UMA ANÁLISE COMPARATIVA NA UTILIZAÇÃO DE UM PLANO DE CONTENÇÃO DE RISCOS DA SEGURANÇA DA INFORMAÇÃO BASEADO NA NORMA ISO/IEC 27005:2008 E NO *FRAMEWORK RISK IT BY ISACA*

Homero Mckinley Falcão Ferreira[1]
Ricardo Bemardes de Mello[2]

RESUMO

A informação é o ativo mais importante no universo das empresas; seja pública ou privada, percebe-se a falta de estrutura do universo corporativo para lidar com a segurança das suas informações. A falta de conhecimento das vulnerabilidades e ameaças e, consequentemente, o despreparo para os impactos negativos que venham a ocorrer por eventos não esperados, evidenciam a necessidade, que se faz fundamental, da implantação de uma política de gestão de segurança pautada em um Plano de Continuidade do Negócio, bem como um Plano de Controle e Contenção de Riscos. A associação desses dois documentos com aplicações e controles bem definidos proporciona para a empresa um cenário mais estável, contribuindo para decisões importantes na esfera da Governança e da Gestão da Segurança da Informação (SGSI). O presente artigo segue a metodologia de revisão bibliográfica e tem o objetivo de mostrar as particularidades dos modelos supracitados, proporcionando ao leitor uma visão mais refinada da ISO 27005 e do *framework RISK IT*, elucidando suas semelhanças e diferenças de utilização, o que contribuirá para decisão do modelo a ser implantado em determinada empresa.

Palavras Chave: Gestão de Riscos. ISO/IEC 27005:2008. ISACA. Gestão da Segurança da Informação.

1 INTRODUÇÃO

Este trabalho aborda, de forma ampla, o assunto Gerenciamento de Riscos da Segurança da Informação, analisando e comparando as duas principais documentações existentes no mercado atual, a ISO 27005 e *o RISK IT by ISACA.*

Na atualidade, é de comum consentimento que o assunto Riscos deve ser abordado em qualquer empresa que almeje implantar os princípios mínimos da Governança Corporativa; no entanto, o que se tem percebido, principalmente no Brasil, é que as Organizações simplesmente não abordam tal assunto, seja por desconhecimento, falta de interesse ou até mesmo por falta de se conseguir, dentro do mercado, pessoal especializado para tal ação (CASACA, 2014).

[1] Engenheiro Mecânico-UPE, MBA em Governança de TI - Estácio de Sá, COBIT 5, Pós em Governança de TI – UNIS/ILA. Email: homero@comar2.aer.mil.br, mck.homero@gmail.com.
[2] Professor orientador, mestre em Sistemas de Produção Agropecuária na Unifenas, pós-graduado em Banco de dados e Gestão de TI e graduado em Ciência da Computação, ambos pelo Unis MG. Email: ricardo@unis.edu.br

É salutar lembrar que a abordagem do assunto Riscos é um componente necessário no segmento de TI, mostrando os benefícios da utilização de um Gerenciamento contínuo nesse segmento, evitando, assim, surpresas inesperadas que trarão prejuízos das mais diversas formas, financeiros e estruturais, seja para empresas públicas ou privadas. Com isso, é importante observar que a confecção e utilização de um PCR é de vital importância para a Governança de TI. E, em cima desse princípio, no decorrer deste artigo, detalhar-se-á, de forma ampla, dois dos principais modelos utilizados no mercado, com o intuito de contribuir na escolha de implantação da metodologia mais adequada.

Ainda dentro do contexto anterior, descreve-se abaixo exemplos de alguns prejuízos causados pela a ausência da implantação e controle de uma política de risco, seriam eles (CASACA, 2014):

a) Possibilidade de sofrer perdas, reduzindo o valor de negócio;
b) Eventos com possibilidade de causarem perdas e danos;
c) Incerteza inerente a fazer negócios;
d) Incerteza nos desempenhos dos resultados correspondentes;
e) Realização potencial das consequências.

Sendo assim, a finalidade deste estudo é comparar, a partir das duas principais documentações supracitadas, os benefícios na utilização de cada uma das metodologias para a implantação dentro das empresas de um Plano de Gerenciamento de Riscos da Segurança da Informação, proporcionando aos interessados uma maior exploração sobre a questão de como se tratar a Gestão de Riscos no contexto da Segurança da Informação em determinados ambientes; oferecendo, assim, informações que possam contribuir para a criação ou aprimoramento da Gestão de Risco da SGSI (Sistema de Gestão de Segurança da Informação).

Para tanto, este artigo segue a metodologia de revisão bibliográfica, a partir da qual identificou-se variáveis de utilização de um Plano de Riscos em SGSI.

2 ISO/IEC 27005:2008

A norma internacional ISO/IEC 27005 é parte da família de normas da ISO/IEC 27000, a qual define uma série bem estruturada de documentações que se referem à gestão de segurança da informação, e são utilizadas em todo o mundo. Elas têm o perfil de poderem ser utilizadas em toda a empresa ou apenas em parte delas, em uma aplicação de TI ou em uma infraestrutura de TI (BECKERS et al, 2011). Essa norma internacional fornece diretrizes e controles para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI).

Expõe-se, aqui, as fases: contexto, análise, tratamento, aceitação e comunicação dos riscos, que devem ser seguidas para a análise e implantação de uma Gestão de Riscos eficiente, referente ao sistema de Segurança da informação. Vale ressaltar, na ISO em questão, a importância dos seis anexos (A, B, C, D, E, F), que são essenciais para o estudo e implantação da Gestão de Riscos.

