



**INSTITUTO FEDERAL
SANTA CATARINA**

**CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DE TI**

Melissa da Silva Calixto

Análise da implantação da gestão de riscos na tecnologia da informação: um estudo de caso

**Florianópolis - SC
2020**

Ficha de identificação da obra elaborada pelo autor.

Calixto, Melissa da Silva

Análise da implantação da gestão de riscos na tecnologia da informação : um estudo de caso / Melissa da Silva Calixto ; orientação de Hamilcar Boing. - Florianópolis, SC, 2020.

56 p.

Trabalho de Conclusão de Curso (TCC) - Instituto Federal de Santa Catarina, Câmpus Florianópolis. CST em Gestão da Tecnologia da Informação. Departamento Acadêmico de Saúde e Serviços.
Inclui Referências.

1. COBIT. 2. ITIL. 3. Segurança da Informação. 4. Implantação de processo de gestão de riscos. I. Boing, Hamilcar. II. Instituto Federal de Santa Catarina. Departamento Acadêmico de Saúde e Serviços. III. Título.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS

CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

MELISSA DA SILVA CALIXTO

ANÁLISE DA IMPLANTAÇÃO DA GESTÃO DE RISCOS NA TECNOLOGIA DA INFORMAÇÃO: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Professor Orientador:

Hamilcar Boing

FLORIANÓPOLIS - SC

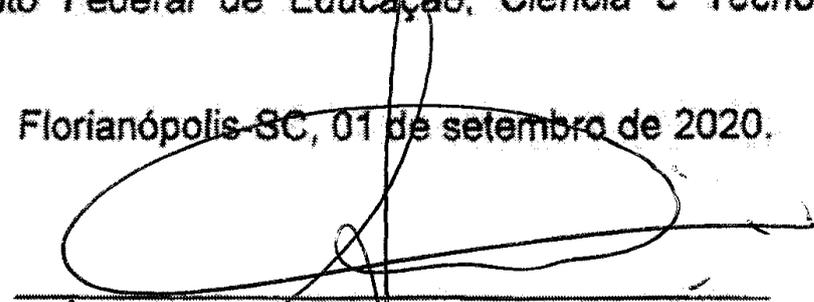
SETEMBRO/2020

**ANÁLISE DA IMPLANTAÇÃO DA GESTÃO DE RISCOS NA TECNOLOGIA DA
INFORMAÇÃO: UM ESTUDO DE CASO**

MELISSA DA SILVA CALIXTO

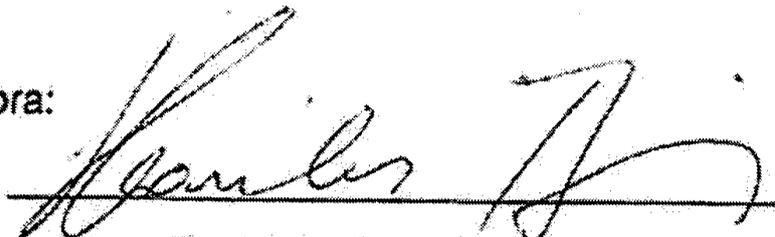
Este trabalho foi julgado adequado para obtenção do Título de Tecnólogo em Gestão da Tecnologia da Informação e aprovado na sua forma final pela banca examinadora do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis-SC, 01 de setembro de 2020.



Prof. Cleverson Tabajara Vianna
Coordenador do CST em Gestão da Tecnologia da Informação
Instituto Federal de Santa Catarina

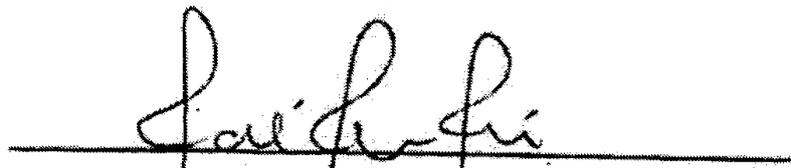
Banca Examinadora:



Prof. Hamilcar Boing, Dr

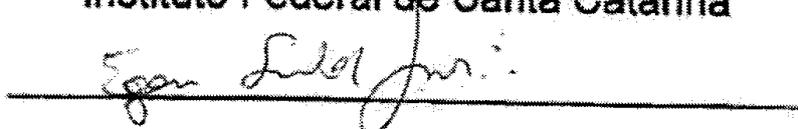
Orientador

Instituto Federal de Santa Catarina



Underléa Cabreira Correa, Dra

Instituto Federal de Santa Catarina



Egon Sewald Junior, Dr

Instituto Federal de Santa Catarina

RESUMO

A presente pesquisa analisou a implantação da gestão de riscos a partir de um estudo de caso em uma empresa de TI que utiliza o framework ITIL, adotando COBIT como base para sua implementação. A partir da participação nas reuniões do processo de implantação foi efetuada a coleta das informações sobre a implantação do processo de gestão de riscos, permitindo a análise com a literatura e gerando considerações que possam auxiliar gestores no processo de implantação do processo de gestão de riscos em outras empresas. Os resultados obtidos permitem identificar pontos positivos e dificuldades encontradas durante a implantação do processo de gestão de riscos, como por exemplo, o alto grau de organização da empresa, o perfil dos profissionais que conduziram a implantação, a dinâmica utilizada na condução das reuniões, a necessidade de agir preventivamente em relação aos riscos e mapear ações para os riscos residuais.

Palavras-chave: COBIT, ITIL, Segurança da Informação, Implantação de processo de gestão de riscos.

ABSTRACT

This research analyzed the implementation of risk management from a case study in an IT company that uses the ITIL framework, adopting COBIT as the basis for its implementation. From the participation in the meetings of the implementation process, information was collected on the implementation of the risk management process, allowing analysis with the literature and generating considerations that can assist managers in the process of implementing the risk management process in other companies. The results obtained allow the identification of positive points and difficulties encountered during the implementation of the risk management process, such as, for example, the high degree of organization of the company, the profile of the professionals who conducted the implementation, the dynamics used in conducting the meetings, the need to act preventively in relation to risks and map actions for residual risks.

Keywords: COBIT, ITIL, Information Security, Risk management Process Implementation.

Sumário

1.INTRODUÇÃO	8
2.JUSTIFICATIVA	9
2.1 Vínculo com o curso de GTI	10
3.DEFINIÇÃO DO PROBLEMA	11
4.OBJETIVOS	12
4.1 OBJETIVO GERAL	12
OBJETIVOS ESPECÍFICOS	13
5.REFERENCIAL TEÓRICO	13
5.1 Segurança da Informação	13
5.2 Riscos e Ameaças em Segurança da Informação	14
5.3 Gestão de Riscos em Segurança da Informação	15
5.3.1 Processo de avaliação de riscos	16
5.3.2 Tratamento e plano de resposta ao risco	17
5.3.2.1 Mitigar o risco	17
5.3.2.2 Evitar o risco	18
5.3.2.3 Aceitar o risco	18
5.3.2.4 Transferir o risco	18
5.3.2.5 Definir ações	18
5.3.2.6 Comunicação e Consulta	19
5.3.2.7 Monitoramento e Análise Crítica dos fatores de risco	20
5.3.2.8 Riscos residuais	20
5.4 Governança de TI	20
5.4.1 Information Technology Infrastructure Library (ITIL)	21
5.4.2 Control Objectives for Information and related Technology (COBIT)	23
5.4.2.1 Princípios do COBIT	23
5.4.2.2 Ciclo de vida da implantação do COBIT	25
6.PROCEDIMENTOS METODOLÓGICOS	26
6.1 Caracterização da pesquisa	27

6.2 Procedimentos aplicados	28
7. ESTUDO DE CASO	29
7.1 Descrição da Empresa	30
7.2 Mapa estratégico para implantação	30
7.3 Fase 1: Quais são os direcionadores?	31
7.3.1 Iniciar o programa	31
7.3.2 Estabelecer o desejo de mudança	31
7.4 Fase 2: Onde estamos agora?	31
7.4.1 Definir problemas e oportunidades	31
7.4.2 Avaliar riscos	32
7.4.3 Fatores críticos de sucesso da implementação	32
7.4.4 Cascata de Objetivos	33
7.4.5 Cascata de objetivos corporativos em objetivos TI	34
7.4.6 Formar equipe de implantação	36
7.5 Fase 3: Onde queremos estar?	36
7.5.1 Definir o guia de implementação	36
7.5.2 Atualização dos riscos cadastrados e modificação de status	39
7.5.3 Comunicar o resultado	40
7.6 Fase 4: O que precisa ser feito?	40
7.6.1 Planejar o programa	40
7.6.2 Identificar o papel das partes	42
7.6.3 Validação do processo de gestão de riscos	43
8. ANÁLISE DOS RESULTADOS	43
9. CONCLUSÕES	47
10. REFERÊNCIAS	49
11. APÊNDICES	52
APÊNDICE A - Item para registro do risco - RTC	52
APÊNDICE B – Modelo para levantamento de informações para o cadastro dos riscos	52
APÊNDICE C - Modelo de atualização de status do risco (individual)	52

APÊNDICE D - Modelo de atualização de status do risco	53
11.ANEXOS	53
ANEXO A - Probabilidade e Impacto do Risco	53
ANEXO B - Classificação do Risco	53
ANEXO C - Mapeamento dos objetivos corporativos do COBIT em perguntas sobre governança e gestão	54

1.INTRODUÇÃO

O crescente uso de tecnologias nas últimas décadas modificou o formato e o funcionamento dos processos das empresas, especialmente nas empresas de tecnologia. Por meio da utilização de dados em larga escala, foi obtida a agilidade na execução das tarefas que possibilitou a melhoria nas atividades entregues nos processos.

O cenário contextualizado anteriormente é denominado como Sociedade da Informação ou Sociedade do Conhecimento. A inserção do homem nesse novo paradigma da sociedade de geração do conhecimento contínuo requereu um grau maior de desempenho para efetuar suas atividades diárias devido à complexidade das informações (FERNANDES, 2013). Nessa sociedade, a informação nas organizações é um ativo essencial e de grande valor que deve ser protegido para garantir a continuidade dos negócios.

Com o crescimento do uso da tecnologia nas empresas, também cresceu a quantidade de ferramentas maléficas para extração de informações (CRUZ, 2017). Dessa forma, conhecer os possíveis riscos e ameaças que permeiam o ambiente corporativo é um dos itens essenciais para gerenciá-los e manter a perenidade dos ativos empresariais.

Nesse contexto, é essencial proteger as informações junto a Segurança da Informação (SI) que visa garantir a confidencialidade, integridade e disponibilidade das informações. E a partir disso, adotar metodologias de trabalho para gerenciar seus ativos (dados) e implantar estratégias para garantir a segurança desses dados, como por exemplo, a gestão de riscos.

