LEANDRO JOSÉ AGUILAR ANDRIJIC MALANDRIN

MODELO DE SUPORTE A POLÍTICAS E GESTÃO DE RISCOS DE SEGURANÇA VOLTADO À TERCEIRIZAÇÃO DE TIC, COMPUTAÇÃO EM NUVEM E MOBILIDADE

São Paulo

2013

LEANDRO JOSÉ AGUILAR ANDRIJIC MALANDRIN

MODELO DE SUPORTE A POLÍTICAS E GESTÃO DE RISCOS DE SEGURANÇA VOLTADO À TERCEIRIZAÇÃO DE TIC, COMPUTAÇÃO EM NUVEM E MOBILIDADE

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia

Área de concentração:
Sistemas Digitais

Orientadora: Professora Doutora
Tereza Cristina Melo de Brito Carvalho

São Paulo
2013

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 25 de maio de 2013.

Assinatura do autor _____

Assinatura do orientador _____

Catalogação da Publicação
Serviço de Documentação
Escola Politécnica da Universidade de São Paulo

FICHA CATALOGRÁFICA

Malandrin, Leandro José Aguilar Andrijic
Modelo de suporte a políticas e gestão de riscos de segurança voltado à terceirização de TIC, computação em nuvem e mobilidade / L.J.A.A. Malandrin. -- versão corr. -- São Paulo, 2013.
155 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1.Análise de risco 2.Política de segurança 3.Normas técnicas 4. Sistema de gestão de segurança da informação I.Universidade São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II.t.

DEDICATÓRIA

Ao meu pai, João Malandrin, engenheiro,
pelo exemplo de vida e de carreira.

À minha mãe, Maria Aparecida Malandrin, professora,
pelos ensinamentos em todas as escolas da vida.

À minha irmã, Tatiana Malandrin, hoteleira,
por me mostrar como receber e acomodar os novos desafios.

Ao meu irmão, Daniel Malandrin, técnico e administrador,
pelo interesse compartilhado em tecnologia e orientação nas decisões da vida.

À minha Vanessa, por estar comigo em todos os momentos e
por me ajudar a ser uma pessoa melhor.

AGRADECIMENTOS

Agradeço a todos os colegas que me ajudaram direta ou indiretamente no desenvolvimento desse trabalho.

Agradeço a toda a equipe do Laboratório de Arquitetura e Redes de Computadores da Escola Politécnica da USP, pelo incentivo à pesquisa em segurança da informação e por toda a ajuda durante as discussões sobre o mestrado.

Agradeço à Profa. Dra. Tereza Cristina Melo de Brito Carvalho, pelas grandes oportunidades oferecidas e pela orientação durante todo o mestrado, essencial para a sua finalização.

Agradeço à PromonLogicalis pela flexibilidade e pelo comprometimento incomparável com a capacitação de seus funcionários, sem os quais esse trabalho não seria possível.

RESUMO

O cenário tecnológico é um fator importante a ser considerado ao se trabalhar com Sistemas de Gestão de Segurança da Informação (SGSI). No entanto, nos últimos anos esse cenário se alterou profundamente, aumentando em complexidade de maneira até antes não vista. Caracterizado principalmente por tendências tecnológicas como a terceirização de infraestrutura de TIC, a computação em nuvem e a mobilidade, o cenário externo atual gera grandes novos desafios de segurança. A abordagem típica para tratar com mudanças de cenário em SGSIs é uma revisão da análise de riscos e a implantação de novos controles de segurança. No entanto, frente a um cenário tão disruptivo, riscos podem passar despercebidos, devido à falta de conhecimento sobre os novos elementos introduzidos por esse cenário. Por causa disso, adaptações mais profundas, durante o próprio planejamento do SGSI, são necessárias. Usando a norma de segurança ISO/IEC 27001 como referência, esse trabalho introduz um modelo de suporte que permite a identificação dessas adaptações. Para construir esse modelo, foram inicialmente levantados os riscos referentes a cada uma das três tendências tecnológicas listadas. Esses riscos foram compilados e analisados em conjunto, buscando a identificação de temas de preocupação recorrentes entre eles. Para endereçar cada um dos temas dentro do modelo de suporte, foram levantadas adaptações do SGSI sugeridas na literatura e na prática de segurança. Essas adaptações foram transformadas em pontos de checagem a serem observados durante a execução das duas atividades principais da fase de Planejamento do SGSI da ISO/IEC 27001: definição de políticas de segurança e gestão de riscos. A contribuição principal do trabalho é um modelo de suporte de segurança com o qual as organizações podem adaptar o seu SGSI e assim melhor protegerem suas informações frente ao cenário tecnológico externo descrito. Como contribuição secundária está a sugestão de uma análise unificada com foco em segurança das tendências tecnológicas desse cenário.

Palavras-chave: Segurança da Informação, Gestão de Segurança da Informação, Gestão de Riscos, Políticas de Segurança, Computação em Nuvem, Terceirização, Mobilidade

ABSTRACT

The technological scenario is an important factor to be considered while working with Information Security Management Systems (ISMS). However, in the latter years this scenario has changed deeply, increasing in complexity in a way not seen so far. Characterized mainly by the heavy use of ITC infrastructure outsourcing, cloud computing and mobility, the current external scenario creates big new security challenges. The typical approach to handle changes of scenarios in ISMSs is a risk assessment review and deployment of new security controls. However, when considering such a disruptive scenario, some risks may go unnoticed, due to the lack of knowledge of the elements introduced by this scenario. Because of that, deeper adaptations are needed, during the actual ISMS planning. Using the ISO/IEC 27001 as a reference, this research introduces a framework for the identification of these adaptations. To build this framework, risks related to each of the three technological trends mentioned were identified. These risks were compiled and analyzed together, searching for recurring themes of concern among them. To address each of these themes in the framework, ISMS adaptations suggested in the security literature and practice were identified. These adaptations were transformed in checkpoints to be verified during the execution of the two main activities of the ISO/IEC 27001 ISMS Plan phase: security policies definition and risk management. The main contribution of this research is a framework which can help organizations adapt their ISMSs and better protect their information in the technological scenario described. As a secondary contribution is the proposal of a unified security analysis of the distinct security trends of the external scenario.

Keywords: Information Security, Information Security Management, Risk Analysis, Security Policies, Cloud Computing, Outsourcing, Mobility

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API – *Application Program Interface*

BPO – *Business Process Outsourcing*

BSI – *British Standards Institute*

BYOD – *Bring Your Own Device*

CIA – *Confidentiality, Integrity and Availability*

CPNI – *Centre for Protection of National Infrastructure*

CRM – *Customer Relationship Management*

CSA – *Cloud Security Alliance*

DLP – *Data Loss Prevention*

DNS – *Domain Name System*

ERP – *Enterprise Resource Planning*

GSI – Gestão da Segurança da Informação

IaaS – *Infrastructure-as-a-Service*

IEC – *International Electrotechnical Commission*

IDS – *Intrusion Detection System*

IPS – *Intrusion Prevention System*

ISF – *Information Security Forum*

ISO – *International Standards Organization*

ITSM – *IT Services Management*

NIST – *National Institute for Standards and Technology*

PaaS – *Platform-as-a-Service*

PCI-DSS – *Payment Card Industry – Data Security Standard*

PDCA – *Plan, Do, Check, Act*

ROA – *Real Options Analysis*

RPO – *Recovery Point Objective*

RTO – *Recovery Time Objective*

SaaS – *Software-as-a-Service*

SAS 70 – *Security Auditing Standards 70*

SoA – *Statement of Applicability*

SGSI – Sistema de Gestão de Segurança da Informação

SI – Segurança da Informação

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

VPN – *Virtual Private Networking*

XaaS / EaaS – *Everything-as-a-Service*

SUMÁRIO

1. INTRODUÇÃO

Neste capítulo são apresentadas as motivações e problema abordado por esse trabalho. Também são descritos os objetivos e método utilizado para alcançá-los.

1.1. MOTIVAÇÃO

A informação e o conhecimento gerado a partir dela são comumente considerados por muitas organizações como um dos principais ativos a sua disposição (NONAKA e TOYAMA, 2003), (RANDEREE, 2008). Comum também é o desejo de protegê-la de maneira adequada. De fato muitas organizações pensam dessa forma, mas a realidade não corresponde ao discurso. Basta observar as notícias diárias para notar que incidentes de segurança continuam cada vez mais frequentes e diversos, indo desde pequenas quebras de sigilo de senhas até monumentais perdas de dados e ataques complexos a plantas industriais. Como se isso não bastasse, os incidentes publicados constituem apenas uma fração do número real de casos, pois ainda é grande a falta de conscientização sobre a segurança da informação.

Isso acontece porque, apesar de toda a preocupação com a proteção da informação, a verdade é que hoje a “Informação” e a “Segurança da Informação” são tratadas de maneira bem distintas na maioria das organizações.

A “Informação” corresponde aos dados manipulados constantemente na organização em todo tipo de situação. A discussão realizada durante uma reunião, o fax enviado pela matriz para uma filial, a cópia impressa de um documento e até o bate papo no elevador caracterizam-se como troca de informações que dizem respeito ao trabalho do dia a dia. Dessa forma, a informação pode ser manipulada de diversas formas, por todo tipo de equipe e em diferentes níveis organizacionais.

A “Segurança da Informação”, no entanto, é um tópico visto de maneira bem mais restrita e que normalmente remete a invasores de sistemas, vírus e spam de e-mail, proteção das senhas da rede, entre outros. Assim, a segurança da informação é um assunto discutido apenas do ponto de vista tecnológico, e que é responsabilidade das equipes de Tecnologia da Informação (TI). Dessa forma, cria-

se a ilusão que a única informação que deve ser protegida é aquela em formato digital.

No entanto, durante a última década os incidentes de segurança trouxeram à tona a necessidade de aplicar as técnicas de segurança já conhecidas à informação manipulada por pessoas e processos, e não apenas por meios tecnológicos. Outro ponto importante foi perceber que a proteção da informação não é uma atividade pontual, mas que deve ser executada e revisada continuamente. Agregando essas ideias, foram criados e implantados em muitas organizações os chamados Sistemas de Gestão de Segurança da Informação (SGSI). Com base em métodos de revisão contínua já presentes em abordagens consagradas de gestão, os SGSI tentam implantar o tratamento seguro da informação nas organizações. Hoje existem vários padrões para gestão da segurança: ISO/IEC 27001 – o mais aceito e conhecido – *Payment Cart Industry Data Security Standard* (PCI-DSS), NIST FIPS 140-2 e *Information Security Forum Standard of Good Practice* (ISF) (TSOHOU, KOKOLAKIS, *et al.*, 2010).

