

APO (Alinhar, Planejar e Organizar	- APO01 -> Gerenciar o framework de gestão de TI - APO02 -> Gerenciar a estratégia - APO03 -> Gerenciar a arquitetura corporativa - APO04 -> Gerenciar a inovação - APO05 -> Gerenciar o portfólio - APO06 -> Gerenciar orçamento e custos - APO07 -> Gerenciar recursos humanos - APO08 -> Gerenciar relacionamentos - APO09 -> Gerenciar acordos de serviço - APO10 -> Gerenciar fornecedores - APO11 -> Gerenciar a qualidade - APO12 -> Gerenciar riscos - APO13 -> Gerenciar a segurança
BAI (Construir, Adquirir e Implementar)	- BAI01 -> Gerenciar programas e projetos - BAI02 -> Gerenciar a definição de requisitos - BAI03 -> Gerenciar a identificação e a construção de soluções - BAI04 -> Gerenciar disponibilidade e capacidade - BAI05 -> Gerenciar a habilitação da mudança organizacional - BAI06 -> Gerenciar mudanças - BAI07 -> Gerenciar o aceite e a transição das mudanças - BAI08 -> Gerenciar o conhecimento - BAI08 -> Gerenciar ativos - BAI10 -> Gerenciar a configuração
DSS (Entregar, Reparar e Suportar)	- DSS01 -> Gerenciar operações - DSS02 -> Gerenciar requisições de serviços e incidentes - DSS03 -> Gerenciar problemas - DSS04 -> Gerenciar a continuidade - DSS05 -> Gerenciar os serviços de segurança - DSS06 -> Gerenciar controles de processos de negócios
MEA (Monitorar, Avaliar e Medir)	- MEA01 -> Monitorar, avaliar e medir o desempenho e a conformidade - MEA02 -> Monitorar, avaliar e medir o sistema de controle internos - MEA03 -> Monitorar, avaliar e medir a conformidade com requisitos externos

Tabela 1 – Processos dos domínios do CobiT adaptado do ISACA (2012a)

3. METODOLOGIA E ESTUDO DE CASO

Materiais e métodos

De modo a se alcançar, satisfatoriamente os objetivos propostos, procedeu-se uma ampla pesquisa descritiva, com maior ou menor profundidade, diversos livros e sítios da internet (listados na Referência Bibliográfica). Devido a própria natureza do problema envolvido, os esforços acabaram por se concentrar em duas obras principais, as quais, foram criteriosamente estudadas, a saber:

- Implantando a governança de TI: da estratégia à gestão dos processos e serviços (Fernandes**,** Aguinaldo Aragon: Brasport, 2014); e

- Governança de TI: Tecnologia da Informação (WEILL, P; ROSS, J. W,Makron Books, 2006)

Após a pesquisa inicial, iniciou-se uma análise para se criar uma matriz de Controles de Processos, baseando-se nas Leis *Sarbanes-Oxley* e o *Framework de CobiT,* no sentido de garantir que, a partir da utilização das metodologias e dos requisitos legais exigidos na Lei, todos os processos estariam devidamente aplicadas, controladas e acompanhadas conforme necessário.

Por fim, e uma vez estabelecida a correlação entre a Lei *Sarbanes-Oxley* e o *Frameworkde CobiT,* iniciou-se o processo para acriação de uma Matriz de Controle de Processos, essencial para o início dos controles individuais dos processos a serem controlados em TI.

Estudo de Caso

Inicialmente foi verificado que a Empresa necessitava de uma equalização dos processos dentro do departamento de Tecnologia da Informação (TI), visto que cada unidade da empresa possuía um processo diferente, e que em momentos de auditoria não se tinha um relatório único e padronizado, assim gerando altas demandas de tempo do time envolvido para efetuar a adequação dos relatórios em um formato único, o qual deveria ser entregue para que os processos fossem auditados.