Diante dessa realidade, a investigação se constitui em um estudo de caso que analisa a estruturação da implantação do processo de gestão de riscos em uma empresa de TI por meio de uma pesquisa de caráter descritivo, exploratório e

natureza bibliográfica, alicerçada nas melhores práticas por meio do *framework* ITIL e do COBIT visando obter maior segurança dos ativos por meio da prevenção e da gestão de riscos.

2.JUSTIFICATIVA

Com a potencialização do acesso à informação e ao conhecimento, as empresas começaram a atuar por processos, integrando os seus setores, melhorando a qualidade e o tempo de entrega dos serviços. Dessa forma, as informações da empresa estão em todos os dispositivos conectados à rede da empresa.

Nesse cenário, as informações da empresa precisam ser protegidas uma vez que não estão somente visíveis fisicamente. Nos últimos tempos, houve o aumento no número de ataques cibernéticos e seu comportamento também se modificou. No ano de 2018, segundo Fernandes (2019), os crimes e ataques cibernéticos dobraram em menos de um ano e, diariamente, são registrados pelo menos 366 crimes cibernéticos em todo o país. Não obstante, segundo a *Computer World* (2019), 72% das médias e grandes empresas do Brasil sofreram incidentes com dados no ano de 2018 e sofreram um prejuízo médio de 388 mil dólares. Nesse cenário, também houve o aumento de 265% dos ataques *fileless* (conjunto de técnicas de invasão sem arquivos executáveis) criados para disfarçar atividades maliciosas em comparação com o mesmo período do ano anterior.

Segundo O Globo (2017) na pesquisa efetuada pela empresa de Segurança da Informação Kaspersky, o Brasil é o sexto (6º) país mais vulnerável a vírus e, para os especialistas, as empresas locais investem pouco em segurança. Neste ano, o Brasil foi ranqueado como o terceiro país em golpes do mundo e o número de empresas que afirmam ter passado por ataques cibernéticos passou de 25% em 2017 para 34,71% em 2018 (BAND, 2019).

Nesse contexto, o país regulamentou, no ano de 2018, a Lei nº 13.709, Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) que estabelece normas sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, exigindo maior segurança e governança dos dados que entrará em vigor em agosto de 2020 e instigou o crescimento do profissional de *threat intelligence* (inteligência de ameaças, em tradução livre) para gerenciar as ameaças nas empresas.

Atuar preventivamente e estruturar a gestão de riscos passou a ser fundamental, contudo, seu processo de implantação depende do uso de metodologias adequadas e deve respeitar as peculiaridades de cada empresa, englobando a adoção de boas práticas como apresentadas pelo *framework* ITIL, COBIT e pela SI em conformidade com a LGPD.

Dessa forma, atendendo os termos da LGPD, teremos um cenário favorável para obter a correta gestão das informações nos ambientes corporativos e depende somente das empresas reconhecerem a necessidade de investir e implementarem os processos de segurança da informação para agirem de forma preventiva.

2.1 Vínculo com o curso de GTI

A pesquisa realizada neste trabalho tem vínculo direto com o curso de Gestão da Tecnologia da Informação, uma vez que o profissional formado - ao atuar na área de governança – enfrentará a problemática de gerenciar cenários de riscos internos ou externos, com a busca por soluções a fim de minimizar a probabilidade e os impactos nos processos.

Nesse contexto, fica evidente a relação dessa pesquisa com o perfil de egresso no Projeto Pedagógico do Curso (PCC) Superior de Tecnologia em Gestão da

Tecnologia da Informação (CST GTI) do IFSC (2014), conforme descrito, entre as competências esperadas do profissional de TI:

1. a capacitação de profissionais que possam realizar o planejamento da infraestrutura de empresas, orientando a aplicação tanto ao ambiente organizacional interno, como ao ambiente externo;
2. desenvolver atividades que busquem a integração das diversas unidades curriculares, estimulando a interdisciplinaridade.

3.DEFINIÇÃO DO PROBLEMA

Em um cenário de ataques cibernéticos cada vez mais recorrentes e mais complexos, as empresas ainda resistem em efetuar investimentos em Segurança da Informação, não direcionando investimentos para efetuar medidas preventivas. Segundo O Globo (2017) o investimento em segurança é pequeno e as empresas veem segurança como algo com pouco valor agregado. Essa decisão resulta em perdas financeiras para as empresas devido a roubo de informações corporativas/financeiras, interrupções de negócios e perdas de negócios ou contratos (EVALTEC, 2019).

Além das perdas financeiras causadas pela falta de investimentos em Segurança da Informação também existem os custos para restabelecer a perenidade dos ambientes e serviços. Além disso, os danos à reputação são maiores que os danos financeiros, podendo ocasionar a perda de clientes, perda de vendas, redução nos lucros e até levar à falência (EVALTEC, 2019).

Nesse contexto de pouco investimento em Segurança da Informação, ação reativa aos riscos e buscando complementar o *framework* ITIL no que se refere a gestão, será utilizado o COBIT, *framework* citado nas referências bibliográficas para atuar a partir da visão de gestão e estruturar a implantação do processo de gestão

de riscos em conjunto com o ITIL. Nesse sentido, restrições na descrição da aplicação de algumas etapas do COBIT neste estudo de caso ocorreram devido à impossibilidade de acesso às informações estratégicas ou de participação na decisão da implantação do processo. Esta pesquisa acompanhou as atividades da equipe de implantação da gestão de riscos, mas não pode acompanhar e documentar os passos desenvolvidos até a criação da equipe de implantação. Entre essas restrições, podemos citar: (1) definição das atribuições da equipe de implantação; (2) resultados esperados partem da alta gestão da empresa; (3) atribuições da equipe de implantação até o nível 4 e sem participação nas atividades de gestão (nível interno); (4) mapeamento dos objetivos somente no nível interno, treinamento e crescimento; (5) mapeamento efetuado sem a implementação do processo devido à limitação do tempo.

Nesse cenário, a presente pesquisa objetiva responder a seguinte pergunta: “De que forma pode se efetuar a implantação da gestão de riscos em uma empresa de TI que adota as boas práticas do *framework* ITIL por meio do COBIT e quais foram os benefícios e dificuldades encontradas para sua aplicação no ambiente corporativo?”.

4.OBJETIVOS

4.1 OBJETIVO GERAL

- Identificar benefícios e dificuldades encontradas na implantação do processo de gestão de riscos de segurança da informação para aplicação no ambiente corporativo.

4.2 OBJETIVOS ESPECÍFICOS

- Analisar e documentar a implantação de um processo de gestão de riscos em uma empresa de TI que adota o *framework* ITIL.
- Acompanhar e identificar aspectos da estruturação do processo de gestão de riscos em uma empresa que adote o *framework* ITIL;
- Mapear os processos e estruturar a aplicação do COBIT na implantação do processo de gestão de riscos em uma empresa que adota o *framework* ITIL em sua operação;
- Sugerir aperfeiçoamentos na implantação da gestão de riscos nas empresas que adotem as boas práticas do *framework* ITIL por meio da visão de gestão do COBIT.

5.REFERENCIAL TEÓRICO

Neste tópico, serão apresentados os conceitos e metodologias aplicáveis à gestão de riscos e ameaças em Segurança da Informação. Na redação deste trabalho visando a legibilidade, o termo “gestão de riscos” deverá considerar também as ameaças, embora exista uma definição diferente entre ambos os termos.

5.1 Segurança da Informação

A Segurança da Informação (SI) visa proteger a informação das ameaças, garantindo a integridade, disponibilidade e confidencialidade (BEAL, 2005). No contexto da SI, a informação é um ativo que possui grande valor para a organização e será protegido pela SI de qualquer ameaça ou acesso não autorizado visando

garantir a continuidade dos negócios e minimizar os possíveis danos com o intuito de maximizar o retorno e utilizar as oportunidades de negócios visando manter a perenidade do ambiente corporativo (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

Para atingir estes objetivos, a SI necessita que os três pilares estabelecidos por Pfleeger (1997) se integrem em consonância, sendo eles: processos, tecnologia e pessoas (Côrte, 2014). Por meio dos processos que estruturam e definem as ações nas organizações, junto a tecnologia utilizada para otimizar o funcionamento destes processos, temos as pessoas que garantem que estes processos funcionem da melhor forma possível.

A partir da consonância dos pilares da SI será possível sustentar a tríade: confidencialidade, integridade e disponibilidade. A confidencialidade garante que os dados sejam acessados somente por aqueles que devem ter acesso aos mesmos. A integridade assegura que os dados estejam em sua totalidade durante todo o seu ciclo de vida, sem haver qualquer modificação. A disponibilidade garante que os dados estejam disponíveis a qualquer momento, sem interrupções (MONTEIRO, 2016).

5.2 Riscos e Ameaças em Segurança da Informação

Todos os processos de uma empresa envolvem riscos e ameaças. Dessa forma, as organizações precisam gerenciar e acompanhá-los continuamente (MONTEIRO, 2018).

Nesse cenário, se faz necessária a distinção entre riscos e ameaças. O Risco é a probabilidade de uma determinada ameaça ocorrer, explorando vulnerabilidades de um ativo ou de um conjunto de ativos, visando prejudicar a organização, podendo ocasionar um incidente (MONTEIRO, 2016). O risco também pode ser

compreendido como um evento ou condição incerta que pode causar um efeito positivo ou negativo nos objetivos da empresa (FABRA, 2006).

Uma ameaça é uma potencial violação de segurança que pode gerar um evento que cause danos e prejuízos aos sistemas, sendo, normalmente, externas, não estando sob controle de uma pessoa específica (MONTEIRO, 2016).

Ainda neste contexto, conforme Monteiro (2016), as ameaças podem ser classificadas de acordo com a intenção: (1) naturais; (2) involuntárias; (3) voluntárias.

1. *Ameaças naturais*: estamos predispostos diariamente, sendo normalmente vinculadas a questões da natureza, tais como: incêndios naturais, tempestades, poluição, entre outros.
2. *Ameaças involuntárias*: vinculadas ao desconhecimento, como por exemplo: acidentes, erros, falta de energia, entre outros.
3. *Ameaças voluntárias*: relacionadas às intervenções humanas, tais como hackers, vírus, invasores, entre outros.

Dessa forma, é necessário gerenciar os riscos e as ameaças de forma planejada e agir de forma preventiva.