A definição de políticas de segurança da informação e uma avaliação constante dos riscos aos quais a organização está exposta são chaves para os SGSIs. Por exemplo, no caso do SGSI estabelecido pela ISO/IEC 27001, uma das primeiras definições a ser feita é justamente a da política e do método de avaliação de riscos. Uma vez definido o método, ele é executado periodicamente de forma a identificar novos requisitos de segurança derivados dos cenários interno e externo. Essa abordagem clássica, quando bem executada, consegue mitigar os riscos causados por novas vulnerabilidades ou ameaças. No entanto, vê-se que ela utiliza como premissa que a política e método definidos são capazes de identificar novos requisitos de segurança. Infelizmente isso acontece apenas quando se consideram ativos de informação e processos bem conhecidos pela organização

A realidade é que as organizações atualmente se veem imersas em um cenário muito dinâmico, que traz consigo várias mudanças tecnológicas e novos paradigmas. Entre as tendências tecnológicas podem ser citadas a terceirização de serviços, a computação em nuvem e a mobilidade. Entre os novos paradigmas estão o uso constante de mídias sociais, a convergência de ambientes profissionais e pessoais e a "consumerização[1]", com modelos BYOD (*Bring Your Own Device*).

[1] Consumerização se refere à tendência de novos produtos serem desenvolvidos inicialmente para o mercado consumidor e depois se espalhar para mercados corporativos e governamentais.

Esse é um cenário bem disruptivo, onde novas formas de trabalho estão sendo estabelecidas e novos conceitos são introduzidos no dia a dia das organizações, de maneira até então nunca vista.

Observando essas características e a premissa da abordagem do SGSI comentada, nota-se que os impactos desse cenário para a gestão de segurança da informação podem ser muito grandes. Mais agravante é a noção que a adoção de determinadas tecnologias acontece naturalmente devido às inúmeras vantagens que ela traz. Portanto, as organizações precisam agora descobrir formas de minimizar as suas desvantagens. Por exemplo, no uso de serviços terceirizados para a gestão da infraestrutura tecnológica, o controle sobre informação e o conhecimento sobre processos executados diminui significativamente. No entanto, o aumento da disponibilidade sobre a infraestrutura e o ganho de tempo disponível das equipes de sistemas são muito significativos. Da mesma forma, a entrada de dispositivos pessoais no ambiente de trabalho aumenta a possibilidade de novas vulnerabilidades e ataques à informação. Mas a produtividade dos profissionais seria impactada se lhes for proibido o uso desses dispositivos, em especial se a organização não oferece dispositivos próprios, como *smartphones* e *tablets*.

Assim as organizações não podem mais depender de controles pré-definidos em processos específicos a fim de garantir a segurança da informação. A segurança é mais do que nunca um alvo em movimento. Além disso, também é essencial o foco cada vez maior no grau de conscientização da segurança da informação pelos colaboradores, pois esses representam os maiores riscos para a organização. Nesse cenário são comuns as situações não planejadas, que dependem de decisões tomadas com base em entendimento de conceitos mais básicos de segurança da informação (LACEY, 2010).

Então, pode-se imaginar que a abordagem típica descrita para os SGSI, baseada em uma simples reavaliação dos riscos, requer adaptações para lidar com essa nova realidade. Para tal, é necessário o desenvolvimento de práticas que permitam reduzir a distância entre a “Informação” e a “Segurança da Informação”, buscando a criação de uma cultura de segurança que esteja adaptada às novas tendências tecnológicas e ao mesmo tempo seja flexível para lidar com outras mudanças. Isso é essencial para garantir que todos os benefícios do novo contexto tecnológico sejam aproveitados ao máximo e de maneira segura.

1.2. DESCRIÇÃO DE PROBLEMA

A situação descrita na seção 1.1 leva a um questionamento principal, a saber:

Como permitir às organizações continuarem respondendo adequadamente aos riscos de segurança da informação frente às profundas alterações do cenário tecnológico?

Uma análise mais profunda desse questionamento facilita a correta descrição do problema em questão. A gestão de segurança da informação por si só é um conceito relativamente novo no dia a dia das organizações. Além disso, é também bem amplo, onde práticas diversas podem ser aplicadas para atingir os resultados desejados. Sendo assim, é importante que o escopo da pesquisa a ser realizada seja delimitado.

O primeiro ponto de delimitação de escopo é a caracterização do tipo de organização a ser considerada. Atualmente tecnologias típicas do novo cenário, como a terceirização da infraestrutura de TIC, serviços de computação em nuvem e mobilidade, estão presentes no dia a dia de todo tipo de organização, em qualquer ramo de atividade. Mesmo quando essas tecnologias não são adotadas de forma corporativa, seus colaboradores as trazem para o dia a dia naturalmente, mudando paradigmas típicos de trabalho, como comunicação, localização e jornada de trabalho. Por exemplo, o uso de dispositivos móveis pessoais conectados a serviços na Internet é comum em todo ramo de atividade. Assim, a área de atuação da empresa por si só não é um ponto de grande diferenciação para os propósitos dessa pesquisa. Além disso, é importante observar que as técnicas de gestão de segurança da informação são aplicáveis a qualquer organização (ISO/IEC 27001, 2005), independente seus fins e ramo de atividade. No entanto, é provável que organizações que empregam essas tecnologias de maneira corporativa se beneficiem mais de qualquer iniciativa voltada à adequação de práticas de segurança para o novo cenário. Isso porque existe uma chance maior da informação da organização ser manipulada através de uma determinada tecnológica quando essa é utilizada de maneira corporativa do que se essa tecnologia fosse utilizada apenas pontualmente por um ou outro colaborador.

O segundo ponto de delimitação de escopo diz respeito ao porte da organização. Novas medidas de segurança tem impacto em maior ou menor grau de acordo com o quão forte é a cultura organizacional de segurança. Essa cultura, por sua vez, é construída e depende de funcionários, executivos e todas as pessoas que manipulam as informações da organização. Quanto maior o número de funcionários, portanto, maior a dificuldade de mudar ou uniformizar essa cultura e de obter resultados a partir da implantação de novos controles. Por exemplo, espera-se que uma organização de mais de 1000 funcionários (considerada de médio porte para os propósitos dessa pesquisa) tenha muito mais dificuldade de alterar sua cultura do que uma organização de 100 funcionários (considerada de pequeno porte para os propósitos dessa pesquisa). Assim, a pesquisa aqui desenvolvida deve focar em organizações de médio e grande porte, onde é necessário um maior suporte para adaptação da cultura de segurança.

O terceiro ponto a ser considerado é o grau de maturidade das organizações quanto ao tema segurança. Apesar das práticas de gestão de segurança serem aplicáveis a todo tipo de trabalho, muitas organizações sequer possuem programas estruturados sobre o tema. Para esse tipo organização, mesmo conceitos básicos como proteção de senhas de usuários, classificação da informação e identificação de incidentes precisam ainda ser inseridos e disseminados na cultura organizacional. Isso torna a adoção de novas posturas quanto à segurança uma tarefa bem complicada, em especial se é necessário considerar o novo cenário tecnológico externo e suas implicações.

Para organizações que já possuem práticas de segurança estabelecidas, a situação é diferente. Nesse caso, os conceitos mais básicos de gestão de segurança já fazem parte do dia a dia e é possível pensar na adaptação de algumas abordagens clássicas para melhor preparar a organização para lidar com novos riscos de segurança. Assim, faz sentido delimitar a área de estudo da pesquisa em organizações que estão nessa situação. Para melhor caracterizar esse tipo de organização, podem-se considerar aquelas que já possuem um sistema de gestão de segurança formalmente estabelecido.

O quarto ponto de definição para a pesquisa é a caracterização do sistema de gestão de segurança, dentre os diversos existentes, que deverá ser considerado. É interessante que qualquer iniciativa no sentido de modificar práticas já existentes não impacte profundamente o modo de trabalho da organização com segurança. Daí

a necessidade de se escolher um padrão para o estudo. A abordagem estabelecida pela ISO/IEC 27001 é a mais comumente referida para se estabelecer um Sistema de Gestão de Segurança da Informação (SGSI). A série 27000 da ISO mudou profundamente a percepção de problemas em segurança (BELSIS e KOKOLAKIS, 2005). Dessa forma, apesar de existirem outros padrões aceitos no mercado – PCI-DSS, NIST FIPS 140-2 e ISF, por exemplo – essa pesquisa irá focar em organizações que estejam trabalhando com o modelo de gestão de segurança proposto pela série 27000 da ISO.

O quinto e último ponto de delimitação do escopo da pesquisa diz respeito ao momento mais interessante para realizar qualquer intervenção no modelo proposto pelo SGSI da ISO/IEC 27001. A maior parte das abordagens existentes para a Gestão de Segurança da Informação possui uma fase inicial de planejamento onde são definidas as principais diretrizes de todo o sistema de gestão a ser implantado (TSOHOU, KOKOLAKIS, *et al.*, 2010). A ISO/IEC 27001 não é diferente: como será apresentado com maiores detalhes nos próximos capítulos, esse modelo utiliza o ciclo PDCA (*Plan, Do, Check, Act*). Ele é utilizado como meio de garantir a melhoria contínua da segurança organizacional (ISO/IEC 27001, 2005). A fase de Planejamento, a primeira a ser executada é a base para todo o processo e é composta por duas atividades principais:

- Definição da Política de Segurança da Informação; e
- Gestão de Riscos de Segurança.

Essas atividades direcionam a condução das demais fases. Sendo assim, a criação de uma Política de Segurança bem estruturada combinada com execução adequada de uma Análise de Risco é crítica para a melhoria da segurança da informação (ISO/IEC 27001, 2005). Entre os dez enganos mais comuns relacionados à Gestão de Segurança da Informação estão justamente a falta de um desenvolvimento adequado de políticas de segurança e de uma análise de riscos (VON SOLMS e VON SOLMS, 2004). Sendo assim, essa pesquisa irá focar na adequação dos resultados da fase de Planejamento do SGSI da organização para lidar com perspectivas do novo cenário de segurança.

De fato muitas organizações enfrentam uma série de dificuldades na criação de um SGSI, as quais muitas vezes estão relacionadas à maneira com que a fase de

Planejamento (*Plan*) foi executada. As várias dificuldades enfrentadas nessa etapa podem ser resumidas em:

- Internamente à organização, o uso de técnicas e soluções de mercado, tomadas como “melhores práticas” sem nenhuma adaptação (SIPONEN e WILLISON, 2009), além da falta de dedicação de tempo e recursos ao planejamento adequado do SGSI; e
- Externamente à organização, alterações causadas pelo novo cenário tecnológico, onde a infraestrutura é baseada intensivamente em serviços, de forma a proporcionar alta flexibilidade e mobilidade.

Como evidências dessas dificuldades podem ser citadas: políticas de segurança desconhecidas; políticas distantes do dia a dia dos colaboradores; criação de evidências falsas para auditorias; análises de risco conduzidas uma única vez e sem acompanhamento; controles com alto índice de rejeição e investimentos desnecessários e duplicados em soluções de segurança (HERLEY, 2009), (FURNELL, 2005).