Para esse estudo de caso, serão apresentados os modelos utilizados para a criação dos controles e relatório de auditoria, necessário para implantação no departamento de tecnologia da Informação (TI).

A Empresa

A empresa no qual está sendo realizado o estudo de caso, é uma empresa do ramo automotivo, onde atualmente conta com mais de 2000 (Dois Mil) funcionários e mais de 7 plantas, as quais possuem processos de controle de TI independentes.

A gestão de Tecnologia da Informação (TI) da empresa, é responsável por selecionar, controlar, documentar, compatibilizar necessidades e gerenciar a mudança de sistemas para a administração do negócio, onde são realizados os testes de viabilidade de novas soluções de forma inovadora, eficiente e de forma rentável para a corporação.

Documentação e padronização dos processos dentro de TI

A documentação e padronização dos processos, teve início na criação de uma Matriz de Controle Principal (*Master Control Matrix*) pelo time de Governança e Conformidades da Empresa *(Governance e Compliance)*, onde foram identificados todos os controles e para alguns controles fora feita uma consolidação, assim gerando 27 (vinte e sete) Pontos de Controle para o Departamento de Tecnologia da Informação (TI).

Abaixo o Fluxo de Controle para o Departamento de TI, note que todos os controles estão inter-relacionados entre si.

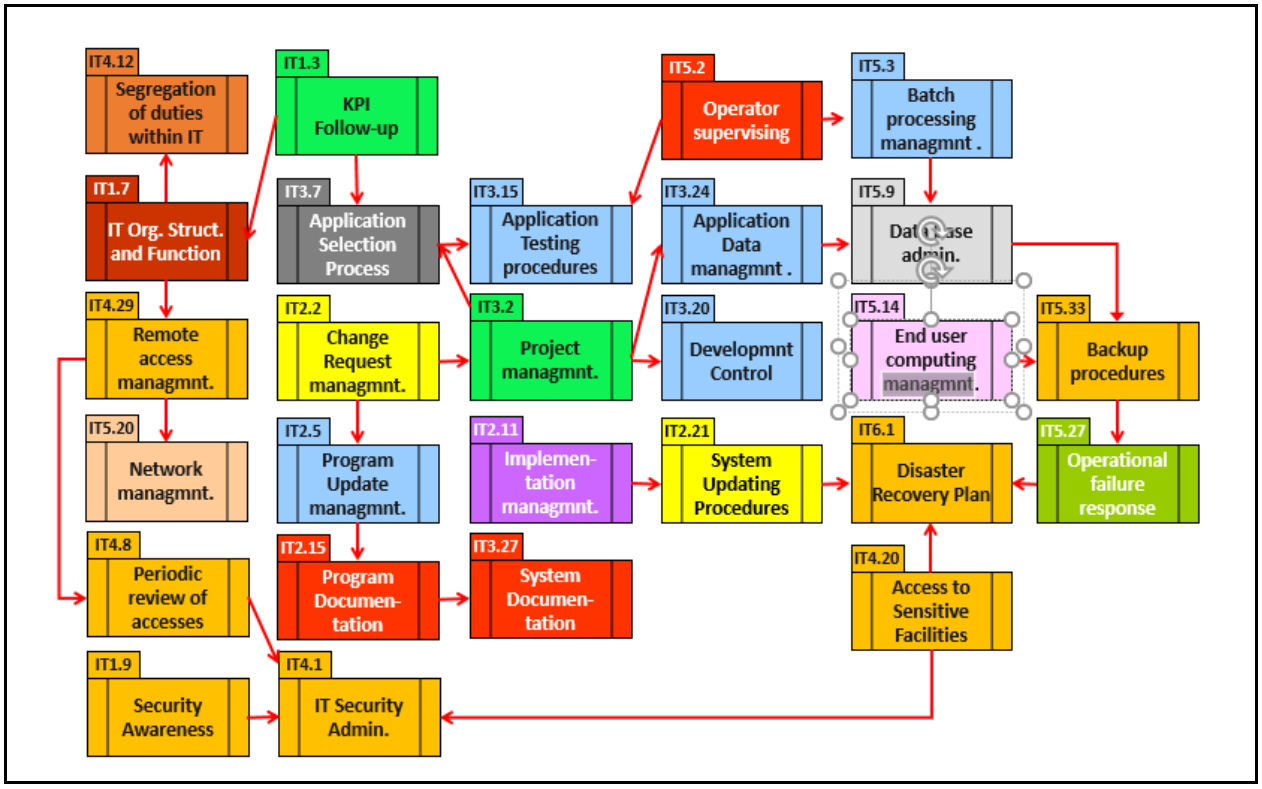

Figura 3.1 – Fluxo de Processos de Controle

Abaixo o Fluxo de trabalhodo projeto de Controle de Processo (KeyControl), demonstra ao Dono do Processo (Process Owner) como proceder para elaborar o controle de processo pelo qual é responsável.

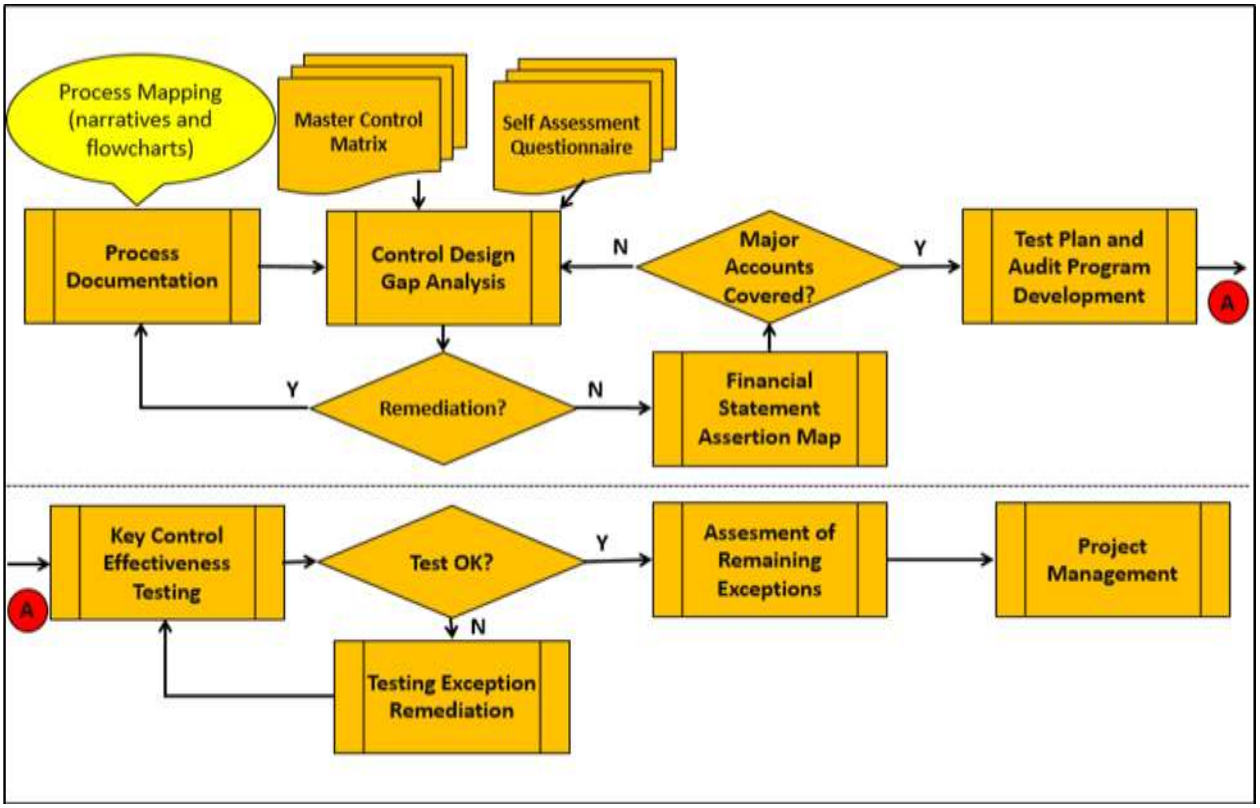

Figura 3.2 – Fluxo de Trabalho de criação do Controle

A Matriz de Controle foi elaborada contendo os seguintes pontos:

- Controle de Atividade (Activity Control)
- Assunto (Subject)
- Frequência que o processo ocorre *(Frequency)*
- Objetivo do Controle *(Control Objectives)*
- Tipo do Controle*(Type Control, "Completeness" "Accuracy" "Validity" "Restricted Access")*
- Controle do Risco *(Control Risks)*
- Ponto de Foco do Controle *(Point of Focus)*
- Dono do Processo *(Process Owner)*

A matriz de controle é somente uma referência para que o dono do processo (*Process Owner*), tenha uma referência (*Guideline*) para início da construção da documentação que deverá ser o controle de processo (*KeyControl*).

Matriz de Controle

Control Activity	Subject	Frequency	Control Objectives	Type	Control Risks	Points of Focus	Process Owner
IT2.5	Program Update Management	Ad-hoc	1) Only authorized and tested changes are accepted by the users in the live environment.	C,A	1) Exclusion of necessary IT functionality; Application of unauthorized changes after completed testing; Increased errors, bugs, and application down-time; Inappropriate support documentation; Simultaneous changes made to one piece of code, leading to lost efforts, loss of functionality, or even destruction of the application.	1.1) All mission critical implementations must be adequately tested by either running a parallel test, running a pilot project (or prototype), and/or by exhaustively testing all changed program logic to ensure the mission-critical system performs as expected prior to implementing into a production mode; 1.2) Ensure unauthorized changes made after the completion of testing but before staging in the live environment are prevented or detected; 1.3) Ensure that source code used corresponds to most recent version of program; 1.4) Ensure modifications to a program by more than one programmer are coordinated; 1.5) Program changes are appropriately tested by IT staff and users to ensure intended functionality in the live environment.	Douglas Dalapicola

IT3.15	ApplicationTesting procedures	Ad-hoc	1) There is segregation of duties between systems development and systems operations.	C,A,V	1) Increased bugs in application; Delay of application release; Undiscovered incompatibilities between application and live environment; Inappropriate/unauthorized and untested changes made to application; Delay in business operations.	1.1) Ensure appropriate testing is carried out by the IT staff and users to prevent or detect errors in program coding and ensure the application operates as intended in the live environment; 1.2) Ensure that appropriate levels of testing are applied after modifications are made subsequent to initial testing; 1.3) Ensure that unauthorized changes cannot be made after the completion of testing but before transfer into the live environment; 1.4) Any program modified or added to the applications systems environment must be tested using copies of real data or test data to verify the program functions as intended; 1.5) User departments should be included in the testing procedures to ensure the new system or changed program meets the user's functionality expectations.	Douglas Dalapicola
IT3.20	Development Control	Ad-hoc	1) There is segregation of duties between systems development and systems operations.	C,A,V	1) Unauthorized/inappropriate changes on the live application; Application failure; Loss of necessary application functionality; Lack of audit trail/no assignable responsibility for changes; Incongruent data processing and subsequent data corruption; Outdated application support.	1.1) A program "check-out" or similar procedure needs to exist to prevent the possibility that two different developers are making changes to the same production object at the same time. If this is not done, the risk exists that one person will overwrite the other's changes. If automated software is not used, manual compensating controls should exist to minimize the chance of overwriting changes; 1.2) Ensure that only properly tested, reviewed, and approved	Douglas Dalapicola