Anexos esses que não analisaremos detalhadamente (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

São eles:

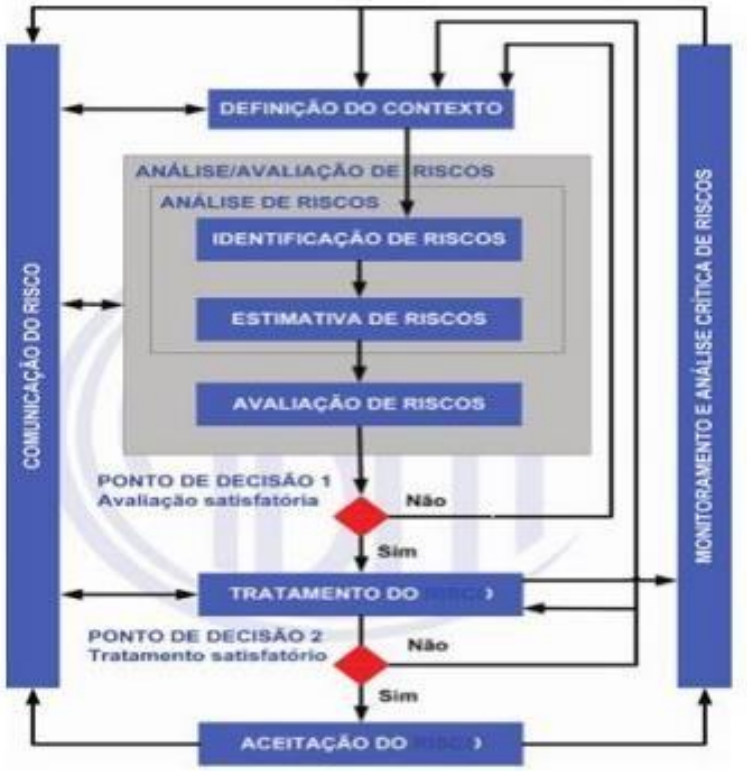
a) Anexo A: Definindo escopos e limites do processo;
b) Anexo B: Identificando a valoração dos ativos a avaliação do impacto;
c) Anexo C: Exemplo de ameaças comuns;
d) Anexo D: Métodos para avaliação de vulnerabilidades técnicas;
e) Anexo E: Diferentes abordagens para análise/avaliação de riscos do SGSI;
f) Anexo F: Restrições que afetam a redução dos riscos.

A ISO 27005 define o processo de Gestão de Riscos como atividades coordenadas para gerenciar o risco em uma organização (LUND; SOLHAUG; STOLEN, 2010). Nesse contexto, ALBERTS (2006) descreve os riscos apresentados em quatro fases:

a) Contexto: ambiente em que o risco é analisado e influencia a avaliação das consequências;
b) Ação: ato ou evento que desencadeia o risco (sem ação não há a existência do risco);
c) Condição: estado atual ou o conjunto de circunstâncias que podem conduzir aos riscos;
d) Consequências: resultados potenciais ou efeitos de uma ação combinada com uma determinada condição.

Abaixo segue figura 1 com o roteiro desejável, segundo a ISO 27005:2008, para análise e tratamento dos riscos:

Figura 01 – Processo de Gestão de Riscos da Segurança da Informação



Fonte: (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008, p 5)

Pode-se perceber que a norma em questão segue etapas bem definidas com riqueza de detalhes. Destaca-se que esse é um processo contínuo, e que todos os pontos devem ser considerados com extrema cautela; caso contrário, não constituiremos um plano relevante no contexto da Segurança da informação (KOZEN; FOUNTOURA; NUNES, 2012).

Seguindo as etapas para a construção de um PCR da ISO 2007, como na figura 1, relata-se (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008):

> Que em um SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco, fazem parte da fase "planejar". Na fase "executar" do SGSI, as ações e controles necessários para reduzir os riscos para um nível aceitável são implementadas de acordo com o plano de tratamento do risco; na fase "verificar" do SCSI, os gestores determinarão a necessidade de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase "agir", as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação.

Na figura 2, resumem-se as atividades relativas à Gestão de Riscos em quatro fases, o que possibilita ver a semelhança com o ciclo PDCA (*Plan-Do-Check-Adjust*), a consequente continuidade que precede um Plano de Riscos bem elaborado (CASACA, 2014).

Figura 02: Alinhamento do Processo do SGSI e do processo de Gestão de Riscos de Segurança da Informação

Fonte: PDCA (SHEWHART, 1930).

Nos próximos tópicos serão analisadas as principais entradas, saídas e ações das fases do processo de Gestão de Riscos da Segurança da informação com maior especificidade.

2.1 Definição do contexto

Essa é a fase em que serão definidos os escopos e limites que serão levados em consideração. Deverão ser identificados os ativos realmente importantes para a organização. Também nessa fase devem se determinar os critérios para a aceitação e as respectivas responsabilidades no que diz respeito à SGSI (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

Convém ressaltar que é essencial determinar o propósito do Plano, pois afetará em geral a definição do contexto. Esses propósitos podem ser (ARAÚJO, 2012):

a) Suporte a um SGSI
b) Conformidade legal e a evidência da realização dos procedimentos corretos
c) Preparação de um plano de continuidade de negócios
d) Preparação de um plano de resposta a incidentes
e) Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

2.2 Análise/avaliação de riscos

Assim como na ISO/IEC 31000, a análise de riscos será subdivida em duas fases:

a) Análise dos Riscos;
b) Identificação de riscos.