Em resumo, entende-se que pesquisas voltadas a responder o questionamento destacado no início desta seção devem se concentrar em organizações de médio e grande porte que fazem uso corporativo de terceirização de TIC, computação em nuvem e mobilidade, tecnologias essas características do novo cenário. Essas organizações devem possuir maturidade em segurança da informação, expressa através da conformidade com padrões de segurança conhecidos de mercado como o proposto pela ISO/IEC 27001. Finalmente, é interessante a atuação em momentos mais significativos da criação e adequação do SGSI. No caso do padrão citado, esses correspondem à fase de Planejamento do SGSI.

Com base no escopo de atuação para a pesquisa, surge o interesse no desenvolvimento de ferramentas que possam ser utilizadas na fase de Planejamento (*Plan*) do SGSI para melhorar a abordagem de segurança frente a esse novo cenário externo. Esse trabalho busca a criação de uma dessas ferramentas: um modelo de suporte para identificar, adaptar e correlacionar, de maneira uniforme, os principais riscos encontrados e as formas de mitigação. O desenvolvimento do modelo utiliza como referência principal pesquisas realizadas na área de Gestão de Segurança e a experiência acumulada pelo autor ao longo de cinco anos de trabalho de consultoria no tema para clientes nos mais diversos segmentos de atuação.

Esse trabalho servirá de guia para organizações imersas no novo cenário e que estão tentando lidar com os desafios de implantação de Sistemas de Gestão de Segurança da Informação.

1.3. OBJETIVOS

O desenvolvimento de um modelo de suporte para a fase de Planejamento da ISO/IEC 27001 não pode deixar de levar em consideração as práticas e conceitos desenvolvidos ao longo dos anos. Muito pelo contrário – o fato desses conceitos terem sido incorporados a padrões internacionais como a ISO/IEC 27001 indicam a sua validade e solidez (VON SOLMS e VON SOLMS, 2004). Assim, o propósito do modelo de suporte deve ser guiar as organizações na implantação desses conceitos, mas considerando o novo cenário tecnológico que se apresenta.

Uma forma de obter esse tipo de resultado é fazer com que o modelo de suporte permita ao responsável pela fase de planejamento melhor compreender esse cenário durante o desenvolvimento de suas atividades. O modelo deve influenciar os resultados da atividade de planejamento, mas não deve substituir o seu fluxo natural. Ele deve expandir o escopo de atuação em direções bem específicas, oferecendo o suporte ao fluxo principal de trabalho, mas sem substituí-lo.

O objetivo primário do trabalho é a proposição de um modelo de suporte à fase de Planejamento da Gestão de Segurança da informação que siga as diretrizes básicas explicitadas acima. Dado que existem dois fluxos de atividades principais, o modelo deve ser dividido em duas partes: definição de Políticas de Segurança e Gestão de Riscos de Segurança.

Dessa forma, o modelo de suporte proposto poderá ser utilizado paralelamente aos trabalhos de planejamento de um SGSI, não invalidando os conceitos e método, mas ajudando as organizações de forma prática durante a execução.

Antes de dar início do desenvolvimento do modelo de suporte é necessária a compreensão do cenário descrito e quais são as perspectivas para o tipo de trabalho realizado e novas tecnologias. Também é importante um estudo dos problemas já

conhecidos na fase de planejamento de SGSI e como esses problemas influenciam o resto das atividades.

Um objetivo secundário do trabalho é, portanto, a realização de estudo que consolide as pesquisas já realizadas a respeito de problemas práticos identificados para a implantação de Sistemas de Gestão de Segurança da Informação. Também se inclui nesse estudo o levantamento e a análise dos riscos existentes nas tecnologias que caracterizam o novo cenário, de forma que o modelo de suporte possa levar em consideração esses riscos.

Finalmente, outro objetivo secundário do trabalho é a validação da aplicabilidade do modelo de suporte proposto. Existe uma grande dificuldade para justificar a aplicação de práticas de segurança em termos quantitativos ou qualitativos (BOEHMER, 2008). No entanto, dado que o modelo proposto não visa à substituição do processo de Planejamento, mas sim o seu suporte e melhoria, é importante avaliar eventuais dificuldades na sua utilização. Indiretamente, o modelo de suporte visa à melhoria da segurança da informação da organização. Assim, pode ser interessante avaliar os resultados da análise de riscos frente à utilização ou não do modelo, observando a redução dos riscos da organização segundo o método escolhido pela mesma.

Não é objetivo deste trabalho a proposição de modelos de suporte para outras fases além da de Planejamento, ou seja, para as fases de Execução, Verificação e Atuação. Da mesma forma, não é objetivo do trabalho validar mecanismos propostos atualmente para garantir a segurança da informação.

1.4. MÉTODO

O método utilizado para atingir os objetivos do trabalho foi dividido em três grandes etapas, sendo elas:

- Pesquisa e análise de informações;
- Construção do modelo de suporte;
- Estudo de aplicabilidade do modelo de suporte.

1.4.1. ETAPA 1: PESQUISA E ANÁLISE DE INFORMAÇÕES

Foi realizada uma pesquisa referenciada e sistemática em trabalhos já publicados na academia e em outras fontes relevantes da área de Gestão de Segurança. Uma revisão bibliográfica, que contém um resumo dos resultados dessa etapa, pode ser encontrada no capítulo 2. A seguir são detalhados os temas pesquisados e o interesse em cada um deles:

- **Desafios atuais em Sistemas de Gestão de Segurança da Informação (SGSI)**, com o interesse de compreender quais são os principais padrões utilizados no mercado, os pontos críticos encontrados na sua utilização e práticas utilizadas para contorná-los;
- **Caracterização do cenário externo: Segurança em terceirização de infraestrutura de TIC,** com o interesse de mapear riscos identificados pelo mercado e levantar recomendações e técnicas usadas para aumentar a segurança da informação sem depender de infraestrutura terceirizada;
- **Caracterização do cenário externo: Segurança em computação em nuvem,** com o interesse de mapear riscos identificados pelo mercado e, compreender melhor o funcionamento da tecnologia e como ela se relaciona com outras tendências tecnológicas;
- **Caracterização do cenário externo: Segurança em mobilidade,** com o interesse de mapear riscos identificados pelo mercado e avaliar melhor os impactos da utilização de dispositivo móveis em ambientes organizacionais;
- **Planejamento do SGSI: Desenvolvimento de Políticas de Segurança**, com o interesse de levantar a abordagem e conteúdo típicos para o desenvolvimento da atividade e entender os desafios que existem na sua concepção;
- **Planejamento do SGSI: Desenvolvimento da Análise de Risco,** com o interesse de levantar a abordagem típica para a execução da

atividade e mapear práticas e controles existentes para consideração de riscos de novas tecnologias;

- **Cultura organizacional de segurança,** com o interesse de identificar formas mais adequadas para realizar mudanças organizacionais baseadas em segurança, evitando a tradicional resistência dos usuários à segurança da informação.

Com os resultados das pesquisas realizadas durante a primeira etapa, foi definida a estrutura geral do trabalho, as análises a serem feitas na etapa seguinte e o conteúdo necessário para o desenvolvimento do modelo de suporte. O conteúdo pesquisado também permitiu posicionar esse trabalho dentro das pesquisas realizadas sobre o tema.

A estrutura do trabalho busca apresentar os tópicos mais gerais sobre o tema proposto (Gestão de Segurança da Informação), passando para uma particularização desse tema (Sistemas de Gestão de Segurança da Informação). Com esses resultados, pode-se chegar a conclusões sobre os tipos de cuidados a serem tomados para construção do modelo de suporte proposto. As conclusões são apresentadas ao longo dos capítulos iniciais deste trabalho.

1.4.2. ETAPA 2: CONSTRUÇÃO DO MODELO DE SUPORTE

Durante a segunda etapa do trabalho foi realizada uma análise estruturada sobre o cenário externo e as tendências tecnológicas que o definem. Para tal, foi criada uma compilação dos riscos reconhecidos por organizações e artigos relevantes sobre cada uma das três principais tendências tecnológicas desse cenário: terceirização de infraestrutura de TIC, computação em nuvem e mobilidade.

Essas compilações levaram à identificação de pontos de atenção comuns das organizações. Combinando os pontos de atenção identificados com as abordagens típicas utilizadas para a ISO/IEC 27001 foram definidos pontos de checagem para cada uma das atividades da fase de Planejamento. Finalmente, esses pontos de checagem foram organizados no formato do modelo de suporte proposto para cada atividade.

1.4.3. ETAPA 3: ESTUDO DE APLICABILIDADE DO MODELO

Na última etapa do trabalho foi desenvolvido um estudo de aplicabilidade do modelo de suporte proposto. Para tal foi escolhida uma empresa que se encaixasse nos parâmetros de delimitação de escopo apresentados anteriormente. No caso, a empresa atua no setor de integração de soluções de TIC.

O estudo consistiu na verificação da situação do SGSI da empresa, os impactos do cenário externo no seu ambiente e por fim uma análise de cada um dos pontos de checagem do modelo de suporte.

Os resultados do estudo de aplicabilidade foram incorporados na avaliação dos requisitos propostos para o modelo de suporte.

1.5. ORGANIZAÇÃO DO TRABALHO

O presente trabalho foi organizado de forma a documentar os aspectos mais relevantes da pesquisa realizada e justificar as decisões tomadas para construção do modelo de suporte proposto.

O capítulo 2 – VISÃO GERAL DO ESTADO DA ARTE faz um sumário da pesquisa relevante em cada campo de interesse para o desenvolvimento do modelo de suporte proposto. Além disso, são indicados quais dos artigos pesquisados apresentam elementos diretamente relacionados ao modelo de suporte, deixando claro como esses elementos foram combinados para a construção do modelo de suporte.

O capítulo 3 – CONCEITUAÇÃO GERAL EM SEGURANÇA, apresenta aspectos relevantes da evolução da Gestão de Segurança da Informação para o trabalho. Também apresenta as principais fases para criação de um SGSI baseado na ISO 27001 em uma organização.

Na sequencia, o capítulo 4 – CARACTERIZAÇÃO DO CENÁRIO EXTERNO, descreve o novo contexto que as organizações se inserem, dando foco nos serviços disponíveis e como essas organizações trabalham nesse ambiente.

O capítulo 5 – RISCOS IDENTIFICADOS PARA O CENÁRIO EXTERNO, apresenta a compilação de todos os riscos identificados para cada uma das tendências tecnológicas apresentadas como características do cenário externo, e faz uma análise desses riscos em conjunto.

Com base nas informações dos capítulos anteriores, o capítulo 6 – ESPECIFICAÇÃO DE REQUISITOS DO MODELO DE SUPORTE, define os requisitos que devem ser atendidos pelo modelo de suporte proposto.

No capítulo 7 – MODELO DE SUPORTE PROPOSTO, são estabelecidas as bases para criação do modelo de suporte, indicando os motivos da estrutura escolhida e as principais fontes de pesquisa. O capítulo segue indicando como o modelo foi construído e apresentando as versões finais para o modelo de suporte para definição de políticas de segurança e para a gestão de risco.