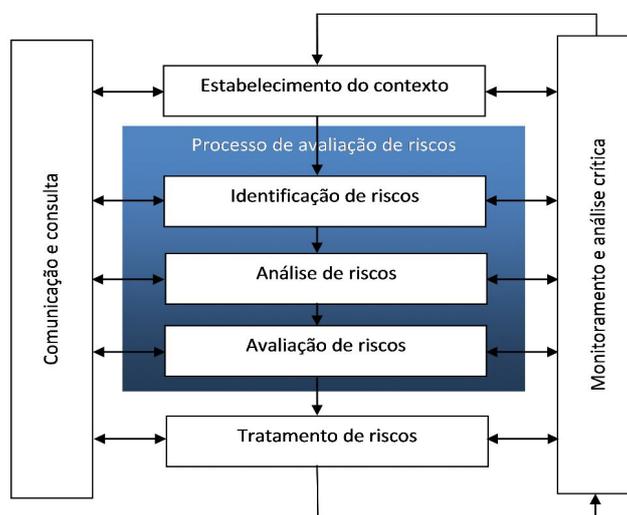
5.3 Gestão de Riscos em Segurança da Informação

A gestão de riscos em SI é caracterizada por atividades estruturadas para direcionar e controlar os riscos visando proteger o valor nas organizações (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011). Ainda, propõe-se a diminuir ou eliminar a probabilidade e o impacto de um evento negativo e potencializar a ocorrência de um evento positivo (FABRA, 2006).

Perante as normas ISO, a gestão de riscos pode ser realizada com base na ISO 27005, que define as linhas de orientação e suporte para a implementação do processo de gestão de riscos de Segurança da Informação (ASSOCIAÇÃO

BRASILEIRA DE NORMAS TÉCNICAS, 2011). Segundo esta norma, o processo de gestão de riscos está estruturado da seguinte forma:

Figura 1 - Processo de gestão de riscos



Fonte: adaptado da norma 27005 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

Primeiro, identifica-se os riscos por meio do cenário da organização, avaliando o ambiente interno e externo (ROSÁRIO, 2018). Após essa etapa, inicia-se o processo de avaliação dos riscos que engloba a identificação, a análise e avaliação dos riscos. Posteriormente, realiza-se o tratamento dos riscos conforme mapeado nas atividades anteriores. Durante todo o processo serão efetuados o monitoramento e a análise crítica do risco bem como a comunicação e consulta.

5.3.1 Processo de avaliação de riscos

O processo de avaliação de riscos permite identificar eventos que possam causar a perda dos ativos e mapear as ações a serem efetuadas (ASSOCIAÇÃO

BRASILEIRA DE NORMAS TÉCNICAS, 2011). O mapeamento destas ações é efetuado com base na probabilidade e impacto de cada risco identificado por meio de pesos previamente definidos, como exemplificado no Anexo A (Probabilidade e Impacto do Risco) que serão inseridos na fórmula: **RI** (Risco Inerente) = **NP** (Nível de Probabilidade) **X NI** (Nível de Impacto).

O valor obtido a partir dessa fórmula permitirá a classificação do risco (ANEXO B) de acordo com a sua faixa de risco, possibilitando mensurar, avaliar e ordenar os eventos de risco que podem impactar os processos empresariais (MONTEIRO, 2018). Possibilitando então, definir com maior precisão o tratamento e plano de resposta ao risco.

5.3.2 Tratamento e plano de resposta ao risco

Após a análise dos riscos, se faz necessário definir um plano de resposta ao risco com a definição das ações a serem realizadas. Esse direcionamento pode variar dependendo do que cada organização aceita como risco (LOPES, 2016).

A norma ISO 27005 define algumas tratativas para o plano de resposta ao risco. No presente trabalho, utilizaremos a denominação de Pereira e Bergamaschi (2018) para o plano de resposta ao risco: mitigar (ou reduzir); aceitar (ou tolerar); transferir (ou compartilhar) ou evitar (ou eliminar) o risco.

5.3.2.1 Mitigar o risco

Ao mitigar o risco, são efetuadas ações para reduzir a probabilidade e/ou impacto do risco. Se, caso o risco ocorrer, os impactos gerados serão menores e de mais fácil ajuste. Dessa forma, mitigar significa restringir os riscos a um nível aceitável pela organização (PEREIRA; BERGAMASCHI, 2018).

5.3.2.2 Evitar o risco

Ao evitar o risco significa modificar o que for necessário para eliminar o objeto sujeito ao risco, eliminando a ameaça na origem (PEREIRA; BERGAMASCHI, 2018).

5.3.2.3 Aceitar o risco

Ao aceitar o risco, a organização não atua no risco encontrado pois encontra-se um nível tolerável para a organização. Normalmente, estes riscos possuem probabilidade e impacto baixos que não justificam as ações a serem realizadas (PEREIRA; BERGAMASCHI, 2018).

5.3.2.4 Transferir o risco

A transferência do risco ocorre quando o risco não é de responsabilidade única de uma organização ou setor ou até mesmo quando a organização não possui acesso para modificar o cenário de risco. Em alguns casos, essa decisão pode ser registrada contratualmente (PEREIRA; BERGAMASCHI, 2018).

5.3.2.5 Definir ações

A partir da definição do tratamento e plano de resposta ao risco deverão ser mapeadas as ações a serem realizadas. Para a gestão das ações, pode-se utilizar o ciclo PDCA (*Plan, Do, Check e Act*) que permitirá o acompanhamento dos riscos do início ao fim, conforme apresentado na norma 27005.

Após o mapeamento por meio da matriz de risco, Rosário (2018) sugere a atitude perante a classificação de cada risco:

Quadro 01 - Atitude perante a classificação de cada risco

Classificação	Atitude sugerida
Risco baixo	Pode-se avaliar oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, por meio da redução de controles.
Risco médio	Não é necessária nenhuma ação, mas deve-se monitorar para manter o risco neste nível ou reduzi-lo sem custo.
Risco Alto	Necessário comunicar existência do risco para definir ações a serem tomadas em um curto período de tempo.
Risco Extremo	Necessárias ações imediatas para estes riscos, devendo ser comunicado para a alta gestão.

Fonte: Adaptado de Rosário (2018)

A atitude perante o risco só será eficaz se a sua classificação estiver correta, permitindo a ação preventiva perante cada risco classificado. Dessa forma, agregará valor aos ativos da organização.

5.3.2.6 Comunicação e Consulta

A comunicação e consulta durante a gestão dos riscos deve ser efetuado durante todo o processo, desde a coleta das informações até o seu fechamento visando alinhar e compartilhar quais ações foram definidas aos riscos mapeados podendo conter informações como probabilidade, severidade, tratamento e aceitação. Dessa forma, as tratativas serão mais assertivas e transparentes a todos os envolvidos facilitando a documentação das ações realizadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

5.3.2.7 Monitoramento e Análise Crítica dos fatores de risco

Como os riscos no ambiente corporativo não são imutáveis, o monitoramento e a análise crítica dos fatores de risco são essenciais para acompanhar as mudanças e efetuar novos planejamentos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

5.3.2.8 Riscos residuais

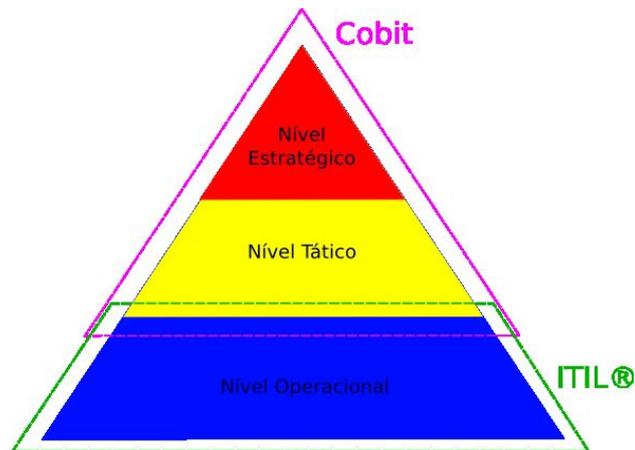
Os riscos residuais são riscos que permanecem mesmo após o tratamento do risco identificado. Alguns autores abordam sobre a necessidade de tratá-los da mesma forma que são tratados os demais riscos sem os distinguir dos demais (PEREIRA; BERGAMASCHI, 2018).

5.4 Governança de TI

A Governança de TI direciona os processos de acordo com as necessidades das partes envolvidas auxiliando na tomada de decisão e monitorando o desempenho e conformidade de acordo com os objetivos estabelecidos (ISACA, 2012).

A Governança de TI atua em todos os níveis nos processos de uma organização visando atingir os objetivos definidos por meio de *frameworks*. Neste trabalho, destacamos o COBIT e o ITIL que atuam em níveis diferenciados:

Figura 2 - Divisão da Governança de TI com COBIT e ITIL



Fonte: LEITE (2010)

No nível estratégico e tático, o COBIT atua direcionando os esforços para os objetivos da empresa bem como monitorando os resultados obtidos. Enquanto, no nível operacional, o ITIL permite alocar os recursos disponíveis de forma otimizada.

5.4.1 Information Technology Infrastructure Library (ITIL)

O ITIL define objetivos e atividades junto aos processos estruturados em empresas de TI. Entretanto, não determina de que forma estas boas práticas devem ser aplicadas dentro da empresa, apresentando de forma clara o *framework* a ser utilizado para desenhar os processos dos serviços de TI (PINHEIRO, 2011).

O ciclo de vida do ITIL é a estrutura cíclica que define como será feita a sua implantação. Ainda, os livros do ITIL são divididos de acordo com o ciclo de vida: (1) estratégia do serviço, (2) desenho de serviço, (3) transição de serviço e (4) operação de serviço.

A Estratégia de Serviço de TI é a primeira etapa do ciclo de vida do serviço da ITIL. Nesta etapa, são identificados os requisitos e necessidades do negócio que possam ser atendidas pela TI objetivando desenvolver estratégias que atendam estas demandas (FAGURY, 2010). Não obstante, na estratégia de serviço de TI há a interação com o negócio permitindo avaliar as demandas dos clientes, identificar oportunidades e riscos, avaliar retorno de investimento e ações a serem realizadas (PINHEIRO, 2011). As considerações que forem realizadas nesta etapa do ciclo serão utilizadas como base para o restante do ciclo de vida do ITIL (PINHEIRO, 2011).

A segunda etapa do ciclo de vida do serviço da ITIL é o Desenho de Serviço de TI, na qual serão utilizadas as informações mapeadas na estratégia de serviço de TI avaliando como gerar valor ao cliente. Nesse estágio, também serão desenhados os processos de Gerenciamento de Serviços de TI que permitirão o funcionamento dos demais (PINHEIRO, 2011).

A terceira etapa do ciclo de vida do serviço de TI é a Transição de Serviço de TI que é realizada a migração do serviço, permitindo que ele seja avaliado pelo usuário/cliente. Nessa etapa, são coletados os *feedbacks* que permitam a melhoria dos serviços (PINHEIRO, 2011).

