GERENCIAMENTO DE RISCOS NA SEGURANÇA DA INFORMAÇÃO: Uma análise de frameworks baseados em COBIT® 5[1]

Felipe Dias Corrêa[2]

Resumo: Este artigo abordará aspectos sobre gerenciamento de riscos que norteiam a segurança lógica corporativa de organizações. O estudo tem como objetivo apresentar soluções e ferramentas para minimização de falhas em ambientes de TI, usando como guia *frameworks* de gerenciamento de riscos. Para que esses objetivos tenham sucesso, iremos utilizar como referência, artigos e autores que contribuíram de forma significativa para o tema, além de usar *frameworks* de gerenciamento de riscos e a poderosa biblioteca de governança COBIT® 5. No estudo também foram citados alguns *cases* de sucesso na implementação de gerenciamento de riscos em ambientes reais. Por fim, a pesquisa mostrou a importância da gestão de riscos para as organizações, e também a relevância que o tema tem, contribuindo de forma satisfatória para empresas, organizações, líderes e gestores de TI, como um meio de conscientização ou um método para aplicação dessas práticas.

Palavras-chave: Gerenciamento de Riscos. Segurança. Frameworks.

1 INTRODUÇÃO

Gerenciar e manter um ambiente de TI (tecnologia da informação) seguro tem sido um grande desafio para organizações de médio e grande porte atualmente. Mesmo com o avanço de ferramentas de gerência e novas tecnologias, ainda sim estamos sempre expostos aos riscos. A preservação da integridade, confidencialidade e disponibilidade dos dados é um fator primordial para a proteção dos ativos da organização, por isso o gerenciamento de riscos é de suma importância nesse cenário. A segurança da informação protege a informação contra vulnerabilidades no intuito de garantir a continuidade dos processos, minimizar os impactos e maximizar os investimentos e oportunidades do negócio (JÚNIOR, 2008).

> O COBIT (*Control Objectives For Information and Related Technology*), *framework* referência para prover Governança de TIC (tecnologia da informação e comunicação), é formado por uma estrutura de domínios, processos e atividades. O domínio de Planejamento e Organização é constituído, entre outros, pelo processo de estimativa e controle de riscos (JÚNIOR, 2008, p.12).

[1] Artigo apresentado como Trabalho de Conclusão de Curso de Especialização em Governança de Tecnologia da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Governança de Tecnologia da Informação.
Orientador: Prof. Luiz Otávio Botelho Lento, Msc. em Ciência da Computação. UNICAMP, 1994.

[2] Pós-Graduando do Curso de Governança de Tecnologia da Informação da Universidade do Sul de Santa Catarina. felipedias_c@hotmail.com

Ao longo da pesquisa estudamos alguns *frameworks* de gerenciamento de riscos, baseado nessa poderosa biblioteca de governança de TI (COBIT 5), que por sua vez podem executar com eficácia a mitigação ou total anulação de falhas na segurança corporativa, protegendo e mantendo os dados em total seguridade. Também usaremos, como base de conhecimento, o guia *Project Management Body Of Knowledge* (PMBOK®, 2013), que determina diretrizes de boas práticas para gerenciamento de projetos. Esse estudo também contribui como forma de conscientização para a implementação de ferramentas de gerenciamento de riscos nas organizações de pequeno, médio e grande porte.

> O Guia "COBIT 5 *for Information Security*" é composto de princípios aceitos mundialmente, bem como de ferramentas e modelos analíticos desenvolvidos para suportar o negócio e a TI, maximizando o grau de confiabilidade e valor que o mercado deposita nas operações da empresa, na sua informação e nos seus ativos de tecnologia (BUCCI, 2012, p.1).

Sendo assim, como podemos minimizar falhas de TI na segurança corporativa implementando, de forma eficaz, frameworks de gerenciamento de riscos baseados em COBIT?

O trabalho em seu objetivo geral apresenta soluções e ferramentas para mitigar falhas de TI na segurança corporativa através de frameworks de gerenciamento de riscos. E como objetivos específicos o trabalho busca mapear e minimizar riscos comuns em ambientes corporativos de TI, apresentar vantagens do uso de *frameworks* e fazer uma análise minuciosa dessas bibliotecas.

A pesquisa foi feita no modelo de pesquisa bibliográfica. Quanto à coleta de dados a pesquisa buscou diversos autores e livros que contribuíram de forma significativa para o tema, com publicações, trabalhos e artigos. Também são destacados e citados alguns *Cases* (casos de uso) que foram bem-sucedidos quanto a implementação de forma prática do tema em cenários reais de organizações. Inicialmente o trabalho poderá ser classificado como pesquisa teórica, pois no primeiro momento não haverá contato com um ambiente real de estudos, mas sim na apresentação e comprovação da teoria e método sugerido pelo estudo. Posteriormente poderá a trabalhar paralelamente com uma pesquisa de campo, contribuindo como referência para que o método e tese discutidos no trabalho sejam aplicados em um estudo de caso de um cenário real.

2 GERENCIAMENTO DE RISCOS DE TI

Planejar e traçar uma estratégia para o gerenciamento de riscos é o que podemos denominar de pontapé inicial para uma boa manutenção da segurança corporativa. Segundo a ISSO/IEC 27005 [...] "A Gestão de Riscos é definida com as atividades coordenadas para direcionar e controlar uma organização no que se refere ao risco" (ABNT, 2008). Para auxiliar gestores nessas tarefas, existem diversos *frameworks* de Gestão de TI, direcionados especificamente para tratamento e gerenciamento de riscos. Ao longo da pesquisa, estudaremos alguns desses *frameworks*, como por exemplo os: *Risk IT (information technology)* e o *Val IT,* e também os códigos de boas práticas de segurança da informação da ABNT (Associação Brasileira de Normas Técnicas): ISO/IEC (*International Organization for Standardization/International Electrotechnical Commission*) 27002, ISO/IEC 27005. O Guia *Project Management Body Of Knowledge* (PMBOK®, 2013), também será agregado na pesquisa, pois traz ótimas referências e o gerenciamento de riscos faz parte de um de seus grupos de processos.