O capítulo 8 – VALIDAÇÃO VIA ESTUDO DE APLICABILIDADE, apresenta os resultados do estudo conduzido para validação do modelo de suporte. Para realização do estudo foi feita uma análise sobre a documentação relacionada ao SGSI de uma empresa do setor de integração de soluções de TIC.

Ao fim do trabalho, o capítulo 9 – CONCLUSÕES faz uma análise crítica dos resultados alcançados, indicando os benefícios e potenciais problemas para a utilização do modelo de suporte. Também são identificadas as principais contribuições para pesquisa na área e trabalhos futuros.

2. VISÃO GERAL DO ESTADO DA ARTE

As pesquisas atuais no meio acadêmico sobre segurança da informação são amplas devido à importância recebida por esse tema na última década. Nessa seção são apresentados quais são os principais campos de pesquisa dentro desse tema e os trabalhos dentro de cada um deles relevantes para a pesquisa aqui conduzida. Como será observado em detalhe na seção 2.3, desses trabalhos foram extraídos elementos importantes para a construção do modelo de suporte.

Em artigo publicado em 2007 foram identificados quatro grandes campos de pesquisa de segurança da informação (SIPONEN e OINAS-KUKKONEN, 2007):

- Acesso a sistemas de informação (*Access to IS*);
- Comunicação segura (*Secure Communication*);
- Gestão de segurança (*Security Management*);
- Desenvolvimento de sistemas de informação seguros (*Development of secure IS*).

Segundo os autores do artigo essa classificação é bem abstrata, mas foi escolhida devido à dificuldade de classificar determinados alguns dos trabalhos de segurança da informação. Utilizar um grau de granularidade maior prejudicaria a qualidade da classificação.

Podemos notar que dentro da classificação apresentada, três campos são focados em aspectos tecnológicos (Acesso a sistemas de informação, comunicação segura e desenvolvimento de sistemas de informação seguros) e um focado em aspectos não tecnológicos (Gestão de segurança). Essa proporção não se limita apenas à classificação escolhida, mas também na quantidade de trabalhos disponíveis em cada campo. A análise dos trabalhos mostrou que mesmo a pesquisa em Gestão de segurança é focada primariamente em problemas técnicos. É provável que o foco em aspectos tecnológicos seja derivado das origens históricas da segurança da informação já comentada.

Dentro da pesquisa realizada para construção desse trabalho foram utilizadas referências relacionadas ao campo de Gestão de Segurança, principalmente, e também ao campo de Desenvolvimento de sistemas de informação seguros. A seguir, utilizando essa classificação, é apresentado um panorama das pesquisas

nessas áreas de interesse, com destaque para os trabalhos mais relevantes para a construção do modelo de suporte.

2.1. GESTÃO DE SEGURANÇA

Entre os principais erros no desenvolvimento de iniciativas de segurança da informação estão: falhas ao entender que a segurança está mais relacionada a negócios que à tecnologia e não perceber o papel crítico que os padrões de segurança da informação internacional possuem (VON SOLMS e VON SOLMS, 2004). Talvez por causa disso uma quantidade cada vez maior de estudos busca entender melhor como funcionam e devem ser aplicados os padrões de segurança da informação, dos quais muitos visam à criação de um Sistema de Gestão de Segurança da Informação (SGSI).

Existe uma quantidade considerável de estudos que procura a correlação entre os padrões de gestão de segurança existentes atualmente. Foi identificado que existem padrões que trazem abordagens completas para segurança da informação enquanto outros lidam apenas com problemas técnicos bem específicos. Esses padrões não são diretamente interoperáveis entre si, o que causa uma série de problemas (SHARIATI, BAHMANI e SHAMS, 2010) nas suas implantações. Apesar disso, é possível desenvolver modelos para viabilizar essa interoperabilidade, auxiliando profissionais de segurança a adequar suas práticas com diversos modelos ao contexto de seu trabalho. Isso pode ser feito através da análise das diretrizes básicas comuns entre os modelos (MILICEVIC e GOEKEN, 2011) ou através da avaliação das áreas de cobertura comum entre eles (TSOHOU, KOKOLAKIS, *et al.*, 2010).

Também na linha de auxílio aos praticantes de segurança, existe uma constante preocupação em mostrar para as organizações como desenvolver as práticas sugeridas em cada norma ou padrão. A abordagem holística de muitos modelos, entre eles a ISO 27001, acaba deixando muitas organizações perdidas na tentativa de entender e aplicar o conceito proposto pelo modelo de gestão sugerido no seu contexto, o que resulta em falhas de segurança da informação (SIPONEN e WILLISON, 2009). Focando especificamente na ISO 27001, foi demonstrado que

apesar de ser o padrão mais adotado e conhecido mundialmente, ainda apresenta uma série de barreiras a sua adoção e certificação, sendo uma das principais a grande quantidade de recursos pessoais humanos e financeiros a serem investidos. Por causa disso existe um constante interesse no desenvolvimento de modelos de suporte focado especificamente na simplificação da implantação da ISO/IEC 27001 (GILLIES, 2011), (ANDERSON e RACHAMADUGU, 2006), (BELLONE, DE BASQUIAT e RODRIGUEZ, 2008).

Outro campo em desenvolvimento na área de Gestão de Segurança trata de um problema um pouco mais específico: como lidar com aspectos não tecnológicos durante a implantação da gestão de segurança, mais especificamente a construção de uma cultura de segurança forte e a alteração do comportamento de colaboradores com relação à segurança.

A alteração da cultura organizacional para inclusão de segurança envolve mudanças profundas na organização. Quando a direção de uma organização não mostra coerência em desenvolver e seguir a política de segurança corporativa, não é possível esperar que os seus colaboradores façam isso (KNAPP, MARSHALL, *et al.*, 2006). Além do apoio gerencial, outras ações devem ser tomadas, como a educação interna e suporte a educação externa em segurança e recompensas para conformidade com políticas (CORRISS, 2010). Na tentativa de melhor entender como funciona esse processo, um modelo de pesquisa foi desenvolvido e aplicado em organizações com diferentes níveis de maturidade com relação à segurança (CHIA, MAYNARD e RUIGHAVER, 2002).

A alteração do comportamento de colaboradores pode ser feita por meio de programas de conscientização de funcionários que nem sempre são eficazes. É possível identificar os tipos de comportamentos que levam ao sucesso ou ao fracasso dessa prática (STANTON, STAM, *et al.*, 2005). Diversos estudos mostram de maneira qualitativa (ALBRECHTSEN, 2007), (FURNELL, 2005) e quantitativa (HERLEY, 2009) que existe uma tendência dos usuários a não respeitarem controles impostos a eles. Outros estudos tentam buscar soluções para esses problemas. O comprometimento dos usuários com relação à segurança é afetado por bonificações, exemplos de pares, certeza de detecção de incidentes e políticas, mas não por penalidades (RAO e HERATH, 2009). Também é possível desenvolver modelos de suporte que permitam aos usuários se sentirem no controle e responsáveis por ativos de segurança, na forma de uma análise pessoal de riscos (VAN CLEEFF,

2010). Fica claro que as organizações devem ser capazes de alterar seus programas de conscientização de forma a treinar seus usuários para identificar incidentes de segurança um cenário mais dinâmico e menos determinístico, como por exemplo, o criado pela computação em nuvem e mobilidade (LACEY, 2010).

2.2. DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO SEGUROS

O desenvolvimento de sistemas de informação seguros depende de um levantamento de requisitos de segurança. A principal fonte para tais requisitos é a realização de uma análise de riscos (ISO/IEC 27002, 2005). Existe no meio acadêmico uma quantidade grande de estudos voltados à análise de riscos de segurança, no entanto, muitos deles se baseiam em abordagens matemáticas, que fogem aos objetivos do trabalho apresentados na seção 1.3. Para o propósito desse trabalho foram observados apenas os trabalhos que focam em aspectos conceituais da análise de riscos.

A análise de riscos deve ser um processo que considera não apenas aspectos tecnológicos e ativos tangíveis, mas também que englobe ativos intangíveis (GERBER e VON SOLMS, 2005). Para tal, modelos de análise de risco focados em processos já foram sugeridos, reduzindo parte dos problemas existentes no acompanhamento de risco de ativos de segurança individuais (KHANMOHAMMADI, 2010). Com o mesmo objetivo, também já se sugeriu uma abordagem para lidar com as diversas interações necessárias para o monitoramento, a identificação e o tratamento de riscos entre os vários níveis organizacionais (MA, 2010).

Devido às mudanças existentes no cenário organizacional causadas por novas tendências tecnológicas como terceirização da infraestrutura de TIC, computação em nuvem e mobilidade, nota-se um grande interesse na consideração dessas tecnologias para análise de riscos.

Para terceirização de infraestrutura de TIC já foram desenvolvidos modelos de decisão com base nos riscos de segurança da informação (ZAVARSKY, RUHL, *et al.*, 2009) e modelos de suporte para identificação desses riscos (DOOMUM, 2008), (KHIDZIR, MOHAMED e ARSHAD, 2010). É possível também desenvolver modelos de negócio focados no planejamento e monitoramento do prestador de serviços,

através de abordagens focadas no risco que eles representam para o negócio (JAKOUBI, TJOA, *et al.*, 2010).

A computação em nuvem traz uma série de novos riscos para segurança da informação. Também para essa tecnologia, que é uma forma particular de terceirização de infraestrutura de TIC, foram desenvolvidos modelos de análise de risco e controle de requisitos de segurança da informação (ZHANG, WUWONG, *et al.*, 2010), (MÜLLER, HAN, *et al.*, 2011), (SCHNJAKIN, ALNEMR e MEINEL, 2010).

Assim como as demais tendências apresentadas, a tendência de mobilidade traz uma série de preocupações do ponto de vista de segurança, o que gera interesse de pesquisas. Algumas das análises relacionadas a esse tópico buscam a identificação e categorização das ameaças geradas pela mobilidade (GOODE, 2010), (LEAVITT, 2011), (AMOROSI, 2011). Também é possível encontrar estudos paralelos que identificam ameaças de segurança na convergência dos ambientes profissionais e pessoais (THORNGREN, ANDERSSON, *et al.*, 2004).

2.3. TRABALHOS RELACIONADOS

Não foram encontrados durante a pesquisa trabalhos que exploram diretamente a ideia de definir modelos de suporte para lidar com alterações profundas no cenário externo de segurança. No entanto, pode-se dizer que a pesquisa aqui apresentada combina elementos encontrados em diversos artigos que ajudaram e deram subsídios para a criação do modelo proposto de suporte a Sistemas de Gestão de Segurança da Informação (SGSI).