A próxima etapa é a de Operação de Serviço de TI, na qual são realizadas ações para manter o funcionamento do serviço atual. Nessa etapa são mapeadas ações que facilitem as atividades diárias que potencializam os resultados (PINHEIRO, 2011).

Durante todo o processo do ciclo de vida do serviço do ITIL é realizada a Melhoria de Serviço Continuada que por meio do ciclo PDCA funciona como uma ferramenta de apoio para todos os processos e serviços. Durante este processo será avaliado se os serviços ainda atendem às necessidades do negócio por meio

de feedbacks e caso necessário, poderá ser reavaliada a estratégia do serviço de TI (PINHEIRO, 2011).

Por meio da aplicação do *framework* ITIL obtêm-se alguns benefícios, tais como: maior alinhamento entre a TI e o negócio da empresa; melhoria no que é entregue e na satisfação do cliente; redução de custos; diminuição de retrabalho das equipes envolvidas e melhor gestão de riscos do negócio (PINHEIRO, 2011).

5.4.2 Control Objectives for Information and related Technology (COBIT)

Enquanto o ITIL apresenta as melhores práticas operacionais para o funcionamento da TI, o COBIT define um conjunto de padrões internacionais de boas práticas e métodos documentados referentes ao uso da TI a partir da visão da gestão (BARROS, 2016). Não obstante, o COBIT fornece um modelo que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI por meio do equilíbrio entre riscos e utilização de recursos com base no *Balanced Scorecard* (BSC). Nesse contexto, o COBIT atua como um roteiro para a otimização de negócios e um direcionador de esforços (ISACA, 2016 apud BARROS, 2016).

5.4.2.1 Princípios do COBIT

Segundo ISACA (2012), o COBIT baseia-se em cinco princípios:

1. **Atender às necessidades das partes interessadas:** criar valor para a organização com o uso da TI. Para isso, pode-se utilizar a Cascata de Objetivos, conforme definido por ISACA (2012), que permite transformar os objetivos da organização em itens atingíveis junto à TI e divide-se em quatro partes:

- a. Os direcionadores das partes interessadas influenciam as suas necessidades: considera-se as influências externas, como por exemplo, mudanças no negócio, nas estratégias, dentre outros.
- b. Desdobramento das Necessidades das Partes Interessadas em Objetivos Corporativos: as necessidades das partes interessadas podem ser estruturadas em objetivos por meio do *Balanced Scorecard* (BSC).
- c. Cascata dos Objetivos Corporativos em Objetivos de TI: estrutura e define os resultados necessários para atingir os objetivos definidos com o BSC no passo anterior.
- d. Cascata dos Objetivos de TI em Metas do Habilitador: permite definir prioridades de implementação, melhorias e garantir da governança com base nos objetivos (estratégicos) da organização e no respectivo risco.

2. **Cobrir a empresa de ponta a ponta**: abrange todos os processos corporativos, não atuando somente na TI diretamente, mas considera a TI como qualquer outro ativo (ISACA, 2012).

3. **Aplicar um *framework* único e integrado**: permite o alinhamento à outros *frameworks* a ser utilizado como um modelo unificado para governança e gestão (ISACA, 2012).

4. **Permitir uma abordagem holística**: visa garantir o alinhamento com os objetivos a partir de sete categorias de habilitadores: (1) Princípios, Políticas e Modelos; (2) Processos; (3) Estruturas Organizacionais; (4) Cultura, Ética e Comportamento; (5) Informação; (6) Serviços, Infraestrutura e Aplicativos e (7) Pessoas, Habilidades e Competências (ISACA, 2012).

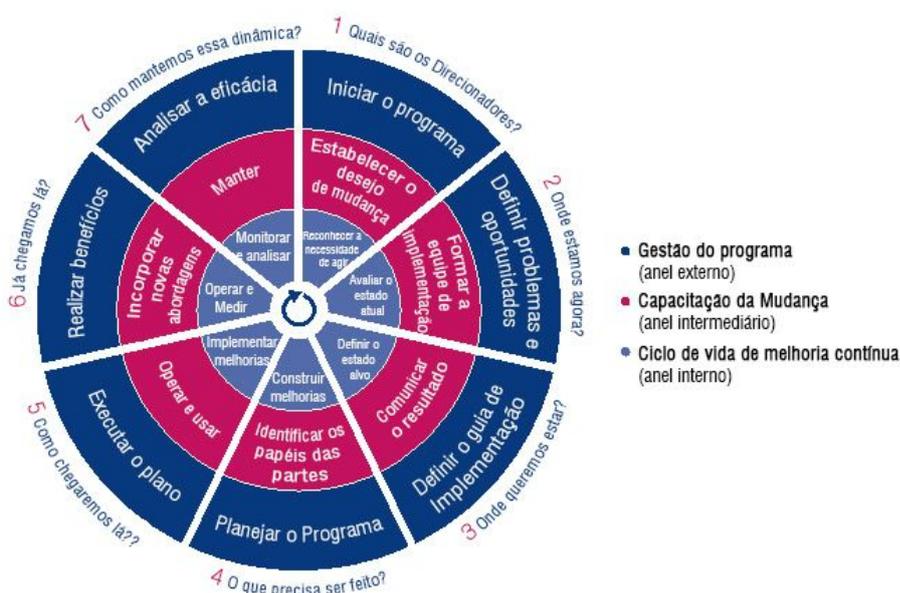
5. **Distinguir a governança da gestão**: distingue estas duas atividades, a Governança visa atender a necessidade das partes interessadas para atingir os

objetivos da organização e a Gestão, planeja, estrutura e monitora as ações com base nos objetivos definidos pela organização (DOURADO, 2014).

5.4.2.2 Ciclo de vida da implantação do COBIT

A partir dessa estrutura, o ISACA (2012) auxilia no processo de implantação do COBIT por meio das sete fases do ciclo de vida da implantação:

Figura 3 - Sete fases do ciclo de vida da implementação do COBIT



Fonte: ISACA (2012)

A 1ª Fase se inicia a partir de uma necessidade, avaliando pontos fracos para criar um desejo de mudança nos níveis de gestão executiva. A partir disso, na 2ª Fase, define-se o escopo da implantação por meio do mapeamento dos objetivos corporativos do COBIT em objetivos de TI e são avaliados os cenários de risco nos quais se deve concentrar. Não obstante, também se avalia o cenário atual da empresa bem como problemas para posterior ações.

Essas ações serão mais delimitadas na 3ª Fase, visando a melhoria junto à identificação de falhas e possíveis soluções. Na 4ª Fase, são planejadas soluções práticas através da definição de projetos apoiados por estudos de casos justificáveis.

Em seguida, na 5ª Fase, as soluções propostas são implementadas como práticas diárias e o monitoramento é estabelecido com o uso das metas e indicadores do COBIT. A 6ª Fase efetua o monitoramento do atingimento dos benefícios esperados enquanto na 7ª Fase, será efetuada a análise dos resultados visando mapear pontos para efetuar a melhoria contínua.

Dessa forma, o COBIT permite a análise das necessidades e riscos envolvidos no contexto organizacional visando formas de tratar e monitorar os resultados, efetuando melhorias constantemente.

6.PROCEDIMENTOS METODOLÓGICOS

Essa pesquisa analisa a implantação do processo de gestão de riscos realizada a partir de um estudo de caso em uma empresa do setor de TI. Por meio de um diário de bordo, foram acompanhadas e documentadas todas as etapas deste processo em detalhes, envolvendo a formação da equipe de implantação, as reuniões do grupo de implantação e os documentos de registro. A partir da análise da literatura buscou-se um *framework* adequado para a solução a ser modelada e uma proposta para a gestão de riscos na empresa, definindo um conjunto de atores, ações, ferramentas e procedimentos a serem adotados.

As conclusões foram alcançadas através da análise dos resultados dessas reuniões e da análise qualitativa do processo de implementação e a comparação com os preceitos dos *frameworks* adotados, ITIL e COBIT.

6.1 Caracterização da pesquisa

O presente estudo classifica-se como uma abordagem qualitativa, apresentando os aspectos encontrados que não podem ser quantificados, observando o processo, compreendendo e explicando a relação do item com o ambiente avaliando a dinâmica que ocorre (GERHARDT, 2009). Dessa forma, será avaliada a estruturação da implantação do processo de gestão de riscos em uma empresa de TI e aspectos considerados durante essa estruturação.

Quanto a sua natureza, pode-se defini-la como uma pesquisa aplicada que objetiva gerar conhecimentos para aplicação prática visando solucionar problemas específicos (GERHARDT, 2009). Nesse contexto, por meio da análise da estruturação da implantação do processo de gestão de riscos nessa empresa, será possível mapear boas práticas que permitam a aplicação em outras empresas.

No que se refere ao seu objetivo, a pesquisa pode ser classificada como exploratória e descritiva. Considera-se como pesquisa exploratória, pois contextualiza o problema visando obter diversas opiniões sobre o tema a partir do que foi divulgado previamente pela ciência. Ainda, classifica-se como pesquisa descritiva pois tem como finalidade descrever o objeto de estudo, suas características e problemas relacionados, apresentando de forma detalhada os fatos e fenômenos (GERHARDT; SILVEIRA, 2009).

Em relação aos procedimentos desta pesquisa, caracteriza-se como uma pesquisa bibliográfica. Segundo Fonseca (2002), a pesquisa bibliográfica se caracteriza pela leitura de conteúdos divulgados previamente sobre um tema específico em qualquer mídia:

A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites.

Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem, porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta (apud Gerhardt; Silveira, 2009, p. 37)

Dessa forma, ao avaliar o que já foi apresentado pela literatura previamente, é possível avaliar o cenário apresentado no estudo de caso. O estudo de caso é caracterizado pelo estudo de uma instituição ou organização visando conhecer de forma aprofundada como e porque determinada situação ocorre, apresentando itens característicos observados durante a pesquisa. Ainda, o estudo de caso pode ser efetuado de forma interpretativa, avaliando como é o ponto de vista dos participantes da forma mais completa possível do objeto de estudo por meio da análise do pesquisador (GIL, 2007, p. 54 apud Gerhardt; Silveira, 2009, p.39).

6.2 Procedimentos aplicados

Para a realização desta pesquisa, foi acompanhada a estruturação da implantação do processo de gestão de riscos através das reuniões de implantação e acompanhamento. As conclusões foram alcançadas através da análise dos resultados dessas reuniões e da análise qualitativa do processo de implementação e a comparação com os preceitos do *framework* ITIL e COBIT.

As reuniões ocorreram de forma semiestruturada por meio de tópicos definidos a partir da primeira reunião na qual foi realizada um *brainstorming* do cenário de implantação. O registro das reuniões e de cada tratativa foi feito de observações nas reuniões registrado em anotações e relatos escritos durante as

reuniões. Por fim, o resultado foi apresentado para a alta gestão para prosseguir com a implementação do processo.