						changes are transferred into the live environment; 1.3) Ensure that, in the case of applications running in a multiple site environment, all copies of live programs are updated; 1.4) Ensure that, for program changes made-in house, source code used corresponds to the most recent version of the program .	
IT3.24	Application Data Management	Ad-hoc	1) There is segregation of duties between systems development and systems operations.	C,A,V,R	1) Data corruption; Loss of business critical data; Unauthorized/inappropriate access to data; Infringement on privacy; Unauthorized/inappropriate access to trade secrets; Missing data fields required by end-users for business function.	1.1) Ensure that appropriate testing of data is carried out by users and IT staff; 1.2) Review the process for establishment of data not used by the old application;	Douglas Dalapicola
IT5.3	Batch processing management	Ad-hoc	All data are completely and accurately processed to meet users needs	C,A,V	1) Lost data; Data corruption at batch process; Inappropriate/unauthorized batch processing; Missing batches; Lack of accountability; Inability to recover from disruption in business continuity.	1.1) Ensure that appropriate planning of batch processes takes place; 1.2) Ensure that all changes to batch processes are appropriate and authorized; 1.3) Ensure that departures from pre-approved schedules are identified and approved; 1.4) Ensure that data required for a batch process are available prior to running the batch; 1.5) Review and verify that the operation of batch processes is appropriately documented.	Douglas Dalapicola

Abaixo, estão apresentados os controles na seguinte estrutura, *KeyControl* (KC), Assunto (*Subject*), Dono do Processo (*Process Owner*), Departamento responsável e Área de aplicação do Processo (*Transaction*)

KC	Subject	Process Owner	Cycle	Transaction
IT2.5	Program Update Management	Douglas Dalapicola	IT	2 Change Management
IT3.15	ApplicationTesting procedures	Douglas Dalapicola	IT	3 Development and implementation
IT3.20	Development Control	Douglas Dalapicola	IT	3 Development and implementation
IT3.24	Application Data Management	Douglas Dalapicola	IT	3 Development and implementation
IT5.3	Batch processing management	Douglas Dalapicola	IT	5 Operations

Documentação e evidência da execução dos processos

Para cada item denominado Controle de Processo (*KeyControl*) foi criado um documento, onde foram documentados todos os processos já executados dentro do departamento, levando em consideração todos os diferentes processos que eram executados nas outras unidades da empresa, com isso foram unificados as melhores práticas e criado um único documento de controle para todo o departamento de Tecnologia da Informação independente da unidade de atuação do departamento. Com isso começamos a ter controle dos processos que o departamento estava fazendo, gerando um único processo, documentação de execução do processo e documentação das evidências de execução.

A seguir temos a estrutura do documento que será utilizado para a Documentação dos processos pelo Dono do Processo (*Process Owner*). Esse documento irá conter todas as etapas de controle daquele processo, bem como exceções ao processo (Pontos que fogem ao controle da Região de atuação ou caso o processo já tenha um controle externo), conterá o quais os tipos de documentação são exigidos para aquele controle, e todo o processo de testes daquele controle.

Key Control Description	ID:
Subject	
Control objective	

Responsible (function / department):

Control Type			
☑ Completeness	☑ Accuracy	☐ Validity	☐ Restricted Access

Control Category		*Control Method*	
☑ Preventive	☐ Detective	☐ Automated	☑ Manual

Frequency				
☐ Annually	☑ Monthly	☐ Fortnightly	☐ Daily	☑ Ad-Hoc

Control Activity Description	
ID	**Steps**
01	

Exceptions			
ID	**Business Case**	**Reason**	**Approval**
01			

Control Evidence	
ID	**Description of the evidence**
01	

Testing Procedures	
ID	**Steps**
01	

Após a construção da documentação do processo que o Controle *(KeyControl)* faz a cobertura, uma reunião com todos os envolvidos é executada, para que todos tenham conhecimento do processo e dos ajustes que foram feitos, para que todo o departamento siga esse novo fluxo do processo, inclusive é nessa reunião que é informada a data, em que esse processo se torna ativo, ou seja, a partir da data que foi estabelecida, fica como obrigatório a execução do novo processo, para que no processo de auditoria tenha-se a eficiência esperada no controle dos processos.