De acordo com REIS "[...] desde os raios que fizeram com que os homens procurassem abrigo aos modernos sistemas de segurança e defesa nacionais, o desejo de se proteger ou tentar diminuir as consequências da incerteza fez parte da natureza humana" (REIS, 2012). Por esse e outros motivos, o gerenciamento de riscos tem sido visto como um fator de suma importância dentro das organizações, pois além de oferecer uma maior proteção aos ativos internos, também maximiza os resultados da empresa diante do mercado.

Planejar e definir o gerenciamento de riscos traz a minimização do impacto de eventos potencialmente negativos aos negócios e ativos da organização, mas também pode colaborar com o aumento do grau confiança das partes interessadas.

> As organizações existem para criar valor para suas partes interessadas. Consequentemente, qualquer organização — comercial ou não — terá a criação de valor como um objetivo da governança. Criar valor significa realizar benefícios com uma ótima relação de custo e ainda otimizar o risco (ISACA, 2012, p. 16).

A gestão de riscos, dentro do cenário da segurança corporativa, deve ser uma atividade com visão de melhoria contínua dos serviços, sendo aplicado um padrão para o GRSI (Gestão de Risco em Segurança da Informação), baseado ou normatizado em um *framework*. De acordo com Silva (2009) "[...] O processo de gestão de risco começa com a definição do contexto. Em seguida é feita a análise/avaliação de riscos, em que os riscos são identificados,

estimados e avaliados segundo critérios definidos no momento do estabelecimento do contexto.” (SILVA, 2009, p. 12). Já segundo o COBIT 5 (2012), a Gestão de Riscos se define como “[...] Um dos objetivos da governança. Implica o reconhecimento do risco; avaliação do impacto e da probabilidade daquele risco; e desenvolvimento de estratégias para evitar o risco, reduzir o efeito negativo do risco e/ou transferir o risco, para administrá-lo no contexto da organização de inclinação ao risco” (ISACA, 2012, p. 95).

2.1 Frameworks de Governança de TI e Gerenciamento de Riscos

A pesquisa busca uma ampla visão de cada *framework* estudado, para que isso ocorra foi feito um levantamento bibliográfico de artigos e pesquisas que falam sobre cada um, mostrando suas aplicações no ambiente corporativo, bem como suas vantagens na implementação. A seguir apresentaremos uma breve descrição de cada um dos *frameworks* citados anteriormente.

2.1.1 COBIT 5

A última edição (2012) da respeitada biblioteca de governança de TI do ISACA (*Information Systems Audit and Control Association*), que ajuda gestores nas tomadas de decisões dos negócios de TI. Destaca-se também que é de grande importância no ambiente corporativo de tecnologia da informação e comunicação, pois seus processos norteiam de forma eficaz no alinhamento dos negócios com a TI.

2.1.2 RISK IT

Framework baseado em COBIT 5, que tem como abrangência todos os fatores do gerenciamento de riscos, norteando gestores no tratamento de todos os tipos de riscos. Uma ferramenta poderosa e pioneira em gerenciamento de riscos.

2.1.3 ISO/IEC 27002

Código de boas práticas para gerenciamento de segurança da informação que de acordo com a ABNT tem como principal objetivo: “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (ABNT, 2005)."

2.1.4 ISO/IEC 27005

Norma técnica que abrange Gestão de Riscos de Sistemas de Informação. É um dos requisitos da norma ISO/IEC 27002, por isso não surgiu se sobrepondo a ela, e sim a complementando como um desdobramento.

2.1.5 VAL IT

Conjunto de práticas de governança que auxiliam gestores e executivos na otimização dos investimentos voltados para TI. Possue três grandes focos: *Value Governance (VG), Portfolio Management (PM) e Investment Management (IM).* Assim como o Risk IT, Também é baseado em COBIT.

2.1.6 PMBOK

O PMBOK® (*Project Management Body Of Knowledge)* é um guia para gestores de projetos, organizado pelo PMI (*Project Management Institute*) que traz um conjunto de boas práticas para profissionais e membros que atuam na área.

3 DEFINIÇÕES E VANTAGENS DE FRAMEWORKS DE GESTÃO DE RISCOS

A tecnologia da informação vem em uma crescente desenfreada dentro das organizações e cada vez mais se tornou mais importante para os processos internos. Com isso veio a grande preocupação com a integridade e segurança da informação. Para que haja a mitigação do impacto dessas vunerabilidades, foi desenvolvido e evoluído ao passar dos anos boas práticas de gerenciamento de riscos. Os *framework* (bibliotecas) são conjuntos de práticas que visam padronizar os processos de TI dentro de uma organização, e alguns deles já citados no trabalho serão de grande auxílio para que o plano de gestão de riscos tenham sucesso.