Para a elaboração deste trabalho, foram efetuadas as seguintes etapas:

1. Avaliar bibliografia sobre o tema a fim de nortear a pesquisa;
2. Desenvolver a fundamentação teórica do tema selecionado;
3. Coletar as informações por meio de um diário de bordo sobre a implantação do processo participando das reuniões e documentar as técnicas, instrumentos, procedimentos adotados e resultados parciais obtidos;
4. Analisar e interpretar os dados coletados, comparando-os com os dados obtidos a partir da análise da literatura;
5. Apresentar considerações que possam auxiliar gestores no processo de implantação do processo de gestão de riscos.

7. ESTUDO DE CASO

O estudo de caso consiste na análise da estruturação da implantação do processo de gestão de riscos gerenciado pela equipe de implantação, que será acompanhado posteriormente pela Governança de TI, que define as boas práticas e os processos a serem seguidos pelas equipes de desenvolvimento e infraestrutura. A implantação do processo foi solicitada pela alta gestão da empresa e teve sua reunião de *kickoff* em julho de 2019, levando 35 dias e 7 encontros para ser mapeado e finalizado pela equipe de Governança e gerências envolvidas.

Além da análise da implantação do processo de gestão de riscos, tem-se como intuito documentar a aplicação de COBIT para servir como referência prática à outras empresas na implantação da governança de TI.

7.1 Descrição da Empresa

A empresa que compõe o estudo de caso é de grande porte, possuindo aproximadamente 1500 funcionários (junho/2019) em todo o Brasil. Em seu plano estratégico podemos destacar os itens norteadores de esforços:

- **Missão:** fazer a diferença na vida das organizações e das pessoas a partir da tecnologia;
- **Visão:** ser reconhecida como uma empresa de classe mundial;
- **Valores:** sustentabilidade, inovação, confiança, valorização de pessoas e criar relações duradouras.

A empresa está no mercado há mais de 20 anos desenvolvendo *softwares* para diversas áreas do setor público e atendendo clientes do Brasil e do exterior. Não obstante, a empresa efetua o uso do *framework Information Technology Infrastructure Library* (ITIL) em seus processos de atendimento e a plataforma *Rational Team Concert* (RTC), desenvolvida em 2008, para a gestão da demanda interna. Por fim, não será citado o nome da empresa uma vez que foi solicitado o sigilo das informações.

7.2 Mapa estratégico para implantação

Para implementar o COBIT 5 no processo de Gestão de Riscos, embasou-se nas boas práticas do seu ciclo de vida de implementação conforme a figura 03, considerando o contexto da empresa a partir da visão da Governança de TI para a implantação do processo até o nível 4 (restrição estabelecida pela alta gestão da empresa).

7.3 Fase 1: Quais são os direcionadores?

7.3.1 Iniciar o programa

O programa foi iniciado a partir do conhecimento de inúmeros casos de ataques que instigaram a gestão da empresa a avaliarem a estruturação de um processo de gestão de riscos. Dessa forma, com essa necessidade, foi definido uma equipe para estruturar o processo de gestão de riscos na organização e nos sistemas utilizados.

7.3.2 Estabelecer o desejo de mudança

A partir da identificação dos pontos de melhoria por meio da matriz SWOT e desenvolvida no planejamento estratégico da empresa e análise do contexto atual, foram iniciadas algumas ações que impulsionaram as mudanças na organização. Após a decisão da implantação do processo, a principal ação que iniciou o processo foi a definição dos membros para a equipe de implantação que permitiu o planejamento para a estruturação do processo.

7.4 Fase 2: Onde estamos agora?

7.4.1 Definir problemas e oportunidades

Para poder efetuar uma análise estratégica da organização, foi desenvolvida uma matriz SWOT que permite identificar forças, fraquezas, oportunidades, e ameaças, que foi parcialmente validada pela gestão da empresa.

Ambiente Interno	Forças	Fraquezas
	<ul style="list-style-type: none"> • Marca forte e reconhecida no mercado; • Abrangência da empresa devido ao foco de atuação; • Única empresa especializada no ramo de negócio. 	<ul style="list-style-type: none"> • Falta de reconhecimento dos profissionais capacitados; • Plataforma tecnológica defasada; • Alta rotatividade; • Processos internos não definidos.
Ambiente Externo	Oportunidades	Ameaças
	<ul style="list-style-type: none"> • Alta demanda por soluções para a área da saúde, construção e justiça; • Novas licitações. 	<ul style="list-style-type: none"> • Mudanças políticas; • Término de contratos; • Chegada de novos concorrentes; • Riscos na área da Segurança da Informação

7.4.2 Avaliar riscos

Podemos identificar os seguintes riscos na implantação do processo de Gestão de Riscos:

- Falta de apoio da gestão;
- Falta de engajamento dos envolvidos;
- Encaminhar corretamente a informação necessária para o registro dos riscos;
- Governança não possuir autonomia para efetuar cobranças;
- Ausência da participação das demais áreas nas reuniões;
- Ausência de uma boa comunicação para as tratativas.

7.4.3 Fatores críticos de sucesso da implementação

Podemos definir como os fatores críticos de sucesso para a implementação do processo de gestão de riscos:

- Todas as partes devem apoiar a governança TI, compreendendo os objetivos de negócio e TI;
- Formato das reuniões de acompanhamento;
- Comitê de Gestão de Riscos ser bem estabelecido;
- Restrição do acesso às informações sobre os riscos;
- Estrutura do cadastro dos riscos;
- Priorização dos riscos a serem tratados;
- Definição do plano de resposta aos riscos;
- Boa comunicação entre as partes interessadas, a sua vontade de mudar e apoio prestado às mesmas;
- Todos os participantes do Comitê de Gestão de Riscos devem seguir as boas práticas definidas, havendo uma uniformização nos procedimentos dos processos;
- Acompanhamento contínuo na Gestão de Riscos.

7.4.4 Cascata de Objetivos

A cascata de objetivos do COBIT é utilizada para converter as necessidades das partes interessadas em objetivos corporativos específicos, que quando personalizados, possibilitem a delimitação dos objetivos de TI. O detalhamento com o mapeamento dos objetivos corporativos do COBIT em perguntas sobre governança e gestão pode ser consultado no ANEXO C.

Para os mapeamentos apresentados abaixo, será utilizada a seguinte escala:

- **Primário (P)**: possui uma relação importante e o objetivo de TI pode ser considerado como essencial para atingir o objetivo corporativo.

- **Secundário (S):** apresenta uma relação menos importante ou o objetivo de TI representa um apoio secundário para o objetivo corporativo.
- **Em branco:** Sem relevância.

Quadro 02 - Objetivos Corporativos do COBIT 5

Objetivos Corporativos do COBIT 5				
Dimensão BSC	Objetivo corporativo	Relação com Objetivos de Governança		
		Realização de Benefícios	Otimização de Risco	Otimização de Recursos
Interna	11. Otimização da funcionalidade do processo de negócio		P	S
	12. Otimização dos custos do processo de negócio		P	
	13. Gestão de programas de mudanças de negócios	S	P	S
	14. Produtividade operacional e da equipe	P	P	S
	15. Conformidade com as políticas internas	P	P	P
Treinamento e Crescimento	16. Pessoas qualificadas e motivadas	P	P	P
	17. Cultura de inovação de produtos e negócios	S	P	

Fonte: adaptado de ISACA (2012)

7.4.5 Cascata de objetivos corporativos em objetivos TI

O objetivo da tabela de mapeamento é demonstrar como os objetivos corporativos possuem vínculo com os objetivos de TI.

Quadro 03 - Mapeamento dos Objetivos Corporativos do COBIT 5 em Objetivos de TI

Mapeamento dos Objetivos Corporativos do COBIT 5 em Objetivos de TI									
		Objetivos corporativos							
		Optimização da funcionalidade do processo de negócio	Optimização dos custos do processo de negócio	Programa de gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com as políticas internas	Cultura de inovação de produtos e negócios		
		1 1	1 2	1 3	1 4	1 5	1 6	1 7	
Objetivo de TI		Interna			A&C				
Interna	09	Agilidade de TI	P		P	S	P	S	
	10	Segurança da informação, infraestrutura de processamento e aplicativos	P				P	P	P
	11	Otimização de ativos, recursos e capacidades de TI				S		P	S
	12	Capacitação e apoio dos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio				S	P		
	13	Entregas de programas fornecendo benefícios, dentro do prazo, orçamento, e atendendo requisitos e padrões de qualidade	P		P	S			
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão	S	S	P	S	P	S	
	15	Conformidade de TI com as políticas internas	P	P	P	S	P	P	
A&C	16	Equipes de TI e de negócios motivadas e qualificadas				P	S	P	S

1	Conhecimento, expertise e iniciativas para a inovação dos negócios	P				S	P	S
7								

A&E: Aprendizagem e Crescimento

Fonte: adaptado de ISACA (2012)

7.4.6 Formar equipe de implantação

As pessoas designadas para compor a equipe de implantação de gestão de riscos foram duas pessoas da equipe de governança e um responsável pela equipe de implantação de processos. Com os integrantes designados, foram mapeados seus conhecimentos prévios, experiências e área de formação:

- Membro 1: a primeira pessoa da equipe de Governança estava há 8 anos na empresa, graduação em Administração e certificação ITIL;
- Membro 2: o outro membro da equipe de Governança estava há 1 ano na empresa e já possuía experiência na área de Governança, implantação de processos sendo especialista em Segurança da Informação;
- Membro 3: o representante da equipe de implantação de processos estava há mais 5 anos na empresa com formação e experiência focada em qualidade de processos gerenciais e implantação de processos.