Inicialmente, o entendimento sobre a necessidade de melhorar a capacidade de segurança das organizações frente a cenários externos muito dinâmicos é explorada no artigo "*Addressing dynamic issues in information security management*", de Abbas (ABBAS, MAGNUSSON, *et al.*, 2011). Nele a teoria de Análise de Opções Reais[2] (ROA – *Real Options Analysis*) é utilizada para lidar com as incertezas causadas por problemas específicos. Entre esses problemas está a existência de requisitos dinâmicos de segurança causados por avanços

[2] A Análise de Opções Reais é uma técnica que permite a tomada de decisões com base na criação de árvores de decisão, que especificam a probabilidade de diversos cenários de evolução a partir de um estado inicial.

tecnológicos, tais como os que podem ser encontrados no cenário externo estudado por esse trabalho. No entanto essa abordagem é voltada para adaptações em controles de segurança muito específicos, os quais podem ser mais bem associados à fase de Execução *(Plan Do, Check, Act)* do que à fase de Planejamento do ciclo PDCA.

Também reconhecendo a necessidade de adaptações na abordagem de gestão de segurança frente ao cenário dinâmico de tecnologia, David Lacey apresenta o artigo "*Understanding and transforming organizational security culture*" (LACEY, 2010). No entanto adota uma abordagem bem mais generalista, buscando identificar quais são as dificuldades existentes nas tentativas de mudança da cultura de segurança em uma organização. Conclui indicando que para trabalhar com segurança no novo cenário tecnológico, é necessário que a proteção da informação seja natural para os profissionais. Contudo, o autor argumenta que isso só pode ser alcançado quando os programas de segurança corporativos derem mais atenção a pessoas do que à tecnologia, inclusive do ponto de vista de investimentos.

O artigo "*A Risk Management Process for Consumers: The Next Step in Information Security*", de André van Cleeff une as motivações dos dois trabalhos citados com a criação de ferramentas de suporte (VAN CLEEFF, 2010). No trabalho é proposto o desenvolvimento de um modelo a ser utilizado por qualquer pessoa para fazer a gestão do seu próprio conjunto de informações pessoais. Da mesma forma que uma organização pode criar um *software* para suportar o processo de análise de riscos, o trabalho mencionado sugere a criação de um software, só que para indivíduos, não organizações. Nesse software, o usuário iria listar suas informações críticas, associando a elas impacto de ataques, vulnerabilidades, ameaças e finalmente, riscos, da mesma maneira que uma organização faria. Apesar da ferramenta proposta pelo artigo ser ousada e de difícil implementação, ela traz em si a noção de que novas abordagens de segurança dependerão fortemente de pessoas e do conhecimento sobre conceitos de segurança que elas possuem. Além disso, também nota-se o posicionamento do indivíduo como responsável pela segurança da informação a sua disposição.

A ideia de propor modelos de suporte para a gestão de segurança é explorada em diversos artigos, conforme comentado anteriormente. No entanto, nenhum visa à adaptação de abordagens para lidar com novos cenários tecnológicos. Por exemplo, Anderson e Rachamadugu no artigo *"Information Security Guidance for Enterprise*

Transformation", apresentam um roteiro derivado em parte da própria ISO/IEC 27001 para a implantação de segurança (ANDERSON e RACHAMADUGU, 2006). Especificamente nesse caso, um dos objetivos da ferramenta criada é aumentar a conscientização sobre segurança nos estágios iniciais do planejamento, de forma a envolver equipes relevantes rapidamente. No modelo de suporte proposto por essa pesquisa, a mesma ideia é utilizada, mas busca um foco maior nas novas tendências tecnológicas logo na fase de Planejamento da ISO/IEC 27001.

Os trabalhos de Gilles, "*Improving the quality of information security management systems with ISO27000*" e de Milicevic e Goeken, *"Application of Models in Information Security Management*" também buscam a definição de modelos de suporte para a implantação da ISO/IEC 27001 (GILLIES, 2011), (MILICEVIC e GOEKEN, 2011). Ambos os artigos sugerem a necessidade de ferramentas de suporte para aumentar a adoção desse padrão, especialmente em pequenas e médias organizações.

O trabalho aqui proposto utiliza os elementos apresentados na construção de uma nova ferramenta para criação de SGSIs baseados na ISO/IEC 27001. Inicialmente, reconhece também as dificuldades existentes na criação desse tipo de sistema e identifica a transformação da cultura organizacional de segurança como um ponto chave para a solução do problema. Nesse contexto, o trabalho aqui desenvolvido utiliza a ideia de modelos de suporte para a ISO/IEC 27001. No entanto, esse modelo é focado especificamente na fase de Planejamento do SGSI e sobre a qual é aplicada uma série de restrições, derivadas da análise do cenário externo e suas tendências tecnológicas.

2.4. CONSIDERAÇÕES FINAIS

Apesar de se apoiar em trabalhos de dois campos de pesquisa em segurança da informação – Gestão de Segurança e Desenvolvimento de Sistemas de Informação Seguros –entende-se que o trabalho aqui proposto se encaixa no primeiro. Como características para essa categorização podem ser citados o forte embasamento em um padrão de SGSI, no caso o proposto pela ISO/IEC 27001, e o

desejo de criação de um modelo de suporte para a implantação desse tipo de sistema em uma organização.

Alguns dos artigos apresentados serviram como referências principais para a construção desse modelo de suporte. Nota-se que muitos dos elementos utilizados na construção do modelo de suporte já existem na literatura, mas nessa pesquisa foram adaptados e combinados de maneira inovadora, buscando a solução do problema proposto.

3. CONCEITUAÇÃO GERAL EM SEGURANÇA

Para sugerir adaptações na abordagem típica da ISO/IEC 27001 para criação de Sistemas de Gestão de Segurança da Informação (SGSI), é necessário o entendimento dos conceitos que fundamentam essa norma.

Nesse capítulo é apresentado, de maneira sumarizada, um histórico da evolução da segurança da informação, que culminou na criação de padrões de Gestão de Segurança, como é o caso da ISO/IEC 27001.

Também é apresentado um detalhamento das fases existentes na norma ISO/IEC 27001, visto que o modelo de suporte proposto deve focar em uma dessas fases, a de Planejamento.

3.1. EVOLUÇÃO DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O acesso à informação nunca foi tão fácil. Através das mídias digitais e conectividade à Internet, a informação necessária está ao nosso alcance a qualquer momento e em vários formatos. Pesquisas recentes indicam que devido a essa facilidade, a própria forma das pessoas pensarem sobre como lidar com suas atividades do dia a dia está mudando. Pessoas acostumadas com essa facilidade para acesso a informação armazenam cada vez menos detalhes, buscando, ao invés disso, guardar formas de localizar conteúdos (SPARROW, LIU e WEGNER, 2011). No entanto, essa facilidade traz como consequência uma maior probabilidade de incidentes de segurança, devido ao acesso generalizado a toda essa informação.

Outro ponto importante é que muitas das falhas de segurança que ocorrem não são ainda reconhecidas como incidentes de segurança da informação. Na verdade existe uma falta de conhecimento sobre o que é de fato a segurança da informação (VON SOLMS e VON SOLMS, 2004). Essa dificuldade tem origens compreensíveis: infelizmente a preocupação com a segurança da informação historicamente foi e continua sendo uma preocupação tecnológica (CORRISS, 2010).

A discussão sobre segurança da informação teve início no meio militar. Boa parte dos trabalhos iniciais no tema derivou da necessidade de proteger os

mainframes utilizados nesse meio. Além da implantação de controles de segurança física rígidos, era necessário garantir a segurança do sistema operacional desses equipamentos. Dessa forma, grandes esforços foram dedicados ao desenvolvimento de sistemas operacionais seguros e de técnicas de controle de acesso. Muitos desses esforços replicaram sistemas e processos de classificação das informações militares. Infelizmente, esses mesmos esforços não poderiam ser aproveitados para aumentar a segurança dentro dos novos paradigmas computacionais que estavam por vir. Isso porque no meio militar, os vetores de ataques[3] possíveis eram limitados, visto que era necessária uma grande quantidade de recursos financeiros e técnicos para explorá-los. Essa premissa deixou de ser válida na era da computação pessoal (ARCE e LEVY, 2003).

A chegada dos computadores pessoais na década de 80 revolucionou as formas de trabalho de muitas pessoas e organizações, mas também criou novos tipos de ameaças de segurança, sendo a principal delas os vírus. Apesar de serem disseminados basicamente por meios físicos, ou seja, a inserção de uma mídia contaminada em algum dispositivo de entrada, os vírus de computador tornaram-se muito comuns. Isso porque a grande quantidade de computadores pessoais criou o potencial para disseminação em grande escala. Os vírus de computador nessa época buscavam atacar a disponibilidade das informações, destruindo discos rígidos e desabilitando computadores. Era necessário proteger os sistemas computacionais contra essa ameaça. Criou-se assim, uma indústria de segurança completamente nova, focada na proteção dos sistemas com base em barreiras físicas e especialmente, na implantação dos primeiros antivírus via *software*.

Por meio das primeiras redes de computadores, já na década de 90, a quantidade de vetores de ataque aumentou exigindo novas contra medidas para proteção. Além disso, a troca de informações facilitou também o desenvolvimento de novas variantes de vírus existentes e formas de contornar os softwares antivírus. As redes de comunicação passaram, então, a ser vistas como o elemento comum que ligava todas essas ameaças. Para proteger tais redes e seus recursos computacionais, foram desenvolvidos *firewalls*[4] e outros dispositivos para a segregação de redes. Infelizmente, sendo criadas inicialmente em ambientes de

[3] O termo vetor de ataque é utilizado em segurança para especificar as diferentes formas que um sistema pode ser atacado.

[4] Firewall é um equipamento de rede que permite ou bloqueia tráfego de pacotes, de acordo com regras pré-estabelecidas ou construídas de forma dinâmica.

pesquisa, os primeiros protocolos e aplicações para redes de computadores não foram concebidos com uma preocupação excessiva com segurança.

O preço a pagar por essa simplificação foi sentido com a disseminação do uso da Internet. Os protocolos e aplicações anteriormente utilizados apenas localmente tiveram de evoluir para permitir a interconexão de redes e o uso em massa por todo o mundo. A falta de mecanismos de segurança no núcleo dessa infraestrutura traz até hoje problemas muito difíceis de resolver, como é o caso do spam de e-mail e ataques possíveis no *Domain Name System* (DNS). Adicionalmente, o uso da Internet em si exige que se evite que qualquer pessoa inadvertidamente coloque informações sigilosas no domínio público. Assim, foram criadas ferramentas de prevenção à perda de dados (DLP – *Data Loss Prevention*) e de controle de acesso individual a redes de computadores (VPN – *Virtual Private Network*), instaladas diretamente nas máquinas dos usuários finais.

Assim, desde a época dos primeiros mainframes até os dias atuais o ponto mais fraco da cadeia sempre foi visto como algum componente tecnológico do ambiente. Esse é o conhecido “jogo” de segurança que é jogado até hoje: atacantes desenvolvem novas ameaças e pesquisadores e organizações buscam formas de mitigar essas ameaças. Infelizmente, para cada salto de evolução nas medidas de proteção, é dado um salto ainda maior na complexidade dos ataques.