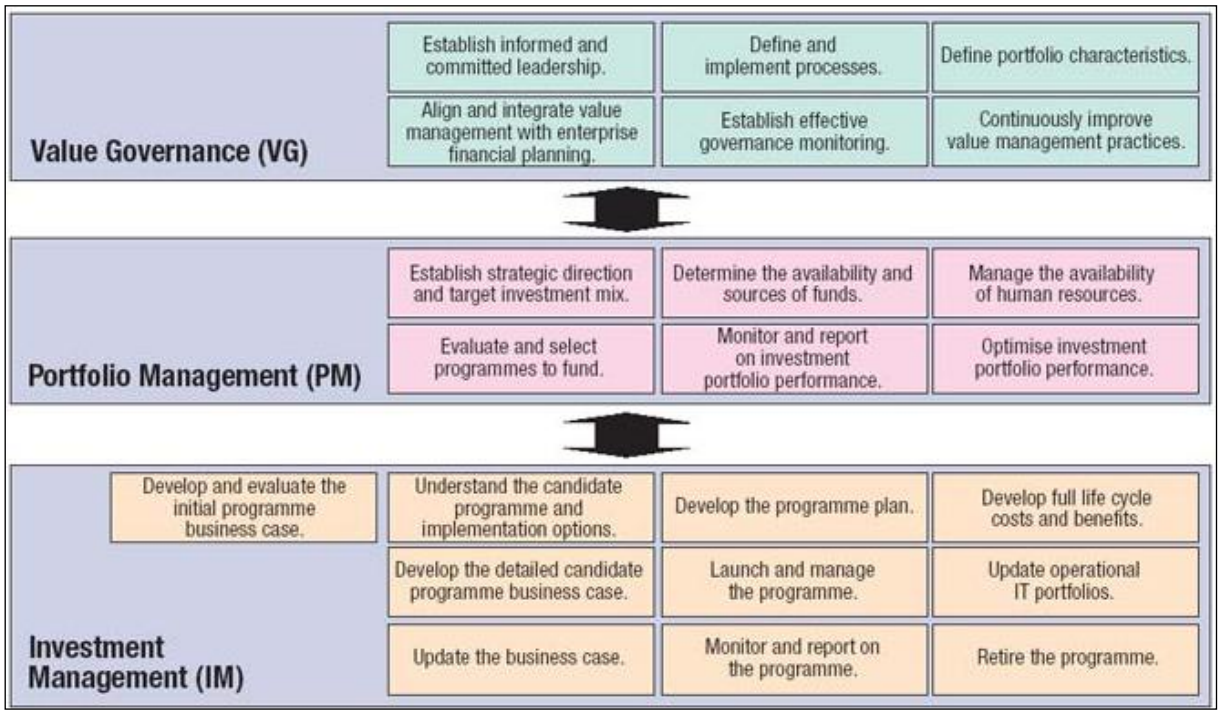
Começaremos por duas importantes normas de segurança da informação, que no geral se completam como duas poderosas ferramentas de gestão de riscos. A Norma ISO/IEC 27002:2005 e a norma ISO/IEC 27005:2008. Segundo a ABNT NBR a ISO/IEC 27002 tem como objetivo “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização” (ABNT, 2005). Já a norma ISO/IEC 27005 define as orientações para a gestão de riscos dentro da segurança da informação. Mas qual a diferença entre as duas? A norma ISO/IEC 27002 está acima pois é ela quem define todos os requisitos da segurança da informação, e a norma ISO/IEC 27005 se torna uma segmentação de um desses requisitos. Ambas podem trabalhar em conjunto e se tornam ferramentas extremamente eficazes se seguidas à risca.

Agora veremos três ferramentas que também, podemos dizer assim, se completam se usadas de forma integrada no plano de gestão. O *VAL IT*, um *framework* que baseia-se na biblioteca COBIT e objetiva definir o valor de negócio sobre os investimentos feitos.

> O Val IT é um framework que habilita a criação de valor de negócios sobre os investimentos de TI. Desenhado para alinhar e complementar com o Cobit, o Val IT integra uma série de práticas e provê princípios de governança, processos e, suportando com orientações para diretores, times executivos de gerenciamento e outros líderes da companhia otimizando o valor sobre os investimentos de TI (OLIVEIRA, 2016).

Mas por quê o *VAL IT* se relaciona diretamente com o COBIT? Ambos trabalham alinhados aos negócios e com um ponto de vista empresarial. O *VAL IT*, trabalha em três grandes focos: *Value Governance (VG)*: estabelece normas para o gerenciamento ficar alinhado aos negócios de empresa; *Portfolio Management (PM)*: gerencia todo o portifólio de investimentos da organização, fortalecendo o valor da empresa; *Investment Management (IM)*: gerencia todos os resultados de investimentos feitos. Abaixo veremos a relação de cada um deles:

Figura 1 – Focos do VAL IT



Fonte: Oliveira, 2016

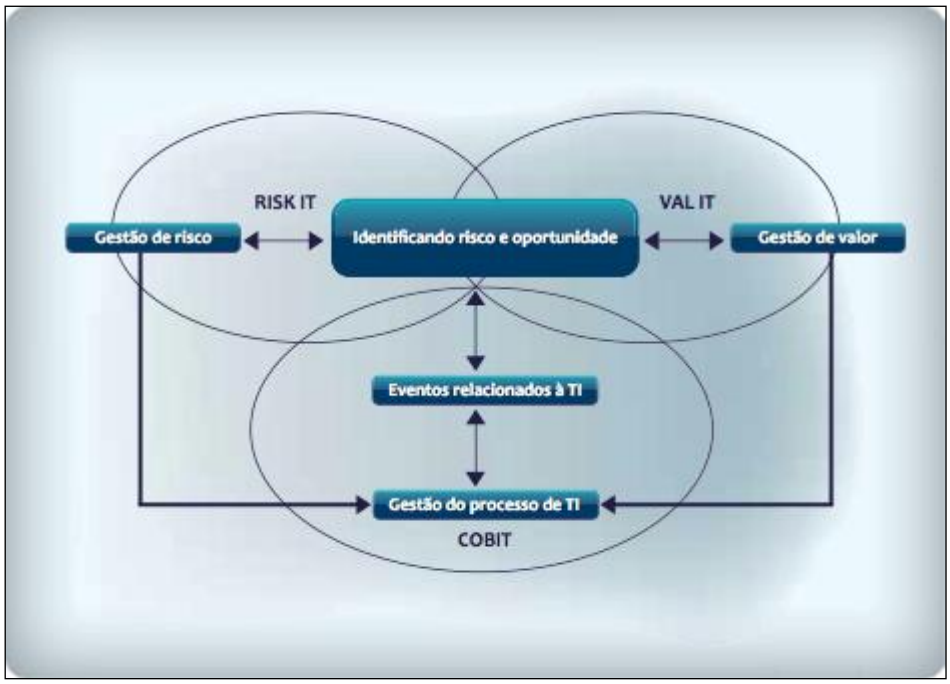
O *RISK IT*, também baseado em COBIT, é um conjunto de práticas que norteiam gestores no gerenciamento de riscos. É também conhecido por ser o pioneiro nesse meio de gestão der riscos. De acordo com OLIVEIRA, "[...] O framework complementa o COBIT, um