Nessa fase, será necessário identificar todos os prováveis riscos existentes que interfiram diretamente no funcionamento dos serviços utilizando ferramentas já pré-estabelecidas. É importante pensar em todas as possibilidades, inclusive as mais banais, além de relevar questões como a conscientização de funcionários, por exemplo. O universo é amplo e não é uma tarefa fácil. Assim, a divisão em categorias pode facilitar o trabalho, por exemplo, internos e externos. Posteriormente, a identificação final deverá ser validada junto à direção. E, finalmente, passa-se à fase adiante (ARAÚJO, 2012): Estimativa de riscos.

Nessa fase, usam-se metodologias para a estimativa dos riscos, listadas no item anterior, baseadas em análise qualitativa ou quantitativa; que são verificadas levando-se em conta o contexto da probabilidade de incidentes e suas consequências (ARAÚJO, 2012).

2.2.1 Análise de riscos

Eis uma questão que necessita de tempo para a constituição do que viria a ser um “Banco de dados” dos riscos pertinentes às atividades fim da empresa. Essa é uma fase que deve ser feita

com extrema cautela e o maior preciosismo possível, pois nela, possivelmente, estarão os vetores que decidirão o destino da empresa no mercado, em ocasião de incidentes não esperados (CASACA, 2014).

Cabe também destacar que, assim como a ISO/IEC 31000, as ferramentas para identificação dos riscos são similares e envolvem políticas de coletas de dados, entrevistas, análise de históricos, entre outros. Exemplos (ARAÚJO, 2012):

1. Análise de documentação;
2. Técnicas de coleta de dados;

1. Brainstorming
2. Técnica de Delphi
3. Técnica de Grupo Nominal
4. Entrevistas
5. Pontos fortes e fracos (Matriz de SWOT)

3. Listas de verificação;
4. Análise de premissas;
5. Técnicas de diagramação;
6. Informações históricas.

Assim como na identificação dos riscos, é nesta fase que será construída uma Matriz de Riscos, seja ela quantitativa ou qualitativa, que seguem as seguintes definições:

a) Qualitativa: A Análise Qualitativa de Riscos, através da metodologia desenvolvida pela Organização, permite classificar o nível de riscos do SGSI, mesmo antes de se ter em mãos dados quantitativos (ARAÚJO, 2012).
b) Quantitativa: A Análise Quantitativa de Riscos avalia os impactos e quantifica a exposição do SGSI aos riscos por meio da atribuição de probabilidades numéricas a cada um e aos seus impactos sobre os objetivos da empresa (ARAÚJO, 2012):

Seguem, nas figuras 3 e 4, exemplos de Matrizes de Riscos que, por observação, podem ser adaptadas ao cenário particular da organização em estudo, lembrando que é uma ferramenta que, se bem dimensionada e exposta em local comum, trará para todos os componentes da equipe uma visão macro da diferenciação quanto ao impacto do incidente ora listado na matriz (ARAÚJO, 2012):

Quadro 01– Exemplo de uma Matriz de Riscos com dados Qualitativos

PROBABILIDADE	**ANÁLISE QUALITATIVA**				
Muito Alta	MA / MB	MA / B	MA / M	MA / A	MA / MA
Alta	A / MB	A / B	A / M	A / A	A / MA
Média	M / MB	M / B	M / M	M / A	M / MA
Baixa	B / MB	B / B	B / M	B / A	B / MA
Muito Baixa	MB / MB	MB / B	MB / M	MB / A	MB / MA
IMPACTO	**Muito Baixo**	**Baixo**	**Médio**	**Alto**	**Muito Alto**

Fonte: (Manual de Gestão de Riscos)

Quadro 02 – Exemplo de uma Matriz de Riscos com dados Quantitativos

VME (Valor Monetário esperado) = P * Impacto a Margem

VME		
Percentual de Margem		**Classificação**
De	**Até**	
0,00%	0,50%	Baixo
0,50%	3,00%	Moderado
3,00%	100%	Crítico

Fonte: (Manual de Gestão de Riscos)

2.2.2 Avaliação dos riscos

Fase em que todas as coletas de dados dos itens anteriores serão ordenadas conforme seus critérios de aceitação definidos pela empresa (CASACA, 2014).