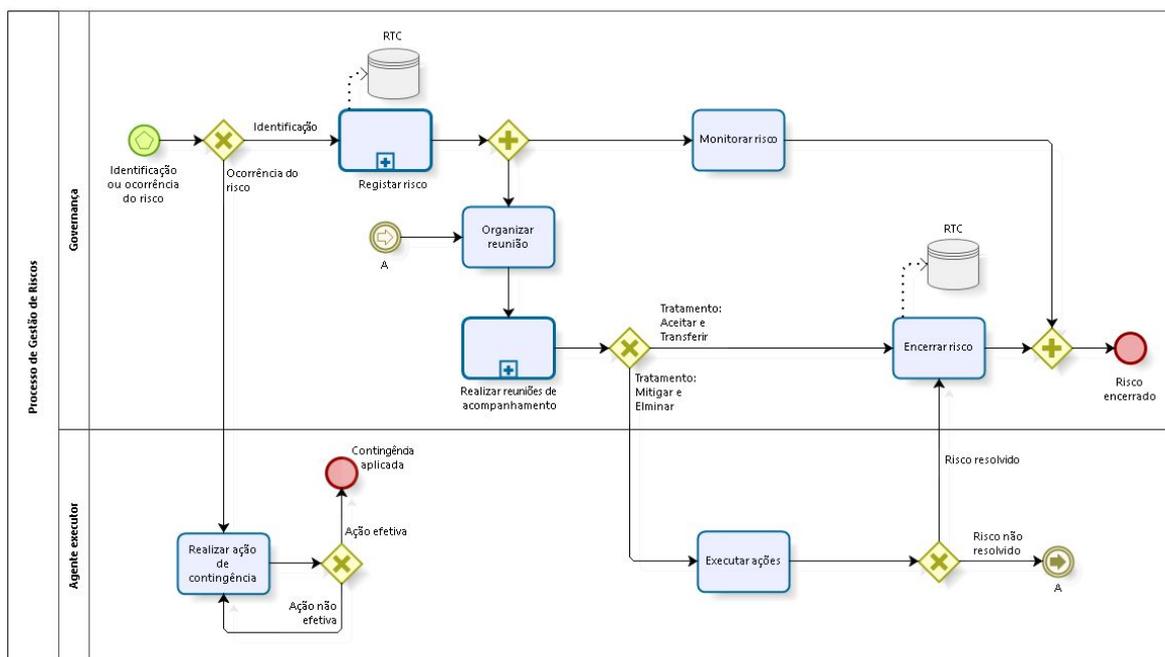
Não havia coordenador de equipe, sendo somente mediado o andamento do processo pelos envolvidos.

7.5 Fase 3: Onde queremos estar?

7.5.1 Definir o guia de implementação

O processo de gestão de riscos foi modelado de acordo com o funcionamento dos processos internos da empresa conforme Figura 8 (Processo de gestão de riscos):

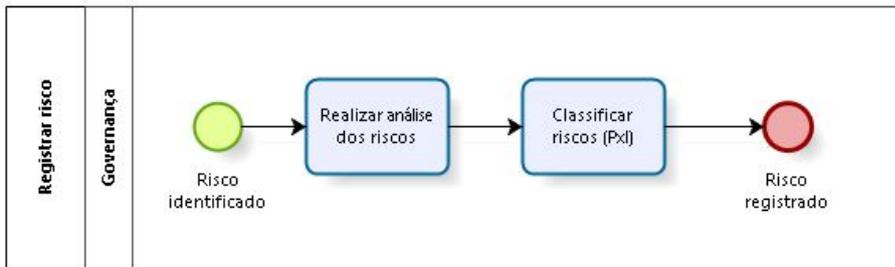
Figura 8 – Processo de gestão de riscos



Fonte: Elaboração do autor, 2019.

Foi definido que o processo de gestão de riscos se inicia a partir do repasse do conhecimento do risco via e-mail (segundo o modelo da Tabela 04) para a equipe de Governança ou pela ocorrência do risco. A partir disso, um dos subprocessos é registrar risco (Figura 9), no qual quando o risco é identificado ou recebida a informação sobre o risco, é realizada a análise e classificação dos riscos para então, efetuar o registro dos riscos.

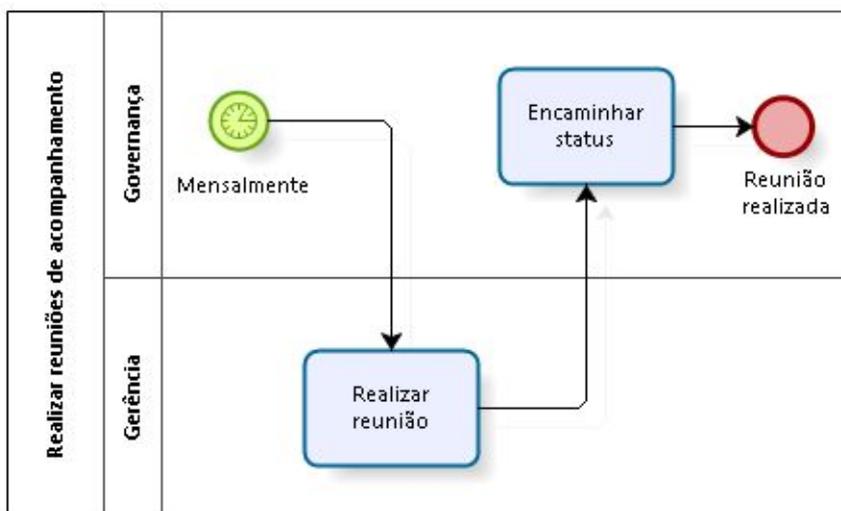
Figura 9 – Subprocesso: Registrar risco



Fonte: Elaboração do autor, 2019.

Outro subprocesso do processo de gestão de riscos, são as reuniões de acompanhamento. As reuniões, conforme a Figura 10, ocorrem mensalmente junto a Gerência, devendo ser realizado posterior atualização de status pela equipe de Governança.

Figura 10 – Subprocesso: Realizar reuniões de acompanhamento



Fonte: Elaboração do autor, 2019.

A partir do repasse do risco, que pode ser encaminhado por qualquer colaborador da empresa, será efetuada a análise, classificação do mesmo e registro

na plataforma RTC adotada pela empresa. No caso de ocorrência do risco, o processo atuará na ação de contingência, tratativa e finalização.

Antes das reuniões de acompanhamento, será realizada a análise e classificação dos riscos pela equipe de Governança. Após essa análise, serão realizadas as reuniões de acompanhamento junto às gerências, na qual serão definidos os planos de resposta aos riscos e prioridades.

A partir dessa definição, o risco poderá ser encerrado ou tratado. O tratamento do risco ocorrerá quando for decidido mitigar ou eliminar, podendo ser resolvido paliativamente ou definitivamente. Quando o risco for resolvido paliativamente, ele voltará a ser abordado nas reuniões de alinhamento até que seu tratamento seja concluído. O risco será encerrado definitivamente quando a decisão do tratamento do risco for aceitar ou transferir.

O processo ocorrerá de forma cíclica por meio do acompanhamento dos riscos já cadastrados, efetuando novos registros, avaliando prioridades nas reuniões de acompanhamento e das tratativas necessárias.

7.5.2 Atualização dos riscos cadastrados e modificação de status

A atualização e a modificação de status dos riscos cadastrados serão encaminhadas por e-mail somente para os coordenadores e gerentes que fazem parte do Comitê de Riscos. Este e-mail poderá ser enviado em dois formatos: atualização individual ou atualização de diversos itens.

Para efetuar a atualização de um risco individual, deverá ser preenchido com: título do risco, cliente que poderá ser impactado, probabilidade e impacto e atualização do status do risco, conforme APÊNDICE C (Modelo de atualização de status do risco - individual). Quando houver mais do que um risco a ser atualizado, deverão ser preenchidos os mesmos itens da atualização de risco individual e

informar a estratégia utilizada para resposta ao risco, no formato disponível no APÊNDICE D (Modelo de atualização de status do risco).

7.5.3 Comunicar o resultado

A comunicação sobre o processo de gestão de riscos foi efetuada em etapas. Primeiro, foi encaminhado um e-mail visando conscientizar os colaboradores sobre a necessidade do levantamento de riscos a todos os colaboradores.

Após essa ação, foi encaminhado o *link* para acessar a página do *Sharepoint* (ferramenta da empresa *Microsoft* que permite a criação de portais e gestão de conteúdo/documental) com o fluxograma e demais informações pertinentes sobre o processo.

A última ação de comunicação foi a apresentação do processo de gestão de riscos para a alta gestão e comitê de gestão de riscos com a proposta de implantação, abordando percepções e possíveis dificuldades no processo.

7.6 Fase 4: O que precisa ser feito?

7.6.1 Planejar o programa

A partir dos itens mapeados durante as reuniões, foram definidas ações e normas sobre o processo divididos em diferentes enfoques:

1. Reuniões / Acompanhamento

- serão realizadas reuniões mensais para acompanhamento de status;
- serão definidas ações e prazos para finalização
- os participantes do comitê serão coordenadores/gerentes

- seria criado um *template* para atualização do status dos riscos.

2. Informação / Cadastro

- acesso às informações somente para o comitê (visualização)
- identificar e informar os riscos é responsabilidade de todos
- conversa com o informante do risco após cadastro
- *template* para encaminhamento de informações por e-mail

3. Priorizações / Respostas

- priorizar os riscos a serem tratados
- definir plano de resposta aos riscos cadastrados

4. Envolvimento

- reforçar formato do processo de risco (Sharepoint / e-mail / processo)
- reforçar levantamento de riscos na reunião gerencial

Em seguida, com as informações referentes aos itens a serem tratados e ações mapeadas, foi definido um cronograma para as próximas ações com prazos na implementação do processo:

- 09/07/2019: Criar *template* para cadastro e atualização de status dos riscos
- 10/07/2019: Avaliar formato das reuniões e informações após cadastro
- 11/07/2019: Estruturar o processo de gestão de riscos e plano de resposta aos riscos cadastrados
- 16/07/2019: Encaminhar e-mail sobre a necessidade do registro dos riscos
- 22/07/2019: Estruturar página no Sharepoint sobre Processo de gestão de riscos

- 12/08/2019: Instruir sobre o processo de gestão de riscos e enviar e-mail com informações sobre o processo.
- 14/08/2019: Fazer reunião com os gerentes para apresentação após a finalização das atividades anteriores

As reuniões de acompanhamento das atividades ocorriam no dia de entrega das atividades mapeadas e eram realizadas com a equipe de implantação, duas pessoas da equipe de governança e um representante da área de processos.

Durante essas reuniões, foram avaliados os resultados e se contemplavam o que havia sido planejado. Além disso, quando possível, eram questionadas algumas ações ao comparar com o referencial teórico deste trabalho e instigar a reflexão dos itens que haviam sido mapeados.

Em paralelo às reuniões de alinhamento foi criado o item para registro dos riscos na plataforma *Rational Team Concert* (RTC) da IBM, podendo ser acessada exclusivamente pela equipe de Governança conforme APÊNDICE A (Item para registro dos riscos).

Para o registro do item de risco na plataforma, as informações deveriam ser encaminhadas previamente por e-mail pela pessoa que tiver conhecimento do risco. No item de registro do risco deverão ser preenchidos itens como: título; clientes e descrição. Itens como probabilidade, impacto e estratégia serão preenchidos pela equipe de Governança após análise do risco informado. O modelo deste e-mail enviado para registro dos riscos será de acordo com a APÊNDICE B (Modelo para levantamento de informações para o cadastro dos riscos).