compreensivo framework para a governança e controle de serviços e soluções baseadas em TI e voltadas para negócios" (OLIVEIRA, 2011). Podemos notar a conexão e o relacionamento dessas ferramentas se usadas junto ao COBIT, por isso estamos ressaltando sempre a conexão entre as três bibliotecas.

> Os benefícios por usar o *Risk IT* incluem uma linguagem comum para ajudar na comunicação entre gestões de negócios, TI, riscos e auditoria; Orientação ponto a ponto sobre como gerenciar riscos relacionados a TI; Um perfil completo de riscos para melhor entender os riscos, de modo a utilizar melhor os recursos da empresa; Uma melhor compreensão dos papéis e responsabilidades em referência a gestão de riscos de TI; Alinhamento com ERM; Uma melhor visão dos riscos relacionados a TI e suas implicações financeiras; Menos falhas e surpresas operacionais; Melhora da qualidade da informação; Utilizações inovadoras dando apoio a novas iniciativas de negócios. (OLIVEIRA, 2011, p.1)

O COBIT é soberano sobre essas duas ferramentas, pois é um conjunto de boas práticas reconhecido mundialmente, com inúmeros processos, inclundo de gerenciamento de riscos, que poderão ajudar a alinhar a TI aos negócios da organização. O ideal seria usar os três agregados, pois os mesmos se complementam, O *VAL IT* otimiza os valores e investimentos da organização, O *RISK IT* minimiza o impacto de riscos sobre o negócio e o COBIT alinha a TI aos negócios. Abaixo, na figura 2, veremos a correlação entre os três.

Figura 2 – Relação entre RISK IT, VAL IT E COBIT



Fonte: MACÊDO, 2012

O PMBOK, guia de gerenciamento de projetos para profissionais da área, que é mantido pelo PMI (*Project Management Institute*), também é importante na ambito corporativo. O gerenciamento de riscos é um processo tratado com muita importância dentro de PMBOK e é considerado de extrema relevância para o sucesso dos projetos de gestores. Dessa forma o PMBOK, pode ser usado como um guia, ou um "guru" no gerenciamento de riscos, para ser consultado sempre que houver alguma dúvida acerca de alguma prática ou processo.

Agora que cada um dos *frameworks* foram retratados afim de exibir as vantagens de cada um, fica a pergunta: qual devo usar? É importante que seja analisado a necessidade de cada ambiente e qual resultado esperado. Quer melhores resultados nos negócios? A melhor solução pode ser o COBIT com *VAL IT* e *RISK IT*. Quer melhores práticas na segurança da informação em geral? A ISO/IEC 27002 e ISO/IEC 27005 é capaz de suprir suas necessidades. Tem dúvida em algum processo ou procedimento de gerenciamento de riscos? O PMBOK pode lhe orientar na busca da melhor saída.

4 COMO IMPLEMENTAR O GERENCIAMENTO DE RISCOS

O trabalho tem como objetivo, além do estudo de forma sistemática dos *frameworks*, guias e procediementos de gerenciamento de riscos, a conscientização sobre a importância da gestão de riscos no ambiente corporativo. Essa conscientização vai desde o usuário final, passando por líderes, gestores de TI, executivos e alta diretoria de grandes, médias e pequenas corporações. É muito importante que todos, tenham em mente, o quanto é importante todo esse conjunto de práticas para o aumento da produtividade dentro do ambiente e o sucesso no mercado afora. Agora veremos de forma breve e objetiva, tópicos importantes para a implementação de gerenciamento de riscos.

4.1 Conscientização dos Colaboradores no Ambiente Corporativo

O ponto primordial do sucesso de um plano de gerenciamento de riscos, além das tradicionais etapas do processo, é o empenho e conscientização de todos os envolvidos no ambiente. Não devemos colocar tudo apenas na conta do gestor de TI, pois se o usuário não tiver discernimento e disciplina para seguir a riscas os protocolos adotados, o plano de gestão pode acabar falhando. Diretores e altos executivos também devem se empenhar para que o processo tenha resultado, pois é desse escalão que virão os recursos e as aprovações de medidas e mudanças que devem ser tomadas.

> O sucesso do gerenciamento de riscos irá depender do compromisso da alta direção, de total e participação da equipe de tecnologia da informação e comunicação, da competência e da experiência do time de gestão de riscos em aplicar com efetividade a metodologia, da consciência e cooperação dos usuarios em cumprir procedimentos e da melhoria contínua da validação e estimativa dos riscos. (JÚNIOR, 2008, p. 36).