Essa abordagem de segurança pode parecer ineficiente, mas é uma das mais utilizadas. Mesmo com o desenvolvimento de técnicas preditivas de segurança, como análise de comportamentos e mitigação baseada em vulnerabilidades, as ameaças são sempre desenvolvidas por seres humanos com objetivos específicos (i.e. evitar a última defesa criada), e ainda não temos computadores capazes de competir de igual para igual com esse tipo de raciocínio. Isso não significa que não existem formas para melhorar a capacidade e velocidade de resposta a ameaças de segurança.

3.2. SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

Felizmente, as organizações perceberam logo que a informação em si, e não a mídia onde ela é armazenada é o que realmente precisa ser protegido. Pode parecer

um conceito relativamente óbvio, mas implica em se ter uma estratégia completamente diferente para lidar com segurança. Isso porque as organizações passam a entender que a informação pode estar presente em diversas formas na organização. Todas essas formas devem ser protegidas, o que envolve não só a abordagem de tecnologia, como também pessoas e processos (ISO/IEC 27001, 2005).

Nesse cenário, passou a existir um interesse cada vez maior pela criação de abordagens fim a fim para segurança da informação, que unissem além de recursos e melhores práticas voltadas à tecnologia, uma maior preocupação com segurança envolvendo pessoas e processos. Assim, começaram a serem implantados novos tipos de controles voltados à segurança da informação, que combinados aos controles tecnológicos existentes, tomaram forma de iniciativas estruturadas ou programas. Como exemplos de controles em geral, podem ser citados:

- Segregação de redes através de *firewalls*;
- Instalação de *softwares* antivírus nos computadores de usuários;
- Implantação de catracas eletrônicas para controle de acesso físico;
- Requisição de acompanhamento de terceiros durante visitas;
- Redação e distribuição de políticas de segurança da informação;
- Treinamentos para conscientização dos funcionários;
- Eliminação de impressões desnecessárias de documentos;
- Definição de procedimentos para descarte de documentos;
- Criação de comitês de segurança organizacional.

De fato a segurança da informação depende de todas essas componentes: pessoas e processos combinados com tecnologia (RAO e HERATH, 2009). A componente tecnológica nunca poderá ser abandonada, mas deve ser constantemente revista. As empresas de segurança criam a cada dia novos produtos, baseados em técnicas preditivas[5] e com maior capacidade de processamento. O grande desafio, no entanto, está nas componentes relacionadas às pessoas e aos processos: é necessário superar barreiras comportamentais

[5] Técnicas preditivas de segurança utilizam informações históricas coletadas sobre um sistema para identificar comportamentos e estados aceitáveis, tomando ações específicas no caso de detecção de uma situação desconhecida.

existentes e criar uma cultura para a utilização segura das informações. O comportamento seguro deve se tornar algo natural (CORRISS, 2010).

Nessa linha, percebe-se que quanto menos relacionada com tecnologia é o trabalho de uma pessoa, menos conscientizada com relação à segurança das informações ela está. Além disso, muitas vezes a conformidade com controles de segurança tem uma relação custo/benefício ruim para os usuários (HERLEY, 2009). O conceito de que a conscientização de pessoas é fundamental para a segurança da informação é relativamente recente. Muitos dos mais famosos ataques à informação foram realizados como uma combinação de conhecimento técnico e engenharia social (MITNICK, 2002). Infelizmente, mesmo hoje é raro encontrar pessoas que consigam detectar e evitar um ataque de engenharia social. Isso resulta em distorções de comportamento em relação à proteção das informações, as quais compõe o desafio existente ao lidar com pessoas e sua influência na segurança das informações.

Contribuindo para a gravidade do problema, não são todos os controles de segurança que são aplicáveis a qualquer tipo de organização. A decisão de aplicação ou não depende de um conhecimento profundo do contexto interno e externo de segurança. A decisão de aplicar controles inadvertidamente gera gastos desnecessários e contribui para a visão de que a segurança da informação não apresenta uma relação custo/benefício adequada. É necessário um processo contínuo de avaliação da situação e decisão sobre os mecanismos de controle a serem adotados e paulatinamente incorporados.

A partir dessa necessidade de uma abordagem para segurança da informação organizacional, melhores práticas foram incorporadas em diretrizes para o trabalho com segurança (SHARIATI, BAHMANI e SHAMS, 2010). Além dos controles de segurança típicos, essas diretrizes incluem também processos de análise de riscos para escolha de quais desses controles devem ser aplicados na organização. Por fim, estabelecem formas de garantir que as análises de riscos sejam refeitas continuamente, melhorando cada vez mais o grau de segurança da organização. Esses conjunto de diretrizes formam a base das abordagens dos chamados Sistemas de Gestão de Segurança da Organização (SGSI).

O SGSI mais conhecido atualmente é o definido pela *International Standards Organization* (ISO) na sua série 27000. A ISO/IEC 27001, em especial, fornece um modelo para o estabelecimento, operação, monitoração, revisão, manutenção e

melhoria de um SGSI (ISO/IEC 27001, 2005). Essa norma é conhecida como o guia de melhores práticas para organizações que desejam trabalhar com segurança da informação de maneira estruturada. Existem diversos outros padrões mundiais para criação de SGSIs (SIPONEN e WILLISON, 2009), mas devido ao reconhecimento dado a ISO/IEC 27001, o trabalho aqui desenvolvido será focado nesse padrão. Em agosto de 2012, o *International Register of ISMS Certificates* contava com 7940 organizações certificadas pelo mundo (IRIC, 2013). Apesar disso, os conceitos incorporados na ISO/IEC 27001 devem ser adaptáveis para outros padrões. A Figura 1 mostra como os principais modelos de SGSI podem se relacionar entre si.

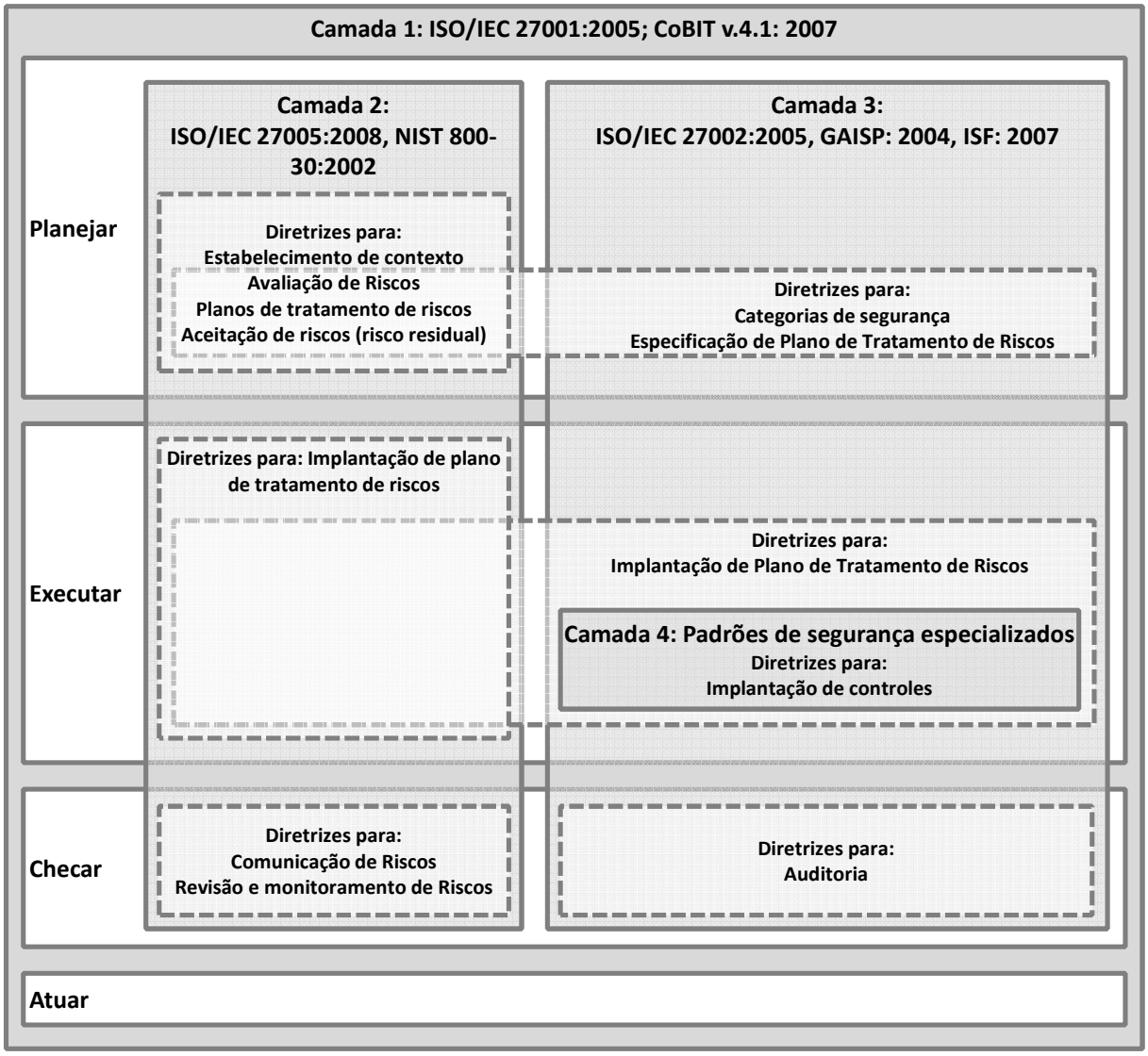

Figura 1 – Relação existente entre os diversos padrões de segurança e a ISO/IEC 27001 (TSOHOU, KOKOLAKIS, *et al.*, 2010)

Apesar das inúmeras vantagens, a implantação de um SGSI é uma tarefa complexa que exige esforços consideráveis de várias áreas da organização. Além disso, uma das maiores dificuldades da abordagem proposta nesse padrão é entender que ele não contém as atividades necessárias para a implantação das melhores práticas propostas. Assim, é essencial que o conteúdo dessas práticas seja assimilado e resulte em uma abordagem customizada para a organização.

3.3. A NORMA ISO/IEC 27001

O nome oficial em língua inglesa da ISO/IEC 27001 é "*Information Technology – Security Techniques – Information Security Management Systems – Requirements*". No Brasil, a ABNT publicou uma versão traduzida da norma, conhecida por NBR ISO/IEC 2700, com o título "Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos".

A ISO/IEC 27001 teve origem na publicação do *Department of Trade and Industry (UK DTI)* da Grã-Bretanha, intitulada "Código de Prática para Gestão da Segurança da Informação" em 1989 (GILLIES, 2011). Em 1995, o British Standards Institute (BSI) incorporou a norma e a publicou com o código BS7799. Em 2000, ela foi incorporada novamente, agora pela ISO, que a publicou sob o código ISO/IEC 17799. Em 2002, uma nova versão do padrão BS7799 é publicada pela BSI, não mais na forma de um código de prática, mas na forma de uma especificação de sistema de gestão, garantindo o alinhamento com outros sistemas, como o da ISO 9000. Finalmente, em 2005, a ISO/IEC 27001 é publicada, substituindo a ISO/IEC 17799 e com alinhamento completo com a última versão da BS7799.