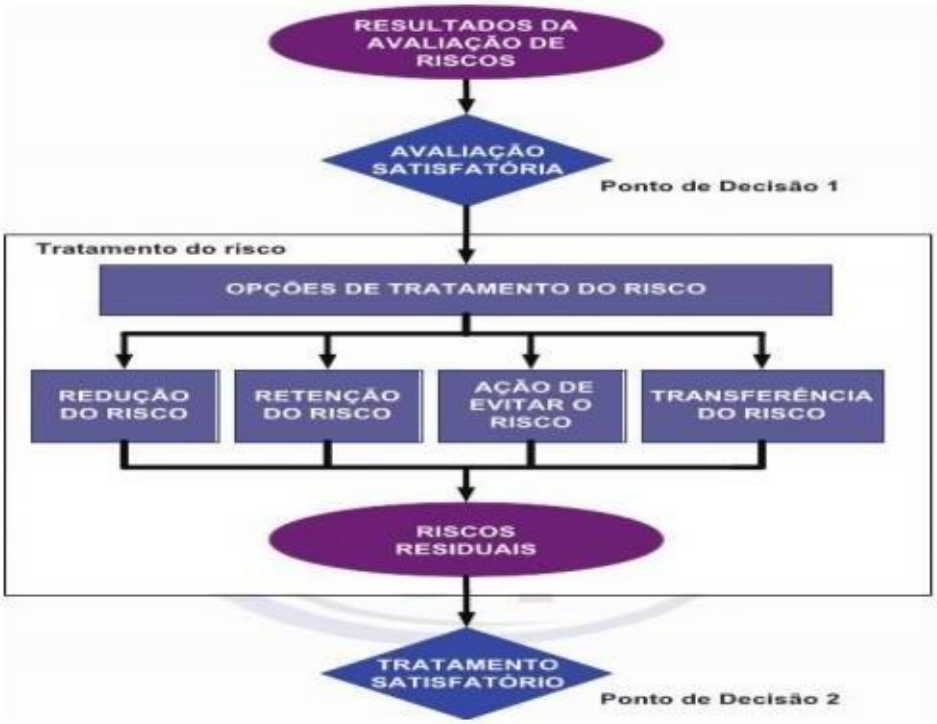
2.3 Tratamento dos riscos

Uma vez que todo o processo for elaborado, é o momento de definir que tipo de ação (tratamento) será acionado na ocasião do surgimento de um incidente. É imprescindível que as decisões estejam alinhadas ao negócio e que resultem no menor dano estimado possível para o funcionamento da empresa (ARAÚJO, 2012).

Mais especificamente sobre o SGSI, onde serão criados blocos de níveis de segurança, evidencia-se o acréscimo de medidas preventivas (controle de acessos físicos, lógicos, etc.) e, se mesmo assim, os intrusos obtiverem êxito, o tempo de resposta será de vital importância (CASACA, 2014).

A figura 5 abaixo descreve, de forma clara, o processo de abordagem e os tipos de tratamentos de riscos, segundo a ISO/IEC 27005:

Figura 05 – Processo de Tratamento de Riscos da Segurança da Informação



Fonte: (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008, p 18)

Cabe lembrar que é considerável que a equipe responsável por todo o processo tenha velocidade e maturidade suficiente para pronta resposta no caso de incidentes, bem como tenha um canal de comunicação junto à administração superior para tomar decisões rápidas e eficazes, como no caso da aceitação dos riscos, e que saiba tratar de forma adequada os riscos residuais, quando houver, evitando assim desperdício financeiro com riscos de pouco impacto (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

2.4 Aceitação do risco da segurança da informação

Nessa fase, não há muito que se definir, pois a aceitação significa que não se criará nenhum plano para tentar evitar ou mitigar o risco, preferindo aceitar as suas consequências, ou que a equipe

não conseguiu elaborar nenhuma estratégia adequada de resposta e não tem alternativa senão lidar com o risco e seus respectivos prejuízos no que se refere à SGSI (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

2.5 Comunicação do risco da segurança da informação

Os processos de comunicação, já tratados anteriormente e não menos importantes, devem estar bem descritos, inclusive, bem informados e exemplificados para os responsáveis, como todo o processo hierárquico de comunicação funcionará no caso de um incidente; haja vista que, quando se trata do ativo informação, o tempo é fator preponderante para se tomar ações no mínimo mitigadoras (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

2.6 Monitoramento e análise crítica dos riscos de segurança da informação

O monitoramento e análise crítica contínua são essenciais para assegurar que o plano de Gestão de Riscos da Segurança da Informação se mantenha eficiente e eficaz. As probabilidades e impactos de cada risco ou suas respectivas oportunidades podem mudar com o tempo, bem como seus custos de tratamento. Por isso, é necessária uma revisão no mínimo anual do ciclo da Gestão de Riscos do SGSI, que segue os mesmos padrões do PDCA (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

Extraídas do manual de Gestão de Riscos, baseado na ISO/IEC 31000, são apresentadas questões substanciais que devem fazer parte do questionário de monitoramento:

Para os riscos que aconteceram:

1. *As ações tomadas foram eficazes?*
2. *Qual foi o valor medido?*
3. *Quais as lições aprendidas?*

Para riscos que não aconteceram

1. *A probabilidade ainda é a mesma?*
2. *O impacto ainda é o mesmo?*
3. *Ainda é tempestivo?*
4. *As ações planejadas estão sendo executadas?*

Importância do monitoramento

1. *Identificação de novos riscos / oportunidades*
2. *Eliminação dos riscos que não mais se aplicam*
3. *Reclassificação dos riscos restantes onde a probabilidade ou o impacto mudou*

O questionário descrito acima tem o objetivo de colher dados que irão, assim que solidificados, contribuir de maneira significativa para as decisões do Corpo Diretivo.

2.6 Framework *risk it By ISACA*

Outra ferramenta para a confecção do PCR é o *framework RISK IT by ISACA,* lançado em 2009, e que vem sendo adotado pelas empresas devido à sua integração com o *framework COBIT (Control Objectives for Information and related Technology),* de Governança de TI também pertencente à ISACA (NETO, REIS, 2015).

Definindo a palavra *framework* como Estrutura Lógica, o COBIT é hoje a ferramenta mais utilizada na implementação de uma governança sólida alinhada ao negócio. Seus benefícios são visíveis para a organização e o *RISK IT* vem para complementar de forma extensa uma pequena lacuna na Gestão de Riscos, que é um dos princípios de Governança do COBIT, bem lembrado no seu processo de governança EDM03, dentro dos contextos de Avaliar, Direcionar e Monitorar (*Evaluate, Direct and Monitor*). (NETO, REIS, 2015).