Auditoriados processos executados

Na etapa de auditoria dos Processos, foram definidos na empresa 4 trimestres de testes, denominados *Quarters*(Q1, Q2, Q3 e Q4). Nesse período de testes, não serão todos os Controles que deverão ser auditados, para avaliação levam-se em conta a frequência (*Frequency*) de cada controle, conforme apresentado na Matriz de Controle Principal (*Master Control Matrix*). Na primeira rodada de testes do 1º trimestre (Q1 – *Quarter* 1), todos os controles são testados sem exceções, para as outras rodadas, serão testados todos os controles que ocorrem eventualmente (*Ad-hoc*), diário (*Dialy*), quinzenal (*fortnightly*) e mensal (*Monthly*). Para os controles Anuais e Semestrais (quando aplicável), a rodada de testes é feita sempre no 4º trimestre (Q4 – *Quarter* 4).

Para a auditoria do processo, é seguido o procedimento de teste (*Test Procedure*) descrito em cada Descrição de Controle de Processo (*KeyControl Description*), solicitando todas as evidências, analisando se houve alguma divergência ou falha no processo de controle e apontado isso no relatório final dos testes.

Abaixo o modelo utilizado para auditoria dos processos, que conter a descrição e identificação do Processo que está sendo auditado, nome do dono do processo (*Process Owner*) e do testador, possui um campo para informar se houve alguma falha no processo de controle (Gap – falha que não tenha invalidado o teste), um campo para apontar se houve alguma falta de controle (*Missing Control*), conterá inda um campo para comentários gerais livre para o testador, campo para o conclusão final do teste (*Final Conclusion*), um campo para recomendações de melhoria do controle, e um campo para inclusão de todos os documentos recebidos para a validação do Processo (*Related WorkPapers – (WP*)).

Abaixo o modelo para teste de auditoria do Controle de Processo (*Key Control*)

Key Control Effectiveness Testing Result	ID:
Subject	Related period:
Process Owner	Tester

Gaps		*Missing Controls*	
☐ Yes	☐ No	☐ Yes	☐ No
Comments		Comments	

Segregation of Duties Issues ☐ Yes ☐ No
Comments

General Comments	
01	

Final Conclusion ☐ Effective ☐ Ineffective
Comments

Recommendations	
01	-

Related Work Papers (WP)	
01	
02	

Após a auditoria e a conclusão final, o relatório pode conter, Falha nos controles do processo (Gap), Falta de controle (Missing Control) e não menos importante, recomendações de melhorias do processo ou escrita para i, melhor entendimento do processo.

Em caso de falta de controle (Missing Control), o responsável pelo controle deverá efetuar os ajustes e adequar a documentação e o processo, conforme falta de controle encontrado. A avaliação e o teste, para garantir que esse ajuste no controle foi efetivo, deverá ser feita uma Auditoria não oficial para testes nesses ajustes, e aguardar a Auditoria oficial para do trimestre seguinte.

3.2DISCUSSÃO DE RESULTADOS

Ao fim da aplicação deste projeto, obtivemos como resultados preliminares na primeira rodada de testes um índice de 70% de aprovação nos controles de processos criados para na área de Tecnologia da Informação (TI), após essa rodada, foram analisados os *GAPS* e *MissingControls*, identificados durante a Auditoria, e com isso foram ajustados. Após esses ajustes, os controles que não foram aprovados na auditoria oficial, foram submetidos a testes internos no departamento de Tecnologia da Informação, afim de garantir que os controles agora estavam cobertos, nos pontos de falhas apresentados no relatório da Auditoria anterior, com isso, para a segunda rodada oficial de testes, obtivemos um total de 100% de aprovação nos controles internos de TI.