Outro entrave que pode vir a atrapalhar esse processo são as resistências as mudanças, que podem partir desde aquele usuário mais antigo e saudosista que acha que tudo desse ser feito "a moda antiga", ou até mesmo vim de um diretor ou membro do alto escalação da organização, que não tem total confiança no plano de gestão de riscos. Por isso é importante destacar a magnitude de fazer um plano de gerenciamento de riscos bem objetivo e eficiente, pois a partir daí conquista-se a confiança da alta administração e de grande parte dos usuários, os que se manterem mais resistentes poderão mudar de opinião ao longo da implementação, ou até mesmo a alta diretoria poderá usar de sua autoridade e respaldo para passar confiança para aqueles usuários mais resistentes as mudanças. JÚNIOR destaca que um dos fundamentos de sucesso do plano de gestão de riscos é o "Patrocínio Executivo: total apoio da alta direção ao processo de gerenciamento de riscos, de modo a reduzir a resistência à mudanças ou incredulidades em relação a possíveis riscos." (JÚNIOR, 2008, p. 16)

Agora que sabemos da importância dessa colaboração e conscientização de todos envolvidos, vem a pergunta: mas o que fazer para conscientizar e informar todo mundo sobre os processos do plano de gestão e como reduzir essa resistência? Aí que está o ponto, o gestor deve elaborar treinamentos para a equipe de TI visando a agilidade na detecção, análise e tratamento de incidentes e obviamente deixando todos afiados em um plano de prevenção de riscos. Essa é uma questão de segurança organizacional e operacional, e todos da equipe devem se empenhar ao máximo para estarem prontos para riscos de qualquer natureza. Além de treinamentos para a equipe de TIC, deverá ser elaborado também campanhas de conscientização dentro da organização, voltada para usuários, contendo orientações, procedimentos básicos de prevenção e o que deverá ser feito e a quem deverá ser reportado caso alguma falha ocorra.

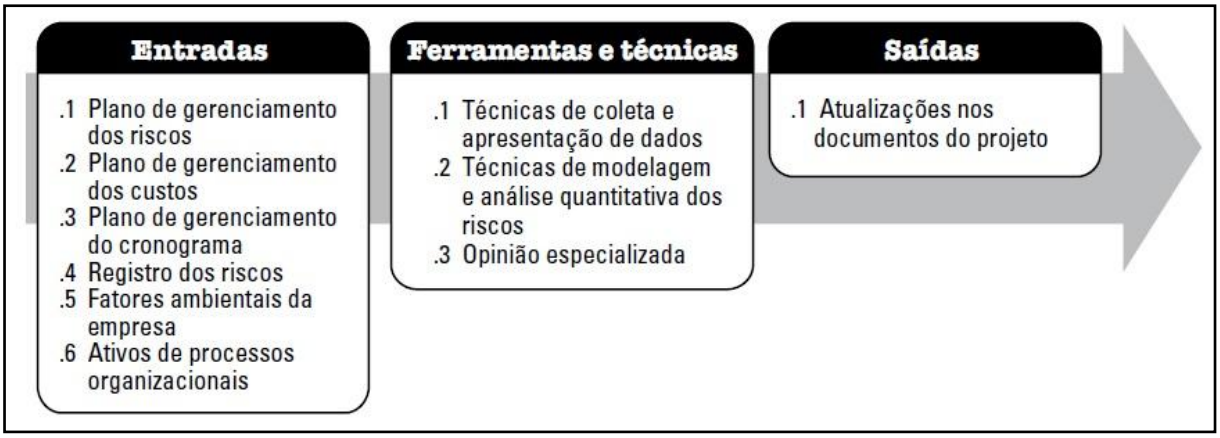
4.2 Mapeamento de Riscos: Análise Quantitativa dos Riscos

A Análise quantitativa dos riscos é o processo onde poderemos calcular qual o valor real do impacto dos riscos no ambiente. Por isso, alguns processos necessitam desse resultado final para obterem suas estimativas, tais quais: metas e cronograma do plano de

gerenciamento de riscos. A principal vantagem da análise quantitativa dos riscos é a redução das incertezas do gestor com relação aos objetivos e as estimativas do plano. Devemos entender que esse tipo de análise só é feita habitualmente nos riscos com prioridade alta, pois envolve muita complexidade no seu cálculo. Agora mostraremos resumidamente as definições de algumas ferramentas que podemos usar na análise quantitativa dos riscos: Análise do valor monetário esperado (VME): decifra em valor monetário o risco para o ambiente; Modelagem e simulação: simula o ambiente em estudo com o objetivo de analisar a probabilidade dos resultados; Análise da árvore de decisão**:** diagrama que adquire uma sentença final baseado na escolha de algumas possibilidades; Análise de sensibilidade: pressupõe quais riscos tem um maior impacto para o ambiente.

A seguir, a Figura 3, mostraremos os processos de entradas e saídas, ferramentas e técnicas da análise quantitativa dos riscos.

Figura 3 – Processos de Análise Quantitativa dos Riscos

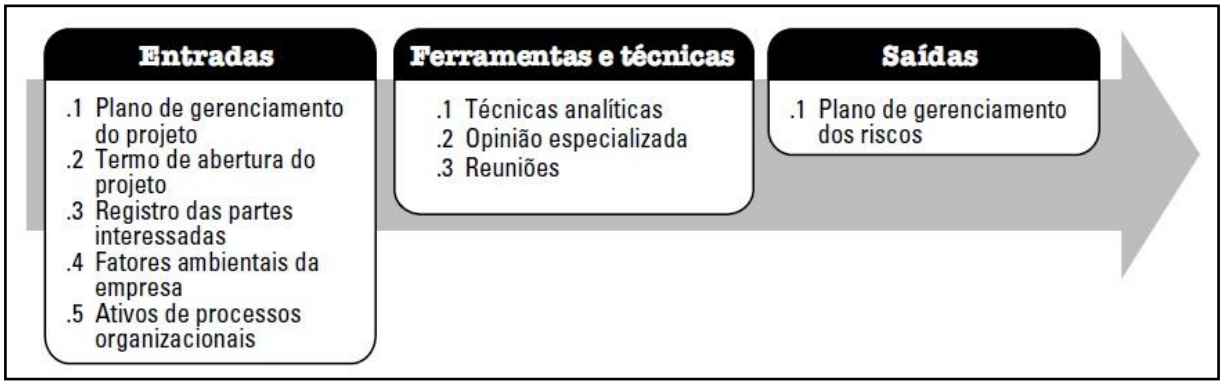


Fonte: Guia PMBOK® (2013)