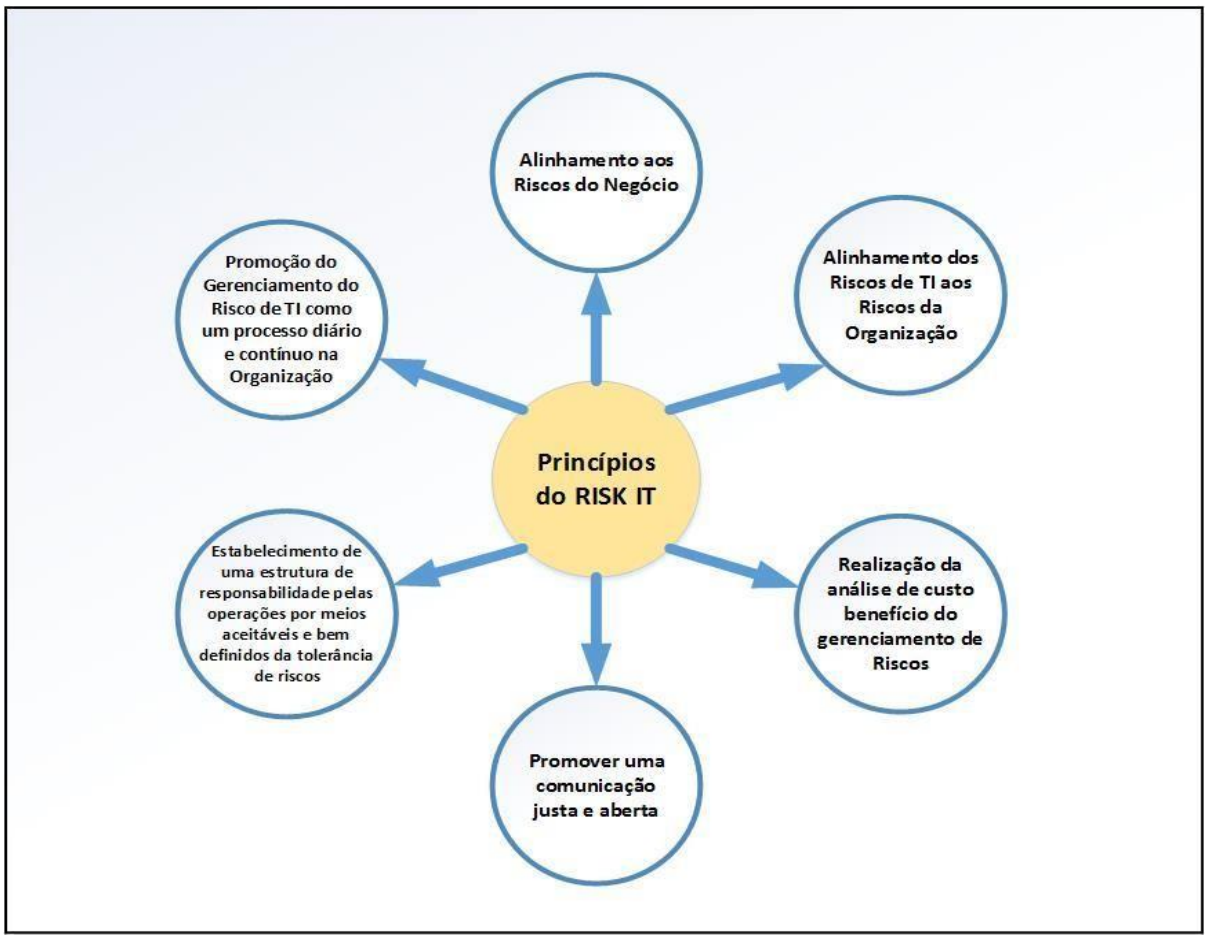
A vantagem visível na utilização desse modelo é a sinergia apresentada na relação com as demais ferramentas da ISACA, que descreve de uma maneira bem clara "como fazer", desde a identificação até o monitoramento dos Riscos de TI (NETO, REIS, 2015).

O *framework* é bem extenso e está delineado em 46 processos, os quais não serão detalhados neste artigo. No entanto, cabe um estudo mais aprofundado para analisá-los um a um, mesmo sabendo que cada caso é um caso, e que não necessariamente precisar-se-á utilizar todos os processos disponíveis (NETO, REIS, 2015).

Os princípios do *RISK IT* são objetivos e práticos na sua abordagem e abrangem, dentro do possível, toda a estrutura que se deseja quando o assunto é Riscos (ISACA, 2009)**.** São eles (ISACA, 2009):Alinhamento aos Riscos do Negócio;

a) Alinhamento dos Riscos de TI aos Riscos da Organização;
b) Realização da análise de custo/benefício do gerenciamento de Riscos;
c) Promover uma comunicação justa e aberta do Risco TI;
d) Estabelecimento de uma estrutura de responsabilidade pelas operações por meios aceitáveis e bem definidos de tolerância de Riscos;
e) Promoção do gerenciamento do Risco de TI como um processo diário e contínuo na vida da Organização.