A implantação de um SGSI baseado na ISO/IEC 27001 em uma organização apoia-se, como mencionado anteriormente, na aplicação de uma série de conceitos básicos e melhores práticas acumuladas por diversas organizações ao longo dos anos. A norma especifica um "modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)". O modelo mencionado pode ser observado na Figura 2. Nele, os requisitos de segurança são inseridos em ciclo de gestão que

inclui atividades de Planejamento, Execução, Checagem e Atuação (detalhados na sequência).

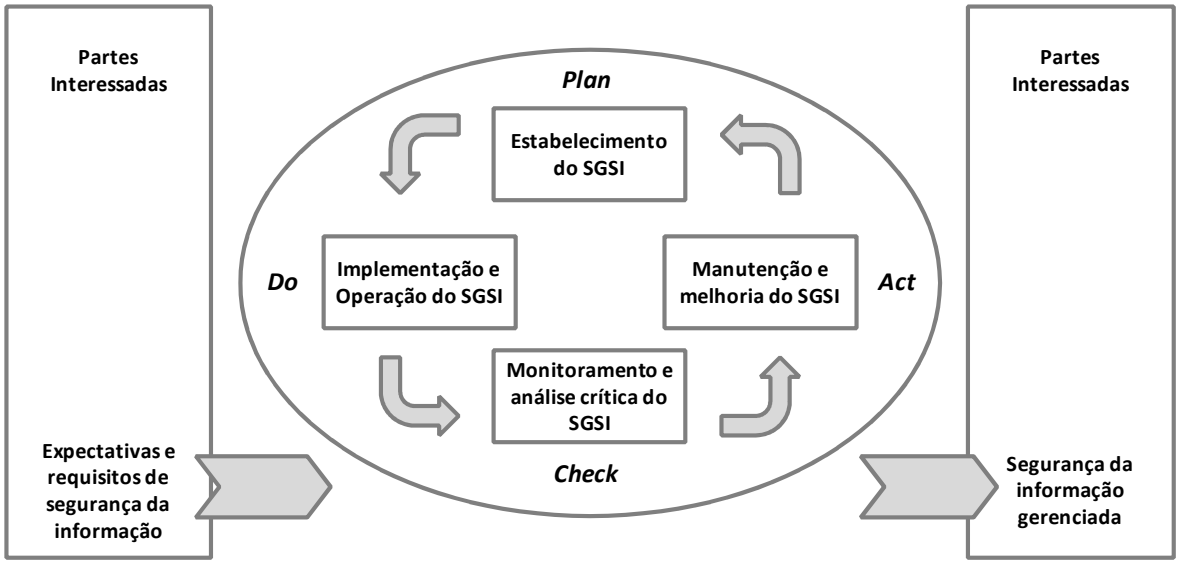

Figura 2 – Modelo de Sistema de Gestão de Segurança da Informação da ISO 27000 (ISO/IEC 27001, 2005)

Observando o ciclo proposto, fica implícita uma mensagem importante. A gestão da segurança não é um projeto, com início, meio e fim, mas sim uma atividade recorrente, baseada em constante planejamento, aplicação e revisão. Se o objetivo é garantir a segurança, e o cenário de segurança está em constante alteração, nada mais lógico que o processo interno de garantia de segurança esteja também em constante mudança.

O ponto de partida desse ciclo deve estar vinculado a um objetivo da organização. A ISO coloca como um dos o objetivos da segurança da informação “garantir a continuidade do negócio, minimizar o risco do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ISO/IEC 27002, 2005). Para muitas organizações, o retorno sobre as oportunidades de negócio se traduz em lucro. Assim a implantação de um SGSI visa algum retorno financeiro, direto ou indireto. O segundo caso é mais comum, como manutenção de negócios devido ao aumento da confiança de clientes e eliminação de investimento desnecessário em soluções tecnológicas.

Para alcançar esse objetivo, a implantação do SGSI e da segurança da informação depende da manutenção de algumas propriedades essenciais sobre a informação da organização. Em geral, são listadas como propriedades da informação a serem mantidas a Confidencialidade, a Integridade e Disponibilidade (CIA – *Confidentiality, Integrity and Availability*):

- **Confidencialidade**: a propriedade que a informação tem de que não será divulgada a entidades não autorizadas. Essa propriedade pode se referir ao conteúdo da informação ou a própria existência da informação. Controles de acesso ajudam a manutenção de confidencialidade da informação;
- **Integridade**: a propriedade que a informação tem de não ser alterada por entidades não autorizadas. Essa propriedade também se refere tanto quanto ao conteúdo da informação como a sua origem. Controles existem para permitir a prevenção contra ataques a integridade ou a detecção de ataques que já aconteceram.
- **Disponibilidade**: a propriedade que a informação tem de que estará disponível para as entidades autorizadas. A indisponibilidade de uma informação é quase tão ruim quando a inexistência da informação.

A atenção a essas propriedades tende a garantir proteção adequada para boa parte das organizações. Além disso, muitas outras propriedades que podem ser atribuídas para a informação podem ser mantidas se o CIA for mantido (BISHOP, 2003). É importante ressaltar, no entanto, que o contexto de cada organização é diferente. É possível considerar determinadas propriedades adicionais, para fins de adequação à cultura organizacional.

A última afirmação reflete mais um conceito importante no estabelecimento de um SGSI: cada organização deve customizar a sua abordagem para segurança da informação. Apesar de algumas regras gerais – no caso, as melhores práticas da ISO/IEC 27001 – serem vitais, muitos dos passos dados por uma organização podem não ser adequados para outra organização, levando-as ao fracasso na implantação do SGSI. Essa também é uma razão para a existência de modelos de suporte para essas atividades, como o que é desenvolvido neste trabalho.

É importante compreender que a “Segurança” deve estar sempre próxima da “Informação”. Ter essa meta clara dentro do processo do SGSI é crítica para seu

sucesso. A lembrança contínua dessa regra facilita a implantação de mecanismos de proteção em locais onde eles tendem a ser esquecidos. Por exemplo, esse é caso de áreas que lidam com pouca tecnologia e tendem a acreditar que a informação armazenada em um formulário, registrada em uma embalagem nunca será uma informação relevante a ser protegida. A consequência é um SGSI cada vez mais maduro e com visibilidade de todos os pontos da organização onde determinada informação é manipulada.

3.4. FASES DO SISTEMA DE GESTÃO DA ISO/IEC 27001

A ISO/IEC 27001 propõe 4 etapas para o estabelecimento de um SGSI: Planejar (*Plan*), Executar (*Do*), Checar (*Check*) e Atuar (*Act*). Essas fases compõem um ciclo conhecido como PDCA, o qual é baseado em um conceito da teoria de qualidade conhecido como Roda de Deming e aplicado inicialmente por Shewhart (GILLIES, 2011). Esse ciclo deve ser executado continuamente na organização buscando, a cada rodada, o aperfeiçoamento dos mecanismos de segurança.

A primeira etapa desse ciclo, o Planejamento, é o foco desse trabalho e corresponde a um momento crítico no ciclo de implantação. Nessa etapa são executadas duas atividades principais: a elaboração da política de segurança do SGSI e a análise de riscos.

A política de segurança é estabelecida definindo as diretrizes gerais da organização em relação ao tratamento de segurança da informação. Nela são estabelecidas as definições do tipo de informação a ser protegida e as responsabilidades sobre a informação. Com base nas definições da política de segurança, a análise de risco é executada, considerando as vulnerabilidades e ameaças de cada ativo de informação. O resultado da análise é a definição de mecanismos de segurança que devem ser implantados, consolidados nos planos de tratamento de riscos.

A ISO/IEC 27001 apresenta no seu Anexo A uma lista de controles que pode servir de referência para a criação do plano de tratamento de riscos previstos no Planejamento. Esses controles foram detalhados na forma de um Código de Prática para a Gestão da Segurança da Informação na ISO/IEC 27002. Para fins de

auditoria, a organização deve gerar ao fim do Planejamento um documento chamado Declaração de Aplicabilidade (SoA – *Statemento of Aplicability*) que indica quais desses controles são aplicáveis ao contexto organizacional e quais não são, justificando a não aplicabilidade. A norma apresenta também, dentre esses controles da ISO/IEC 27002, quais provavelmente devem estar presentes em todas as organizações, criando um ponto de partida para implantação do SGSI. No entanto, deixa claro que apesar dos controles do Anexo A serem importantes para a maior parte das organizações, essas devem levar em consideração novos controles que julgarem necessários (ISO/IEC 27002, 2005).

Na segunda etapa do ciclo, Execução, são colocadas em prática as iniciativas definidas na etapa anterior. Nessa etapa novos processos são desenhados e executados, processos em andamento são modificados, soluções tecnológicas implantadas e programas de conscientização disseminados, sempre de acordo com os planos definidos. Nessa etapa em muitos casos podem ser utilizados os controles apresentados no Anexo A da ISO/IEC 27001.

A etapa de Execução deve ser estar sempre ancorada nos resultados da análise de risco. Os resultados da análise de risco levam em consideração as prioridades da organização quanto a investimentos e cultura organizacional. Ações definidas sem um planejamento adequado tendem a trazer à prática medidas paliativas que geram investimentos desnecessários sem grandes benefícios do ponto de vista de segurança.

A etapa de Checagem, terceira do ciclo, identifica através de análises qualitativas e quantitativas, se os mecanismos implantados estão atingindo os resultados esperados durante a análise de risco. Em geral, durante essa etapa é realizada uma revisão da análise de risco considerando as medidas implantadas. O resultado dessa etapa é a visualização do risco residual ao qual está sujeita a organização. A partir daí devem ser definidos os planos de ação para lidar com os riscos residuais encontrados.

A última etapa do ciclo, Atuação, busca a revisão das definições da fase de Planejamento, de forma que os desvios observados durante a execução do ciclo atual não se repitam para o próximo ciclo. A etapa de Atuação traz para o SGSI a capacidade de acompanhar mudanças internas e externas da organização, realizando uma análise crítica do que foi feito e buscando alternativas de melhoria.

As mudanças sugeridas através da análise crítica podem alterar completamente o SGSI, desde que visem uma garantia melhor da segurança da informação.

3.5. CONSIDERAÇÕES FINAIS

As discussões sobre segurança tiveram início com controles baseados puramente em tecnologia. Com o aumento da complexidade de sistemas e da quantidade de informação disponível para acesso, notou-se que esses controles não eram suficientes. Eram necessários, além de controles baseados em tecnologia, aqueles também focados em pessoas e processos.