Os resultados encontrados no presente estudo, sugerem que após a implementação do Processo de Controle Chave no departamento de Ti da empresa, tivemos um melhor entendimento dos processos que deveriam ser feitos pelo departamento, assim tornando padrão os processos já existentes e adotando para todos o mesmo processo, diferente do que era feito anteriormente a esse projeto. A padronização e entendimento dos processos executados, não gerou grandes impactos no dia-a-dia dos colaboradores, pois inicialmente o levantamento foi de documentar o processo que já era executado, e posteriormente analisar se esses processos continham algum tipo de falta de controle. Após todas as análises concluídos, pode-se verificar que os alguns processos precisam de ajustes, e correções para melhor controle e documentação do processo que era feito, esses ajustes se tornaram um processo padrão dentro do departamento, tanto para os colaboradores atuais, como para os novos.

Obtivemos melhoria na gestão dos processos e na divisão das responsabilidades internas no departamento, tornando claro os responsáveis de cada etapa do processo, e acabando com os “jeitinhos” que antes eram utilizados. Não tivemos impacto em custos, pois esse trabalho foi um trabalho interno, que não demandou a contratação de uma consultoria para que fossem trabalhos os Processos internos, e toda a auditoria é um processo efetuados internamente com os colaboradores da empresa.

4.CONSIDERAÇÕES FINAIS

O Objetivo desse trabalho foi realizar um estudo para implantação de controle de processos para o departamento de TI, afim de garantir uma padronização dos processos no departamento, garantindo assim uma melhor prática para o trabalho exercido no departamento, único processo e uma similaridade nas evidências gerados pelo trabalho de cada um. A identificação de falhas no processo, mostrou nesse momento que esse projeto já seria um sucesso ao seu final, pois nos deu a visão que o departamento

tinha diversas maneiras de se fazer o mesmo processo, em cima disso, tivemos convicção de que poderíamos melhorar todos os processos analisando e comparando qual seria a melhor opção na padronização, e assim o foi, obtivemos ao final da análise, um melhor controle do processo e os resultados foram excelentes para as auditorias, pois as evidências necessárias de cada processo, estava centralizada em um único ponto, fazendo com que a auditoria se torna-se um processo com pouco estresse, algo que era impossível antes da padronização.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Adriana; ROSSETTI, Jose Paschoal, Governança corporativa: fundamentos, desenvolvimento e tendências. 4.ed. atual. eampl. São Paulo: Atlas, 2009.

Borgerth,Vania Maria da Costa: Sox - Entendendo a Lei Sarbanes–Oxley: ThomsonPioneira, 2007

Deloitte, SOX: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-aers-assur-ten-threats-sep2004.pdf

DIGITA: http://home.digita.com.br/novidades/2016/08/o-que-voce-deve-saber-sobre-governanca-de-ti-e-como-ela-pode-ajudar-a-sua-empresa/

FERNANDES, A. A.;; ABREU, V. F. de. Implantando a Governança de TI - da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

Fernandes, Aguinaldo Aragon: Implantando a governança de TI: da estratégia à gestão dos processos e serviços / Aguinaldo Aragon Fernandes, Vladimir Ferras de Abreu – 4 ed. – Rio de Janeiro: Brasport, 2014.

Gil,Antonio de Loureiro. Segurança da informática – 2. Ed. – São Paulo: Atlas 1998.

ISACA, COBIT: http://www.isaca.org/cobit/pages/default.aspx

Portal da Auditoria, SOX: https://portaldeauditoria.com.br/introducao-lei-sarbanes-oxley-sox

Prodanov,Cleber Cristiano. Metodologia do trabalho científico [recurso eletrônico] : métodos e técnicas da pesquisa e do trabalho acadêmico / Cleber Cristiano Prodanov, Ernani Cesar de Freitas. – 2. ed. – Novo Hamburgo: Feevale, 2013.

TCU, Governança de TI: http://portal.tcu.gov.br/comunidades/governanca-de-ti/entendendo-a-governanca-de-ti

U.S Securities and Exchange Commission, SOX:https://www.sec.gov/info/smallbus/404guide.pdf

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