4.3 Mapeamento de Riscos: Análise Qualitativa dos Riscos

O iminente risco de uma falha ocorrer no ambiente lógico corporativo e o impacto que isso pode causar dentro da organização é um fator de suma importância a ser analisado. Por isso agora veremos a Análise qualitativa dos riscos, que privilegia os riscos com maior probabilidade e impacto e em uma lista secundária deixa os riscos com menor impacto sobre o ambiente. O Guia PMBOK® (2013) nos fala que "O principal benefício deste processo é habilitar aos gerentes de projetos a reduzir o nível de incerteza e focar os riscos de alta prioridade" (PMBOK, 2013). Na figura 4, a seguir, mostramos os processos de entradas e saídas, ferramentas e técnicas da análise qualitativa dos riscos.

Figura 4 – Processos da Análise Qualitativa dos Riscos

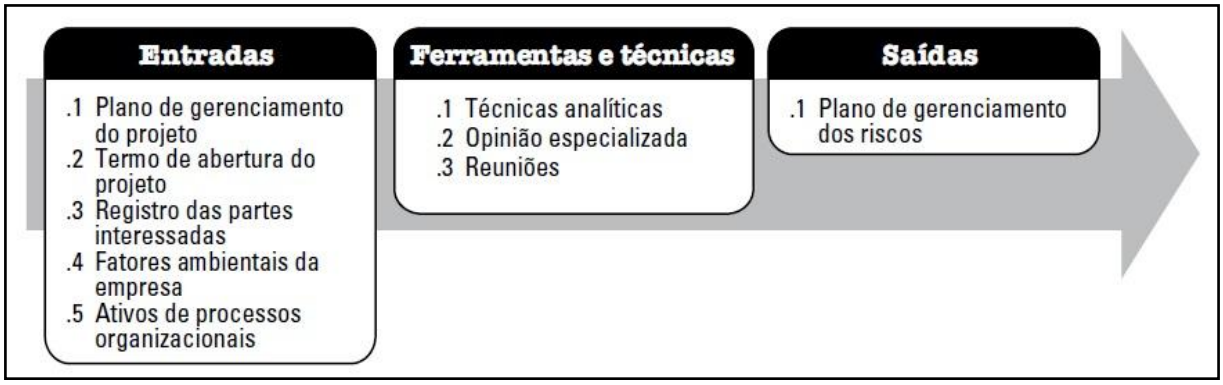


Fonte: Guia PMBOK® (2013)

4.4 Plano de Gerenciamento de Riscos

O Planejamento do gerenciamento de riscos é o pontapé inicial da análise e minimização de riscos. O plano de gestão de riscos é o processo que determina o método de como analisar e realizar as demandas ofertadas pelo gerenciamento de riscos dentro do ambiente corporativo. O guia *Project Management Body Of Knowledge* (PMBOK®, 2013) define a conexão entre os processos do plano de gerenciamento de riscos em: entradas, saídas, ferramentas e técnicas. Entradas e saídas são documentações e artigos em geral que abrangem o projeto. Ferramentas e técnicas são parâmetros utilizados nas atividades exercidas dentro do projeto. A seguir, na figura 5, podemos notar essas entradas, saídas, ferramentas e técnicas do plano de gerenciamento de riscos.

Figura 5 – Processos do Planejamento do Gerenciamento de Riscos



Fonte: Guia PMBOK® (2013)

5 VALIDAÇÃO DA SOLUÇÃO

5.1 Exemplo de Implementação da Solução

Nesse momento validaremos a pesquisa, mostrando a solução implementada, em um case fictício, que inicialmente demonstrará o problema, a solução e os resultados esperados dentro do ambiente criado.

5.1.1 O Problema

Uma empresa de assessoria jurídica, de porte médio, necessita de uma solução para proteger seus dados de terceiros, pois lida constantemente com processos classificados como “segredo de justiça”. A preocupação com o possível vazamento de informações ou iminentes perca de dados, levou a equipe de TI a sugerir para alta diretoria da empresa a implementação de um plano diretor de segurança da informação e de ferramentas que auxiliem no processo de tomada de decisão e no gerenciamento de falhas de segurança. A empresa possui em média 500 colaboradores e um fluxo de movimentação de dados muito grande, por isso o receio por possíveis problemas na segurança dessas informações. Com cerca de 30 filiais espalhadas em todo o estado na qual a organização atua, há a necessidade de maior certeza que os dados transportados entre as filiais cheguem sempre íntegros e seguros em seus respectivos destinos. Com todo esse cenário de incerteza e desconfianças, a alta administração resolveu tomar uma atitude e enfim contratar uma empresa de consultoria em segurança da informação, para que houvesse a implementação de ferramentas e *frameworks* que auxiliassem os gestores de TI.

5.1.2 A Solução

Primeiramente, para que ocorra a mitigação de falhas, é necessário preocuparnos com a prevenção e antecipação de falhas, para isso utilizaremos o plano de prevenção de riscos, como primeiro item a ser implementado na solução proposta.