7.6.2 Identificar o papel das partes

Para a execução deste processo, foram delimitados alguns grupos para as ações no processo:

- **Alta gestão:** gerência e diretoria que identificaram a necessidade do processo e definiram a equipe para implantação do processo e demais planejamentos.
- **Equipe de implantação:** definido pela alta gestão, sendo no total três pessoas. Duas pessoas da governança de TI e uma vinculada à área de processos para encaminhar a implantação do processo e efetuar as comunicações necessárias.
- **Equipe de desenvolvimento e infraestrutura:** principais times envolvidos no processo que realizarão o cadastro dos riscos na plataforma RTC e constantes atualizações conforme modelo delimitado no item Apêndice A, B e C.

7.6.3 Validação do processo de gestão de riscos

A validação da implantação do processo de gestão de riscos foi definida nas primeiras reuniões de estruturação do processo pela equipe de implantação e validado pela alta gestão.

Dessa forma, a validação será realizada através de acompanhamento do progresso das ações durante o período de um ano, havendo a avaliação dos registros e conclusão dos riscos registrados a cada três meses.

8. ANÁLISE DOS RESULTADOS

A presente pesquisa permitiu acompanhar, relatar as etapas e sugerir aperfeiçoamentos na implantação do processo de gestão de riscos de segurança da informação em sua totalidade, englobando: contexto da organização; seleção da equipe de implantação; planejamento para implantação e utilização dos *frameworks*;

ferramentas utilizadas no processo e comparação com o referencial teórico. Os principais instrumentos metodológicos utilizados na execução da pesquisa foram: análises documentais; participação da comissão de implantação e registro das reuniões por meio de um diário de bordo; observações de acordo com as atividades desenvolvidas e o comparação com o referencial teórico abordado.

Durante a análise documental, diário de bordo e observações realizadas, o alto grau de organização da empresa, com colaboradores capacitados, metodologia de gestão implementada e atividades internas bem definidas, foi um item de destaque, uma vez que propicia um ambiente favorável para a implantação de um novo processo. Ainda neste contexto, a seleção de profissionais com experiência nos processos internos e com conhecimento sobre gestão de riscos de segurança da informação foi fundamental para o sucesso do resultado obtido. Embora a equipe de implantação tivesse tamanho reduzido, o comprometimento dos envolvidos deu agilidade à entrega do processo solicitado pela alta gestão da empresa. Entretanto, foi possível identificar a necessidade de um integrante na equipe de implantação que tivesse acesso aos objetivos corporativos e demais informações junto à alta gestão, o que permitiria o alinhamento entre ambas as necessidades.

O planejamento, o modelo e a dinâmica utilizada nas reuniões para a implantação do processo de gestão de riscos permitiram avaliar atentamente as necessidades e os detalhes do processo, principalmente na primeira reunião na qual foram delimitadas as ações e prazos. A partir do planejamento, a estruturação da implantação efetuada com base no COBIT, um framework indicado no referencial teórico a ser utilizado junto ao ITIL, permitiu uma visão ampla da empresa bem como dos objetivos corporativos e, mesmo com a restrição de acesso às informações estratégicas que dificultaram a estruturação de algumas etapas do COBIT, conseguindo alcançar um resultado satisfatório. Dessa forma, as boas práticas do COBIT foram fundamentais para que a implantação do processo de gestão de riscos de segurança da informação fosse bem definida para suprir a

necessidade da empresa. Ainda que os resultados da implantação do processo de gestão de riscos não estejam finalizados, foram direcionados esforços para a atuação com base no COBIT e ITIL, visando maximizar os resultados obtidos.

Sobre a estruturação do processo de implantação de gestão de riscos, o modelo e a dinâmica utilizada nas reuniões de planejamento para a implantação do processo de gestão de riscos permitiram avaliar atentamente os detalhes do processo, sendo a primeira reunião essencial, onde foram delimitadas as ações a serem realizadas ao longo da implantação do processo.

As ferramentas de comunicação escolhidas para a implantação foram essenciais para garantir a clareza e o mesmo conhecimento do processo entre os colaboradores. Nesse sentido, o registro por meio do diário de bordo utilizado nesta pesquisa possibilitou ter as informações detalhadas sobre o processo para compartilhamento por meio do *Sharepoint*. Inclusive, a comunicação por e-mail permitiu que todos os envolvidos e impactados com o processo recebessem essas informações.

Além disso, o uso da ferramenta já utilizada pela organização, *Rational Team Concert (RTC)*, agilizou a implantação do processo de gestão de riscos de segurança da informação, não necessitando de treinamento para uso da ferramenta pelos colaboradores. Entretanto, ainda que a ferramenta tenha atendido as necessidades do processo, sua usabilidade e tecnologia eram divergentes das tecnologias utilizadas atualmente, podendo ser considerada como uma ferramenta obsoleta por ainda manter o funcionamento desde 2008, não sendo uma ferramenta muito prática ou intuitiva.

Ao comparar a implantação do processo junto ao referencial teórico desta pesquisa, foram identificadas algumas limitações que poderiam trazer ganhos ao processo. O processo inicialmente atua nos riscos e ameaças já existentes, não atuando de forma preventiva. Além disso, também não considera as oportunidades que os riscos podem gerar para os processos internos e não foram identificadas

ações com os riscos residuais, que permanecem após o tratamento de um risco, podendo deixar em aberto uma brecha que pode diminuir a segurança de todo o processo e causar retrabalhos desnecessariamente.

Além disso, identificou-se uma análise menos focada nos resultados da fórmula apresentada no referencial teórico para a matriz de riscos. Ainda que os valores vinculados à probabilidade e impacto sejam solicitados, serão utilizados mais como norteadores individuais e as decisões de ação serão definidas junto à alta gestão. Dessa forma, poderia ser utilizada a matriz de riscos de forma automatizada, auxiliando na tomada de decisão com maior assertividade.

Uma das etapas mais complexas dessa implantação foi conscientizar os colaboradores sobre a necessidade de criar os registros e atuar na tratativa de um risco. Dessa forma, sugere-se a criação de uma agenda que permita conversar, apresentar o processo e reforçar o comprometimento da empresa com a segurança da informação. E, a partir disso, transformar em um hábito os treinamentos para que todos os colaboradores possam identificar riscos e realizar as ações necessárias para que esse processo tenha eficácia após a implementação.

Ainda que tenham sido sugeridas algumas melhorias nesta pesquisa, o processo de gestão de riscos permaneceu com a modelagem proposta e teve seu início por meio dos registros dos riscos. Entretanto, uma das ações que será encaminhada será o benchmarking para identificar uma ferramenta que possa auxiliar na identificação dos riscos, sem a necessidade do registro manual visando atuar de forma preventiva.

Por fim, sugere-se que o acompanhamento e aperfeiçoamento do processo de gestão de riscos seja realizado junto a equipe de implantação, possibilitando a melhoria de acordo com o COBIT. Dessa forma, os treinamentos para os novos funcionários estarão cada vez melhores para dar maior agilidade no registro e tratativa dos novos riscos e ameaças e os ajustes nos processos de gestão de

riscos terão melhores resultados, estando de acordo com o *framework* utilizado na estruturação.

9. CONCLUSÕES

Durante o acompanhamento e registro da estruturação da implantação do processo de gestão de riscos em uma empresa que adota o ITIL em sua operação, foi possível identificar como o COBIT, possibilitou a estruturação do processo, atuando no nível estratégico e tático, por meio da visão da gestão, complementando o *framework* ITIL.

Ainda sobre o COBIT, à medida que não foi possível acompanhar as atividades da alta gestão da empresa, os resultados ficam parcialmente limitados na documentação das sete fases do ciclo de vida da implementação do COBIT. Dessa forma, é essencial a participação de um colaborador na equipe de implantação que possua acesso às informações necessárias e acompanhe o processo junto às metas corporativas.

A complexidade da implantação em uma empresa de grande porte e com uma cultura organizacional rígida dificulta a adesão dos colaboradores em processos que não gerem lucro imediato para as áreas atuantes. Nesse sentido, a pesquisa permitiu que fossem mapeados itens que podem ser melhorados junto a outros times de implantação do processo de gestão de riscos, permitindo que a alta direção tivesse maior conhecimento para atuar nas devidas tratativas.

Ao longo da implantação, foram necessários ajustes no processo em relação ao referencial teórico apresentado neste trabalho, uma vez que a empresa possui suas particularidades e a utilização do COBIT foi apresentada como uma nova

abordagem para a estruturação de processos, neste caso, o processo de gestão de riscos.

Em complemento à implantação deste processo, sugere-se que sejam efetuadas ações preventivas, mapeando riscos por meio de ferramentas automatizadas que identifiquem e monitorem ameaças, ou por meio da consulta às bases de ameaças e pelo acompanhamento de comunidades sobre SI. Não obstante, sugere-se também que sejam avaliados os riscos que geram oportunidades e ações para os riscos residuais que permanecem mesmo após o tratamento do risco inicial.

Por meio da análise realizada, podemos identificar que existem algumas restrições no que se refere à investimento em segurança da informação e resistência por parte dos colaboradores como um todo, bem como a necessidade das empresas adotarem ações que contemplem e assegurem a Segurança da Informação, ainda que diversos esforços estão sendo realizados para melhorar este cenário. Por fim, ainda que tenham sido sugeridos alguns ajustes no processo de gestão de riscos no estudo de caso, pode-se concluir que o objetivo inicial foi atingido e demais ajustes poderão ser efetuados durante a finalização do processo de implantação da gestão de riscos na empresa.

Para pesquisas futuras, sugere-se explorar ferramentas que possam auxiliar no processo de gestão de riscos permitindo que não seja necessária ação manual por parte dos colaboradores, atuando na detecção de riscos e ameaças. Dessa forma, possibilitando a análise estratégica das ações a serem encaminhadas sem necessidade de envolver a alta gestão diretamente neste processo. Além disso, também sugere-se acompanhar a aplicação de todas as etapas do ciclo de vida de implantação do COBIT junto ao *framework* ITIL, onde será possível visualizar mais pontos positivos e dificuldades na adoção de ambos os *frameworks*.

10.REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro. 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação — Requisitos**. Rio de Janeiro. 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27005: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro. 2011.

BAND, Metro Jornal Com. **Cresce número de sistemas invadidos por hackers; Brasil é o terceiro em golpes no mundo**. 2019. Disponível em: <<https://www.metrojornal.com.br/metroamp/estilo-vida/2019/05/25/hackers-brasil-golpes.html>>. Acesso em: 29 maio 2019.

BARROS, Conrado Gomes de Queiroz. **GOVERNANÇA DE TI: ESTUDO DAS BOAS PRÁTICAS SOBRE ALINHAMENTO DAS ESTRATÉGIAS DE TI E NEGÓCIO**. 2016. 57 f. Monografia (Graduação) - Curso de Sistemas de Informação, Universidade Federal Fluminense, Niterói, 2016.