Figura 06 – Princípios do *RISK IT*



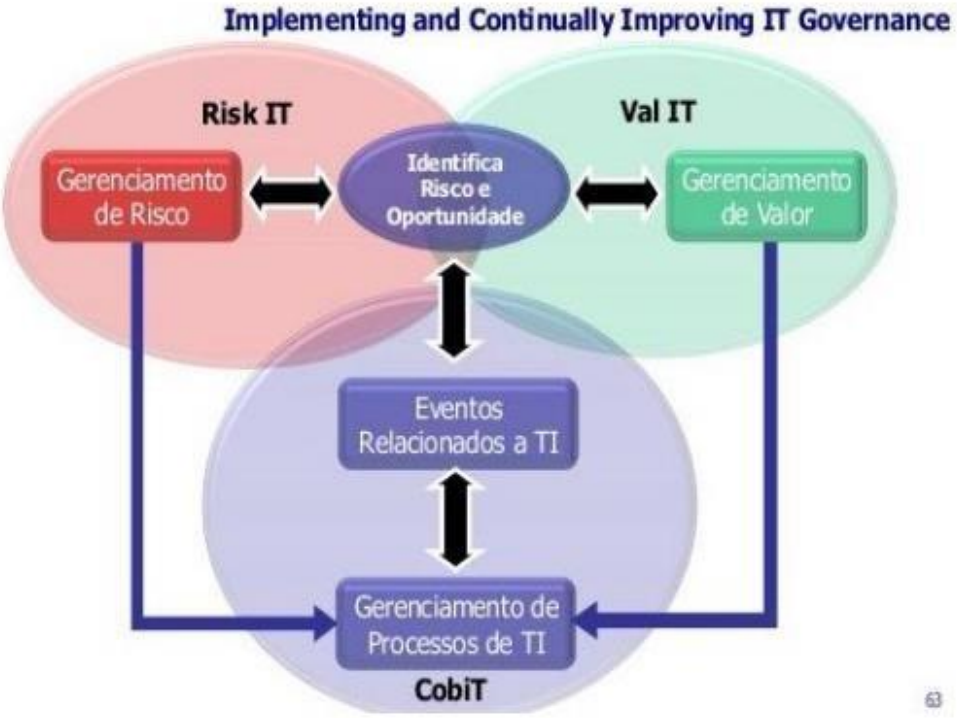
Fonte: (ISACA, 2009, *RISK IT*)

A grande diferença entre o *RISK IT* e as outras ferramentas está no conceito do *Risk Governance* ou no alinhamento com o negócio dos riscos inerentes a TI com todo o resto dos riscos corporativos (SANTOS, 2009).

Essa integração proporciona uma visão mais ampla de todos os processos existentes, como eles se interligam e, consequentemente, uma visão mais clara dos riscos existentes e dos "riscos ocultos" que aparecem exatamente na intersecção desses processos. Essa é uma vantagem inegável a ser considerada na hora da eleição de um padrão a ser utilizado nos tratamentos de riscos inerentes à tecnologia da informação (CASACA, 2014).

Ainda em relação à sinergia do *RISK IT* com o COBIT 5 e com o VAL IT (Geração de Valor), exibe-se, na figura abaixo, essa integração:

Figura 07 – Intersecção entre os frameworks by ISACA



Fonte: (ISACA, 2009)

Conforme mostrado na figura 7 acima, os relacionamentos entre os frameworks funcionariam da seguinte forma:

a) As atividades de TI e os eventos relacionados são controlados pelo COBIT;

b) O COBIT avalia os riscos e oportunidade gerando informações;

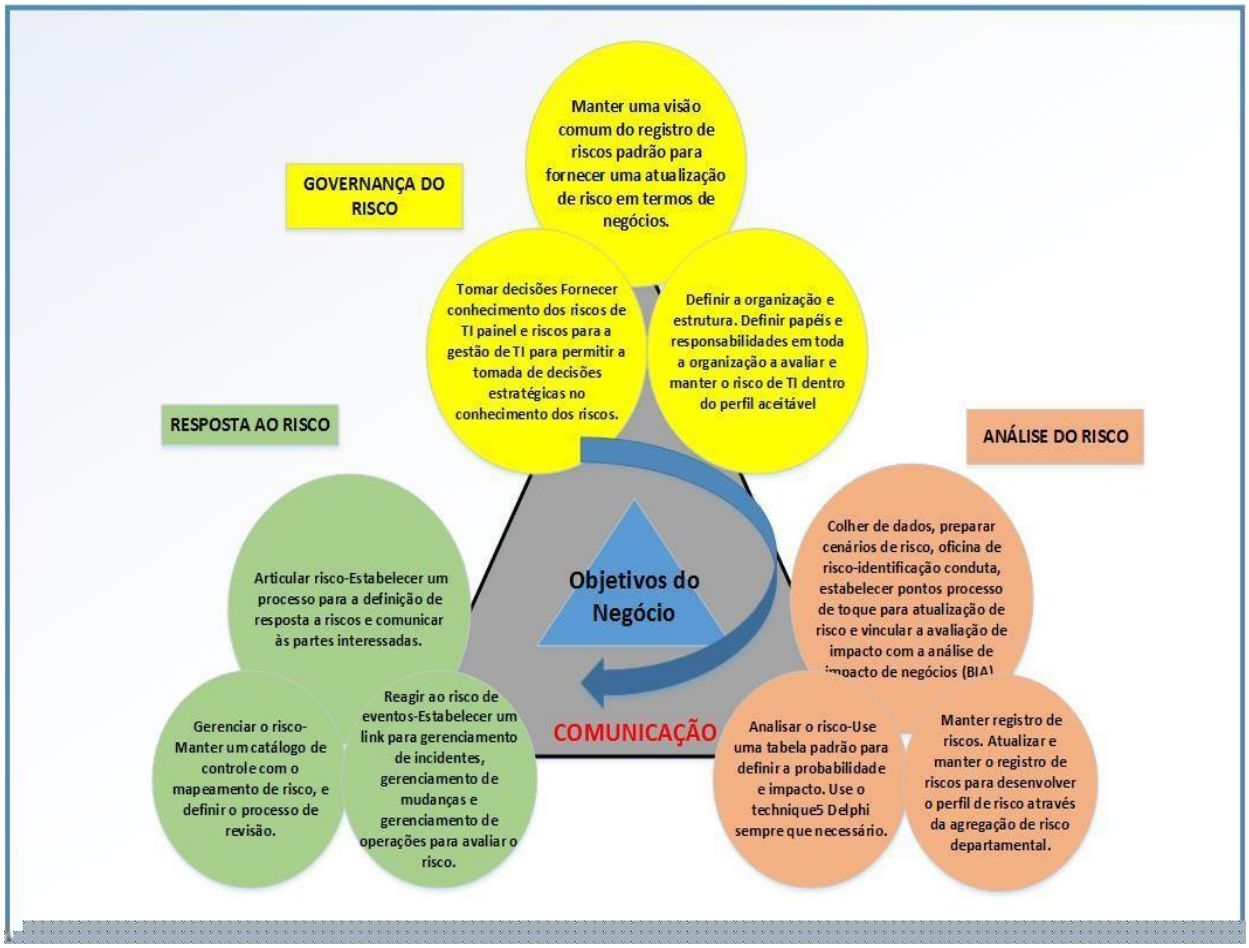
c) Essas informações serão tratadas *pelo RISK IT*, bem como pelo *VAL IT*.