Plano de Prevenção de Riscos: Sabemos que uma equipe bem treinada e colaboradores conscientes e empenhados, em prol da seguridade dos dados, com certeza haverão bons frutos, mas para isso é preciso um plano diretor de segurança da informação bem detalhado e específico. Com a ISO/IEC 27002, que tem como principal objetivo nortear as regras para implementação e melhoria contínua da segurança da informação, a equipe de TI terá uma fonte de informação rica de procedimentos e orientações para que o plano diretor de segurança previna e diminua o impacto de riscos. Inicialmente a ISO poderia ser um guia para a implementação do plano diretor pela empresa de consultoria, mas posteriormente a empresa poderia validar as práticas com uma certificação ISO 27002, dando mais credibilidade para a

segurança da informação na TI.

Anteriormente, citamos o plano de gerenciamento de riscos como pontapé inicial de uma boa gestão de segurança da informação, então nesse momento faremos uso do mesmo como segundo item da nossa solução.

Plano de Análise e Gerenciamento de Riscos: Agora que a empresa possui um plano diretor de segurança da informação é necessário partir para um plano que gerencie possíveis e iminentes falhas. A consultoria em segurança usará o PMBOK, que por ser uma guia de gerenciamento de projetos, também possui um processo dedicado apenas para gerenciamento de riscos e isso será de grande valia para os gestores. Além disso, será usado também o COBIT 5, que melhorará de forma contínua os processos de TI e de gerenciamento de riscos, mantendo um padrão de qualidade para os mesmos. É recomendando que na parte da análise de riscos seja usado o método de Análise Qualitativa do Riscos, estudado anteriormente em outro tópico, pois o mesmo previlegia riscos com maior probabilidade de ocorrer, o que será mais valioso para o este cenário. De grande importância, também deverá ser usado o *RISK IT*, ferramenta importantissíma no gerenciamento dos riscos, que por sua vez será usada para gestão e análise riscos em geral. Por último, mas não menos importante, O *VAL IT*, será usado para alinhar os investimentos e os as normas de gerencimanento com os negócios da empresa. Usando essas ferramentas específicas, como solução para cada um desses problemas, os resultados com certeza serão extremamente satisfatórios.

É sempre importante entender, que por mais cuidado que seja um plano de gestão de riscos, há sempre a possibilidade de ocorrer uma falha. Por isso é muito importante estar bem preparado e treinado para essas situação. Por esse motivo nesse momento utilizaremos o plano de contigência como parte final da nossa solução.

Plano de Contigência: Agora que temos um plano de prevenção e de gestão de riscos é necessário um plano, para saber o que fazer quando alguma dessas falhas ocorrer. A equipe de implementação deverá elaborar uma cartilha que oriente usuários de como proceder caso ocorro algum risco. Também deverá ser elaborado planos de contigências em vários níveis de riscos, para auxiliar colaboradores de TI na tomada de decisão nesses momentos. Com o uso da ISO/IEC 27002 (estabelece orientações para a gestão de riscos) e do *RISK IT*, será mais fácil elaborar e gerenciar esses planos de contigência, por isso o ponto deve ser sempre o uso dessas ferramentas na elaboração desses planos.

5.1.3 Resultados

É necessário também fazer um levantamento de resultados dentro da organização, fazendo relatórios trimestrais para saber riscos eliminados, que mais ocorreram e o nível de satisfação de usuários, afim de validar a solução apresentada pela empresa de consultoria. Com esse levantamento teremos uma base para saber onde deverá ser centrado o foco e onde todo plano de segurança da informação mais obteve sucesso. Com o uso a risca de todas essas ferramentas e bibliotecas aqui mencionadas, com absoluta certeza serão colhidos bons resultados e o nível de satisfação dos usuários deverá ficar entre 75% a 95%.

5.2 Cases de Sucesso

Agora que já vimos as definições, conceitos, vantagens e metódos dos frameworks e exemplos de implentações, é hora de apresentar alguns resultados em ambientes reais. Apresentaremos dois *cases* que obtveram êxito na implementação do gerenciamento de riscos. Usaremos um exemplo em TI e outro no setor de Construção, para ressaltar que a importância do gestão de riscos não tange apenas a área de tecnologia, mas também qualquer área que possua o mínimo de vunerabilidades ou exposição a falhas.

TEREX Roadbuilding Latin America: A TEREX é uma multinacional, presente em boa parte da américa latina, e trabalha no ramo de construção de equipamentos diversos para construção, mineração, portos, infraestrutura e outros. Hoje, com mais de 50 anos de mercado, faz parte das três maiores do mundo em sua segmentação. Com toda essa grandiosidade da empresa, é possível imaginar a gama de informações e o fluxo de dados que o data center engloba. Foi pensando nisso que a TEREX resolveu tomar uma atitude e contratar uma consultoria que implementasse uma gestão de riscos, para ascender os níveis de segurança da informaçao e que se alinhasse as necessidades de mercado e produção da empresa. A TI SAFE, empresa especializada em segurança da informação, entrou em ação e fez um plano de gerenciamento de riscos para a TEREX, com mapeamento de riscos e plano de contigência bem traçado. Isso foi possível com uma série de entrevistas e sabatinas, com funcionários da empresa para adquirir o máximo possível de informações da atual, tais como controles de segurança, requisitos de segurança e etc. Com isso o resultado foi extremamente satisfatório e hoje a empresa conta com outra realidade em gestão de riscos. Hoje é utilizado o SE Riscos da SoftExpert, para gerenciar e controlar as diversas vunerabilidades que foram descobertas. Foram criados também, 5 planos de gerenciamento e contigência de riscos com uma gama de opções de execução.