BARROS, Leonardo. **2018 | O ano da evolução dos ataques cibernéticos. 2018**. Disponível em: <<https://canaltech.com.br/seguranca/2018-o-ano-da-evolucao-dos-ataques-ciberneticos-107168/>>. Acesso em: 28 jul. 2019.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, ago 2018.

CORREA, Rafael Murilo. **ITIL: o que é, importância e como implantar em sua Gestão de TI**. 2018. Disponível em: <<https://www.euax.com.br/2018/10/itil-o-que-e-importancia-como-implantar/>>. Acesso em: 25 out. 2018.

DOURADO, Luzia. **Apostila COBIT 5: Framework de Governança e Gestão Corporativa de TI**. São Paulo: Gestão Por Processos, 2014.

FERNANDES, Augusto. **Crimes virtuais e ataques cibernéticos mais do que dobram em um ano**. 2019. Disponível em: <https://www.correiobrasiliense.com.br/app/noticia/politica/2019/08/04/interna_politic>

a,775357/crimes-virtuais-e-ataques-ciberneticos-mais-do-que-dobram-em-um-ano.s.html>. Acesso em: 04 ago. 2019.

COMPUTER WORLD. **Ataques fileless têm crescimento de 265% em 2019, alerta Trend Micro.** 2019. Disponível em: <<https://computerworld.com.br/2019/09/02/ataques-fileless-tem-crescimento-de-265-em-2019-alerta-trend-micro/>>. Acesso em: 02 set. 2019.

COMPUTER WORLD. **72% das médias e grandes empresas do Brasil sofreram incidentes com dados.** 2019. Disponível em: <<https://computerworld.com.br/2019/08/07/72-das-medias-e-grandes-empresas-do-brasil-sofreram-incidentes-com-dados/>>. Acesso em: 12 set. 2019.

CÔRTE, Kelson. **Segurança da Informação baseada no valor da informação nos pilares tecnologia, pessoas e processos.** Brasília, DF, 2014. 212 p.

EVALTEC. **Como a falta de investimento em segurança afeta uma empresa?** 2019. Disponível em: <<https://www.evaltec.com.br/como-a-falta-de-investimento-em-seguranca-afeta-uma-empresa-2/>>. Acesso em: 05 set. 2019.

FABRA, Marcantonio Giuseppe Maria Carlo. **Gerenciamento de Riscos em Projetos de Implantação de Sistemas ERP.** 2006. 85 f. Dissertação (Mestrado) - Curso de Engenharia Industrial, Pontifícia Universidade Católica, Rio de Janeiro, 2006.

FAGURY, Thiago. **Apostila de ITIL V3.** São Paulo: Intinerante, 2010. 42 p.

FERNANDES, Nélia Ocampo. **Segurança da Informação.** Cuiabá: Universidade Federal do Mato Grosso, 2013.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa.** Porto Alegre: Universidade Federal do Rio Grande do Sul, 2009. 120 p.

IFSC. **Plano Pedagógico do Curso de Gestão da Tecnologia da Informação.** Florianópolis, 2014. Disponível em: <<http://florianopolis.ifsc.edu.br/images/stories/ppc/graduacao/ppc%20cst%20gestao%20em%20tecnologia%20da%20informacao%20%202015.pdf>>. Acesso em: 20 de mai. de 2019.

INFORMATION SYSTEMS AUDIT AND CONTROL.: **Modelo Corporativo para Governança e Gestão de TI da Organização - COBIT.** 5 ed. Rolling Meadows: Isaca, 2012.

LEITE, Charlene da Silva et al. **Gerenciamento de serviços de TI: um estudo de caso em uma empresa de suporte remoto em tecnologia da informação.** : um estudo de caso em uma empresa de suporte remoto em Tecnologia da Informação. Revista Eletrônica Sistemas & Gestão 5, Rio de Janeiro, v. 2, n. 5, p. 85-104, jun. 2010.

LOPES, Artur Cesar Sartori. **GESTÃO DE RISCOS**: A importância da resiliência em eventos indesejáveis. São Paulo: Fundação Getúlio Vargas, 2016.

MONTEIRO, Sheila de Góes. **gestão de riscos, Ameaças e Vulnerabilidades**. Estácio de Sá, Rio de Janeiro, 2018.

MONTEIRO, Sheila de Góes. **Fundamentos de Segurança da Informação**. Florianópolis: Estácio de Sá, 2016. 40 p.

PINHEIRO, Flávio R.. **Apostila ITIL V3 Foundation**. São Paulo: Ti Exames, 2011.

PEREIRA, Helena Acácio Santini; BERGAMASCHI, Alessandro Bunn. **Manual de gestão de riscos do INPI**. Rio de Janeiro: Instituto Nacional da Propriedade Industrial, 2018.

ROSÁRIO, Wagner de Campos. **METODOLOGIA DE GESTÃO DE RISCOS**. Brasília: Ministério da Transparência e Controladoria-geral da União - CGU, 2018.

SAMPAIO, Dhiêgo Rhubens Lima. **Um estudo sobre riscos de Segurança da Informação no campus da ufc em quixadá com base na norma iso/iec 27005**. Quixadá: Universidade Federal do Ceará, 2014.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva – Rio de Janeiro, 2003.

11.APÊNDICES

APÊNDICE A - Item para registro do risco - RTC

The screenshot shows a web-based interface for recording a risk item. At the top, there is a title bar with the text 'Risco <13:23:03>' and a 'Não iniciado' status. Below this are tabs for 'Overview', 'Links', 'Approvals', and 'History'. The main content area is divided into several sections: 'Dados de Controle' with dropdowns for 'Prioridade' (set to 'Não Designado') and 'Planejado para' (set to 'Não designado'); 'Detalhes' with dropdowns for 'Probabilidade' (set to '1 - Raro') and 'Impacto' (set to '1 - Sem Impacto'), and a 'Estratégia' section with radio buttons for 'Seleção', 'Eliminar', 'Mitigar', 'Transferir', and 'Aceitar'; 'Description' with a 'Descrição' field and a 'Resolução' field; and 'Discussion' with a text area for 'Incluir um comentário...'. On the right side, there are sidebars for 'Quick Information' (with 'Nenhum link'), 'Tags', and 'Área de Equipe e de Projeto' (with 'Produto / Gestão de Riscos').

Fonte: Elaboração do autor, 2019.

APÊNDICE B – Modelo para levantamento de informações para o cadastro dos riscos

<p>CADASTRO DE RISCO</p> <p>Título: descrever o risco que está sendo cadastrado</p> <p>Informação Técnica: descrever qual é o risco e como o risco poderá acontecer</p> <p>Possível impacto do risco: descrever qual será o possível impacto do risco, quais setores poderão ser afetados</p> <p>Cliente: inserir nome dos clientes que poderão ser impactados com o risco</p>

Fonte: Elaboração do autor, 2019

APÊNDICE C - Modelo de atualização de status do risco (individual)

<p>Modelo Atualização de Status Risco</p>	
<p>ATUALIZAÇÃO DE RISCO</p>	
<p>Título:</p>	<p>Cliente:</p>

Probabilidade:	Impacto:
Atualização do Status:	

Fonte: Elaboração do autor, 2019.

APÊNDICE D - Modelo de atualização de status do risco

Título	Cliente	Probabilidade	Impacto	Estratégia	Comentário

Fonte: Elaboração do autor, 2019.

11.ANEXOS

ANEXO A - Probabilidade e Impacto do Risco

Tabela 1 - Probabilidade e Impacto do Risco

Probabilidade	Impacto	Peso
Muito Baixa (Improável)	Muito Baixo (Mínimo)	1
Baixa (Rara)	Baixo (Pequeno impacto)	2
Média (Possível)	Médio (Moderado)	5
Alta (Provável)	Alto (Significativo)	8
Muito Alta (Praticamente certa)	Muito Alto (Catastrófico)	10

Fonte: Adaptado de Rosário (2018)

ANEXO B - Classificação do Risco

Tabela 2 - Classificação do Risco

Classificação	Faixa
---------------	-------

Risco Baixo – RB	0 – 9,99
Risco Médio – RM	10 – 39,99
Risco Alto – RA	40 – 79,99
Risco Extremo - RE	80 – 100

Fonte: Rosário (2018)

ANEXO C - Mapeamento dos objetivos corporativos do COBIT em perguntas sobre governança e gestão

Mapeamento dos Objetivos Corporativos do COBIT 5 em Perguntas sobre Governança e Gestão							
Necessidades das partes interessadas	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas de gestão de mudanças no negócio	Produtividade e operacional e da equipe	Conformidade e com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	11	12	13	14	15	16	17
Como faço para obter valor com o uso de TI? Os usuários finais estão satisfeitos com a qualidade do serviço de TI?							
Como posso gerenciar o desempenho de TI?							
Como posso explorar melhor as novas tecnologias para novas oportunidades estratégicas?							
Como faço para criar e estruturar da melhor forma o meu departamento de TI?							
Qual é a minha dependência de fornecedores externos? Quão bem os contratos de terceirização de TI estão sendo gerenciados? Como faço para obter garantia dos fornecedores externos?							
Quais são os requisitos (de controle) da informação?							
Considerarei todos os riscos de TI?							
Estou conduzindo uma resiliente e eficiente operação de TI?							

Como posso controlar o custo de TI? Como utilizar os recursos de TI de forma mais eficaz e eficiente? Quais são as opções de terceirização mais efetivas e eficientes?							
Tenho pessoal suficiente para TI? Como faço para desenvolver e manter sua capacitação, e como controlo seu desempenho?							
Como faço para obter garantia do funcionamento de TI?							
As informações que estou processando estão bem protegidas?							
Como posso melhorar a agilidade dos negócios com um ambiente de TI mais flexível?							
Os projetos de TI falham para entregar o que prometeram – e caso afirmativo, por quê? TI está atrapalhando a execução da estratégia de negócios?							
Quão crítica é TI para a sustentação da organização? O que fazer se ela não estiver disponível?							
Quais processos de negócios críticos dependem de TI, e quais são os requisitos dos processos de negócios?							
Qual tem sido o custo adicional médio dos orçamentos operacionais de TI? Com que frequência e em que medida os projetos de TI estouram o orçamento?							
Quanto do esforço de TI é dedicado para apagar incêndios em vez de facilitar a melhoria do negócio?							
Foram disponibilizados infraestruturas e recursos de TI suficientes para alcançar os objetivos estratégicos da organização?							
Quanto tempo é necessário para a tomada de decisões importantes de TI?							
O esforço total de TI e seus investimentos são transparentes?							

A TI apoia a organização no cumprimento dos regulamentos e níveis de serviço? Como faço para saber se estou em conformidade com todos os regulamentos aplicáveis?							
---	--	--	--	--	--	--	--

Fonte: adaptado de ISACA, 2012.