2.7 Domínios do *risk it*

Segundo Fischer, em uma série de artigos "*Identify, Govern and Manage IT RISK*" publicados no ISCA 2009, o framework *RISK IT* está consolidado em práticas efetivas no que se refere a uma eficiente Gestão de Riscos e traz com ele semelhanças com outros frameworks já consagrados, como o COSO ERM, a ISO 27005 e ISO 31000 (SANTOS, 2009).

Com a intenção de atingir os objetivos descritos nos princípios do *RISK IT*, ele foi dividido em três domínios, conforme figura 8 abaixo:

Figura 08 – Domínios do RISK IT



Fonte: (ISACA, 2009, RISK IT).

2.7.1 Governança do risco *(risk governance)*

Esse domínio tem por principal função certificar que as práticas de atividades inerentes ao Risco de TI estão incorporadas ao negócio, permitindo que a empresa tenha assegurado um retorno aceitável do risco controlado. É bom lembrar de que quanto maior o lucro, maior o risco (SANTOS,2009).

Esse domínio possui três processos, são eles:

a) Estabelecer e manter uma visão comum dos riscos;

b) Integração com Gerenciamento dos Riscos Corporativos;

c) Incluir consciência de riscos nas decisões de negócio (NETO, REIS, 2015).

2.7.2 Avaliação dos riscos *(risk evaluation)*

Esse domínio tem por função assegurar que os riscos existentes de TI serão identificados, analisados, catalogados e acompanhados. De certa forma, é prudente também gerar um banco de dados com todas essas informações que seja atualizado continuamente. É nessa fase que são gerados os indicadores (KRIs), que contribuem de forma significava para a análise dos riscos (NETO, REIS, 2015).

Assim como no primeiro domínio, esse também é dividido em três processos, são eles:

a) Coleta de dados;
b) Analisar os Riscos;
c) Manter um perfil dos Riscos**.**

2.7.3 Resposta ao risco *(risk response)*

Esse domínio tem por objetivo que os riscos de TI, as oportunidades e eventos, serão tratados de forma aceitável em relação ao custo/benefício, considerando as prioridades do negócio (NETO, REIS, 2015).

É válido frisar que os riscos fazem parte de uma ciência não exata e que o mesmo risco pode se apresentar de maneira diferente, trazendo consequências desastrosas. Ter uma equipe motivada, detentora de conhecimento e pronta para atuar na resposta ao risco, contribui de forma significativa para a erradicação do risco ou para a mitigação em valores aceitáveis. Lembrando também que a comunicação fluida com a alta direção da empresa só vem a contribuir para uma resposta ao risco rápida e eficiente, trazendo ganhos à Organização (CASACA, 2014).

Os processos da resposta ao risco, conforme o *Risk IT*, são os seguintes (SANTOS,2009):

a) Articular os Riscos;
b) Gerenciar os Riscos;
c) Reagir aos eventos (*RISK IT*, 2009).

2.8 Modelo completo do *RISK IT by ISACA*

Pode-se perceber, em análise à ISO 2007, que o *RISK IT* é uma ferramenta mais extensa e detalhada que as demais, proporcionando uma visão de “lupa” nos assuntos específicos de riscos relacionados à tecnologia da informação (NETO, REIS, 2015).

Ele interage com outras ferramentas, trazendo na sua estrutura conceitos de vários outros *frameworks* já consolidados no mercado, passando assim uma confiança em sua utilização (NETO, REIS, 2015).

3 ISO 27005:2008 X *RISK IT BY ISACA*

Como apresentado anteriormente, não é intenção deste artigo dizer qual a melhor ferramenta para controle, análise e resposta aos riscos, mas sim mostrar as vantagens e desvantagens de cada uma, assim como suas semelhanças (SANTOS, 2009).

Pode-se perceber que o *RISK Evaluation* do *RISK IT* está relacionado à Análise/Avaliação de Riscos da ISO 27005. Já o *RISK Response do RISK IT* pode ser relacionado ao Tratamento dos Riscos da ISO 27005. A ISO 27005 também tem processos como Monitoramento e Comunicação dos Riscos, que podem ser relacionados ao *RISK Response do RISK IT*. Por último, vale ressaltar que, no caso da ISO 27005, todos os processos são colocados dentro do ciclo PDCA de Deming (CASACA, 2014).

Analisando as correlações supracitadas, são verificáveis algumas semelhanças entre os modelos em questão. Sabe-se ao certo que um PCR (Plano de Contenção de Riscos) é essencial, no entanto, a utilização de cada modelo depende da adequação no cenário existente. A utilização da ISO 27005 segue padrões bem definidos e detalhados, enquanto o *RISK IT* sintetiza alguns processos e está alinhado ao COBIT 5 (NETO, REIS, 2015). Seja qual for a utilização, o PCR em SGSI sempre deve estar alinhado aos riscos corporativos da organização.