UTC Engenharia S.A: A UTC é uma grande empresa de engenharia brasileira, com mais de 40 anos de mercado e consolidada em seu segmento. A empresa resolveu inovar, afim de envolver todos os profissionais no gerenciamento de riscos. Foi desenvolvido o Planejamento Operacional 3D - Barreiras Quebradas para Antecipação de Perigos e Riscos. Trata-se de uma inovadora ferramenta que visualiza toda a obra em 3 dimensões, expondo todo o projeto e visualizando riscos em potencial. Resultados? Houve 90% de redução da exposição de colaboradores a riscos nas obras, pois além de gerenciar o ambiente, a ferramenta auxilia na montagem de peças. Riscos em geral foram neutralizados e podem ser gerenciados diretamente por qualquer pessoa com acesso a ferramenta. E para finalizar, o processo foi imensamente reconhecido, vencendo o Prêmio Proteção Brasil 2012 na categoria gerenciamento de riscos.

6 CONCLUSÕES

Ao longo do trabalho, foi possível fazer uma análise objetiva de frameworks de gerenciamento de riscos, além de algumas bibliotecas comumente usadas por gestores de TI no auxílio da tomada de decisão. No desenvolvimento da pesquisa foi buscado a conscientização de colabores, diretores, líderes e gestores que possuam algum envolvimento com segurança da informação. Focamos nessa parte, pois é um dos objetivos do trabalho, e como dito anteriormente, um ponto importantíssimo para o colhimento de bons resultados.

A importância de cada *framework*, de cada ferramenta e método, foi devidamente mostrada de forma objetiva e sucinta, pois o modelo do trabalho não permite um estudo mais aprofundado e detalhista. Os resultados expostos na pesquisa foram muito satisfatórios, pois mostraram que o gerenciamento de riscos não é fundamental apenas em tecnologia, mas em qualquer segmento. Ferramentas inovadoras como o Planejamento Operacional 3D da UTC Engenharia, mostraram que todos os colaboradores envolvimentos nos processos da empresa, podem contibruir e gerenciar riscos em potencial. A TEREX, por sua vez, nos mostrou a importância de implementar um plano de gerenciamento de riscos, com diversas contingências, e uma ferramenta de gerenciamento bem alinhada aos negócios da empresa.

Com a pesquisa bibliográfica, conseguimos filtrar de diversos autores, artigos e publicações bons argumentos e ideias, que comungam com os objetivos do trabalho. Sendo assim, confirmamos a devida relevância da pesquisa e a devida importância das ideias tanto no âmbito acadêmico quanto no profissional.

Dada à devida relevância do assunto trabalhado, fica a necessidade de um estudo mais detalhado sobre o tema, podendo haver um estudo de caso com um ambiente real ou até mesmo a confirmação dos resultados de meios de novos métodos de implementação desenvolvidos por outros autores. Podemos até mesmo, sugerir o desenvolvimento de uma ferramenta simples e de boa usabilidade, que qualquer usuário possa manusear, baseada em COBIT e no PMBOK, que auxilie usuários e gestores de TI na tomada de decisão e na melhoria do gerenciamento de riscos dentro da segurança da informação.

RISK MANAGEMENT IN INFORMATION SECURITY: An Analysis of Frameworks Based on COBIT[2]

Felipe Dias Corrêa

Abstract: This article aims to focous on aspects of management of risks that guide the logical security of organizations. The study aims to present solutions and tools for minimizing failures in IT environments, using risk management frameworks as a guide. In order for these goals to be successful, the author will use as references, articles and authors that contributed significantly to the topic, as well as using risk management frameworks and the powerful COBIT® governance library 5. Throughout the study, it will also be cited some cases of success in implementing risk management in real environments. Finally, the study will show the importance of risk management for organizations, as well as the relevance that the research may have, contributing satisfactorily to IT companies, organizations and managers, as a means of raising awareness or a method for applying these practices.

Keywords: *Risk Management. Security. Frameworks.*

[2] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Governança de Tecnologia da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Governança de Tecnologia da Informação.

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Código de Prática para a Gestão da Segurança da Informação**. Rio de Janeiro, 2005.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Gestão de Risco da Segurança da Informação**. Rio de Janeiro, 2008.

BUCCI, Antônio. **Gestão de Riscos e o COBIT 5 para Segurança da Informação.** Grupo Treinar, 12/08/2012. Disponível em: <www.grupotreinar.com.br/blog/2012/8/12/gestão-de-riscos-e-o-cobit-5-para-segurança-da-informação.aspx> Acesso em: 04 Nov, 2016.

ISACA. **COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização.** Illinois, EUA. 2012.

JÚNIOR, A. G. **Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação e Comunicação - abordagem prática para conscientização e implantação nas organizações.** Porto Alegre, 2008.

MACÊDO, D. **Gestão de Riscos**. 21/08/2012. Disponível em: <www.diegomacedo.com.br/gestao-de-riscos/> Acesso em: 08 Abr, 2017.

OLIVEIRA, M. **Val IT Framework – Retorno de Valor em Seus Investimentos de TI.** 03/11/2016. Disponível em: < www.redbelt.com.br/blog/2016/11/03/val-it-framework-roi/> Acesso em: 08 Abr, 2017.

OLIVEIRA, T. **Resumo do Risk IT Framework.** 18/11/2011. Disponível em: <blog.thalissonoliveira.com.br/?p=551> Acesso em: 08 Abr, 2017.

PMI. **Um guia do conhecimento em gerenciamento de projetos. GUIA PMBOK® 5ª ed.** EUA: Project Management Institute, 2013.

REIS, Luís C. D., NETO, Elias F. N. ***Risk IT Based On COBIT*: Uma visão sistêmica para auditoria de TI.** CNASI, 28/05/2012. Disponível em: <www.cnasi.com.br/risk-it-based-on-cobit-uma-visao-sistemica-para-a-auditoria-de-ti> Acesso em: 04 Nov, 2016.

SILVA, Pedro J. S. **Análise de Riscos de Segurança da Informação para a Administração Pública Federal: Um Enfoque de Alto Nível Baseado na ISO/IEC 27005**. Brasília, 2009.