3 CONSIDERAÇÕES FINAIS

O embasamento de diretrizes de modelos de referência pode ser fundamental para que as empresas implantem seus respectivos planos de Gestão de Riscos da Segurança da Informação. Porém, as normas possuem, na sua essência, definições das direções que dizem o que deve ser feito; no entanto, não deixam claro como deve ser feito.

A norma ISO/IEC 27005 define detalhadamente o que deve ser analisado na questão dos Riscos no âmbito da Segurança da Informação; no entanto, será necessário considerar também a leitura ISO/IEC 27001 e 27002, que irão, juntas, delinear todo arcabouço para a estrutura de uma Gestão de Risco de SGSI bem estruturada. Há de se ressaltar que este estudo requer tempo e maturidade para aplicação dos procedimentos relacionados.

Este artigo não pretende, de forma nenhuma, incitar a utilização imediata dos ***frameworks***, por serem eles mais objetivos ante as normas padrão; porém alvitra utilizá-los em paralelo, buscando o equilíbrio das funcionalidades.

Conforme estudo da *Global Data Protection Index*, encomendado à *Vanson Bourne pela EMC*, só em 2014 as empresas brasileiras tiveram um prejuízo de U$ 2,8 bilhões com a perda de dados e U$ 24,1 bilhões com interrupção dos serviços.

Assim, é perceptível que, muitas vezes, esses prejuízos são irreparáveis. Portanto, independente do modelo adotado, a existência e a utilização de um PCR em relação à segurança das informações deve fazer parte do cotidiano de qualquer empresa, a fim de mantê-la competitiva em um mercado globalizado; sempre considerando que, quanto menor a probabilidade, menor o

impacto, ou seja, manter os riscos em padrões aceitáveis deve ser uma das metas essenciais em qualquer empresa.

Este trabalho não pretende esgotar as exemplificações dos caminhos a seguir na constituição de um plano de Gestão de Riscos; pelo contrário, deixa indícios que será preciso estudar outras normas, padrões e frameworks existentes, no intuito de contemplar uma análise mais profunda sobre um tema tão importante e ainda pouco difundido no Brasil.

A COMPARATIVE ANALYSIS ON THE USE OF A SECURITY RISK RETENTION OF PLAN BASED INFORMATION IN ISO / IEC 27005: 2008 AND FRAMEWORK RISK IT BY ISACA

ABSTRACT

Information is undoubtedly the most important asset in enterprises, public or private ones, we see the lack of structure of the same to deal with the security of your information. The lack of knowledge of their vulnerabilities and threats and hence the lack of preparation for the negative impacts that may arise from unexpected events, highlight the need, which is fundamental, the implementation of a safety management policy guided in a Plan Business Continuity and, in a Control Plan and Risk Avoidance. The combination of these two documents with well-defined applications and controls, provide to the company a more stable scenario, contributing to important decisions in the sphere of Governance and Information Security Management (ISMS). This article follows the methodology of literature review, and aims to show the characteristics of the above models, providing the reader with a more refined view of ISO 27005 and RISK IT framework, clarifying their similarities and differences in use, which will contribute to decide the model to be implemented in your company.

Keywords: Risk Management - ISO / IEC 27005: 2008 - ISACA - Information Security Management.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27005:** Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS **NBR 31000:** Gestão de Riscos - Princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

ALBERTS, C. J. **Common Elements of Risk**, 2006. Pittsburg, PA: Caenegie Mellon University, Software Program. Recuperado em 11 de Maio, 2007. Disponível em: http://www.seicmu.edu/pub/documents/06.reports/pdf/06tn014.pdf. Acesso em: 9 de maio de 2016.

ARAÚJO, F.C.D. **Manual de Gestão de Riscos**, São Paulo, 2012. Disponível em: <http://pt.slideshare.net/fabiocdaraujo/manual-de-gesto-de-riscos>. Acesso em: 9 de maio de 2016.

BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C.; FABENDER**. S.** Pattern-Based Support for **Context Establishment and Asset Identification of the ISO 27000** in the Field of Cloud Computing. Sixth International Conference on Availability, Reliability and Security, 2011, p.327-333

CASACA, J. A**. Gestão de riscos na segurança da informação**: conceitos e metodologias, Lisboa, 2014.

ISACA. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, *framework Risk IT*, 2009, Illinois, United States. Disponível em: <https://www.isaca.org>. Acesso em: 9 de maio de 2016.

KOZEN, M. P.; FONTOURA, L. M.; NUNES, R. C. **Gestão de Riscos de Segurança da Informação, Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança**. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 9, 2012, Rio de Janeiro.

LUND, M. S.; SOLHAUG, B.; STOLEN, K**. Evolution in relation to risk and trust management.** IEEE Computer Society, 2010, p. 49-55.
NETO, E. F. L.; REIS L.C.D. **RISK IT Based on COBIT**: uma visão sistêmica para auditoria em TI. In: CONGRESSO DE SEGURANÇA DA INFORMAÇÃO E AUDITORIA DE GOVERNANÇA, 28., 2015, São Paulo. Disponível em: <http://www.cnasi.com.br/risk-it-based-on-cobit-uma-visao-sistemica-para-a-auditoria-de-ti/>. Acesso em: 9 de maio de 2016.

SANTOS, G. S. **Gestão de Riscos**: uma avaliação do Risk IT Framework do ISACA/ITGI. Abril de 2009, Gestão de Segurança da Informação. Disponível em <http://gestaosistemasdeinformacao.blogspot.com.br/2009/04/gestao-de-riscos-uma-avaliacao-do-risk.html>. Acesso em: 9 de maio de 2016.

SHEWHART, W- **PDCA (*PLAN - CHECK - ACT / Plan-Do-Check-Adjust)***, 1930, EUA.