Os SGSIs foram criados para consolidar essa visão dentro das organizações, desenvolvendo práticas de revisão contínua de riscos de segurança e aplicação de controles diversos de acordo com o contexto. A ISO/IEC 27001, principal referência para definição de SGSI atualmente, traz uma abordagem baseada em 4 etapas distintas: Planejamento, Execução, Checagem e Atuação.

Infelizmente, essa abordagem pode não ser eficiente ao tentar assimilar grandes alterações no cenário externo. O modelo de suporte proposto nesse trabalho é focado na etapa de Planejamento da ISO/IEC 27001 e busca adequá-la para as mudanças introduzidas por esse cenário externo. Essas mudanças são detalhadas no próximo capítulo.

4. CARACTERIZAÇÃO DO CENÁRIO EXTERNO

As principais fontes de requisitos para a segurança da informação são os princípios e cultura organizacionais, legislações e normas aplicáveis e principalmente, a análise de risco (ISO/IEC 27002, 2005). Os princípios e cultura organizacional representam os valores, as diretrizes e a missão da organização. Esses tipos de conceitos alteram-se pouco ao longo do tempo de vida de uma organização. Da mesma forma, as legislações e as normas aplicáveis constituem-se em fontes de requisitos que apresentam pouca variação. Assim, tendo implantado um conjunto de ações focados no atendimento desses requisitos, existem poucas alterações a serem feitas durante o funcionamento do SGSI.

No entanto, o mesmo não acontece para os requisitos derivados da análise de riscos. O grande desafio da segurança da informação sempre foi acompanhar os riscos gerados pela situação do cenário externo. Novas tecnologias, novas formas de comportamento e relações sociais geram novos vetores de ataques que precisam ser controlados e evitados.

Dentre essas diversas componentes do cenário externo, a tecnologia é a que mais influencia as decisões de segurança. Como apresentado, a gestão de segurança da informação é uma teoria relativamente nova, onde boa parte dos conceitos tende a estar vinculada ao contexto tecnológico. Na medida em que o contexto tecnológico se altera, a gestão de segurança também precisa ser alterada. Por exemplo, a criação de dispositivos de análise de tráfego passou a ser importante na medida em que as redes se tornaram mais comuns. Da mesma forma, antivírus evoluíram para *antimalwares*[6] na medida em que as ameaças existentes passaram a assumir outras formas, como *phishing*[7], *trojans*[8] e *spam*.

No entanto, acompanhar essas tendências está se tornando cada vez mais complexo, pois o cenário externo traz mudanças cada vez mais disruptivas. Para caracterizar esse cenário nesse trabalho, foram escolhidas três grandes tendências

[6] *Malware* é um termo utilizado para descrever qualquer tipo de ameaça em software. Isso acontece, pois atualmente existem diversos tipos de ameaças (trojans, phishing, spam, etc.), que vão além dos antigos vírus de computador. *Antimalware* é uma ferramenta criada para proteger sistemas de todo tipo de *malware*.

[7] *Phishing* é uma fraude onde um usuário é levado a revelar informações sensíveis através do direcionamento desse usuário para sistemas falsos com aparência de sistemas legítimos.

[8] *Trojan* é uma aplicação não autorizada criada para se instalar em um sistema hospedeiro e coletar dados específicos, os quais são posteriormente enviados para uma entidade externa.

tecnológicas: a utilização cada vez maior de terceirização de infraestrutura de TIC, computação em nuvem e a mobilidade. De fato, analistas de mercado de TIC reconhecem essas tendências como chave para os próximos anos de forma recorrente (GARTNER, 2010) (GARTNER, 2011), (GARTNER, 2012), (IDC, 2011), (IDC, 2012). Além disso, essas tendências são reconhecidas como definitivamente impactantes para a segurança da informação (GARTNER, 2013).

A seguir são apresentadas com maiores detalhes as tendências tecnológicas mencionadas, que caracterizam esse novo cenário externo. Na sequencia os riscos gerados por elas são listados e analisados de forma a fornecer insumos para o desenvolvimento do modelo de suporte à fase Planejamento da ISO/IEC 27001.

4.1. TERCEIRIZAÇÃO DE INFRAESTRUTURA DE TIC

Por mais eficiente que seja a operação de uma organização, ela sempre será pressionada a reduzir custos e otimizar ainda mais suas operações. É uma busca constante para garantia da sua sobrevivência dentro da sua área de atuação. No entanto, na medida em que esse tipo de otimização é feita, muitas delas se encontram em uma posição onde não é mais possível contar com os recursos internos para continuar evoluindo nesse sentido. A forma encontrada por muitas organizações para dar continuidade a esse processo é a terceirização, ou seja, a transferência de determinadas atividades para terceiros. Nesse processo, conhecido como Terceirização de Processos de Negócio (BPO – *Business Process Outsourcing*), essas atividades passam a ser contratadas como serviços. Outros motivos para essa decisão incluem a falta de conhecimento interno para operar determinado sistema, redução de pessoal interno e a possibilidade de maior foco na atividade principal da organização (JAKOUBI, TJOA, *et al.*, 2010).

No entanto, é possível ir além. O desenvolvimento tecnológico atual permite a terceirização não só das atividades em si, mas também da infraestrutura de suporte a essas ou outras atividades. Nesse formato, o *hardware* e o *software* envolvidos são disponibilizados para a organização já instalados e configurados, em um pacote único e no formato de serviços. Além da infraestrutura em si, toda uma gama de recursos necessários para a operação da organização também é inclusa no pacote,

tais como processos de atendimento, monitoração, atualização e suporte a incidentes. Entre os tipos de infraestrutura comumente oferecidos podemos citar Telefonia IP, Correio Eletrônico, Portal Web, Data Center, *Desktops/Notebooks* e até soluções mais complexas, como as de segurança – *Firewalls*, VPN (*Virtual Private Network*) e IDS (*Intrusion Detection System*) / IPS (*Intrusion Prevention System*).

Esse formato de contratação vem se espalhando rapidamente no mundo corporativo (KHIDZIR, MOHAMED e ARSHAD, 2010). Nele, a organização não precisa mais se preocupar com investimentos e processos típicos necessários para a operação desse tipo de infraestrutura, tais como instalação de atualizações de *software* e *hardware*, controle de desempenho, escalabilidade e treinamento de equipe de suporte. Isso traz a vantagem de permitir que esses investimentos sejam direcionados para outras iniciativas, mais próximas das atividades principais de negócio.

Existem diferentes formas para terceirização de infraestrutura, as quais variam de acordo com o escopo da contratação – o tipo de infraestrutura necessária – e os requisitos da organização – controle, monitoração, segurança. De maneira geral, as formas de terceirização são variações de modelos centralizados e descentralizados.

O modelo centralizado típico é o baseado em uma solução única que pode ser configurada para atender diversos clientes. Em geral essa solução fica localizada em um ambiente controlado, como um Data Center, que é conectado por meio de enlaces de dados a sistemas computacionais secundários, localizados fisicamente nos clientes. Esses sistemas podem ou não fazer parte do escopo de contratação de serviços. Esse modelo apresenta a vantagem de ter custos menores, já que permitem ao fornecedor do serviço o compartilhamento de recursos centralizados entre alguns clientes. Em geral nesse modelo, a cada novo cliente é necessário a reconfiguração da solução centralizada para atender ao novo escopo, o que pode ser feito de maneira total ou parcialmente manual. Como é visto a seguir, em modelos de computação em nuvem a necessidade de interação manual é bem menor. É importante observar que nem toda terceirização de infraestrutura de TIC (Tecnologia da Informação e Comunicação) utiliza modelos de computação em nuvem, apesar de ser comum usar o termo “Infraestrutura como serviço (IaaS – *Infrastructure-as-a Service*)” quando se fala sobre computação em nuvem.

O modelo descentralizado típico é o baseado na oferta de uma versão local da solução que foi terceirizada pelo cliente. Nesse caso, o provedor de serviços precisa

de equipes e infraestrutura mais numerosas para atender diversos clientes, visto que as equipes tendem a ser mais dedicadas. Apesar de em geral apresentar um custo maior, esse tipo de modelo tende a permitir uma maior adequação dos serviços prestados às necessidades do cliente, uma vez que a solução não será compartilhada com outros.

Também é comum que os próprios provedores desses serviços contratem, por sua vez, outros terceiros para realizar parte de suas atividades, criando uma cadeia de empresas utilizadas para terceirização de uma atividade.

Independente do modelo adotado, a terceirização de infraestrutura de TIC passa informações da organização para o controle de terceiros (DOOMUM, 2008). Dessa forma, é crucial para todo processo desse tipo o entendimento dos riscos de segurança da informação envolvidos. Se por um lado muitas organizações entendem que o planejamento da segurança da informação durante o processo de terceirização é complexo, por outro todas elas sabem dos benefícios de praticá-lo (KHIDZIR, MOHAMED e ARSHAD, 2010).

É importante reconhecer que apesar da potencial existência de novos riscos de segurança da informação no processo de terceirização de infraestrutura de TIC é provável que outros riscos sejam mitigados. Isso acontece devido à especialização que os provedores de serviços costumam apresentar, uma vez que possuem a experiência para atender demandas de diversos clientes e o conhecimento técnico necessário para tal.

4.2. COMPUTAÇÃO EM NUVEM

A computação em nuvem pode ser entendida como uma abordagem revisada de terceirização de infraestrutura de TIC. Apesar de ainda não ser possível contratar qualquer tipo de serviço de infraestrutura através de computação em nuvem, ela está se disseminando de maneira sem precedentes no mundo corporativo.

A definição apresentada pelo NIST (*National Institute for Standards and Technology*) para computação em nuvem é uma das mais aceitas atualmente e engloba todos os níveis de complexidade. Por isso será utilizada aqui para apresentar essa tecnologia. Nela, a “computação em nuvem é um modelo para

permitir o acesso via rede a um conjunto compartilhado de recursos de computação de forma ubíqua, conveniente, sob demanda, o qual possa ser rapidamente provisionado e liberado com mínimo esforço ou interação com provedores de serviço" (NIST, 2011).

Para permitir toda essa alta escalabilidade, flexibilidade e baixos custos, essa abordagem apoia-se fortemente em tecnologias de virtualização, ou seja, a criação de múltiplos equipamentos virtuais em equipamentos físicos. Os últimos avanços dessa tecnologia possibilitam não só a criação dinâmica de novas instâncias virtuais de equipamentos, mas também a movimentação dessas instâncias através de equipamentos e sistemas computacionais conectados por redes de comunicação ao redor do mundo. Isso permite que novos serviços sejam aprovisionados e liberados de maneira automática e sem esforço humano, o que constitui uma das principais diferenças entre computação em nuvem e terceirização típica de infraestrutura de TIC.

Segundo o NIST, são também especificados as 5 (cinco) características básicas de serviços de computação em nuvem:

- **Auto-serviço sob demanda** – Capacidade de um consumidor solicitar e provisionar unilateralmente novas unidades de recurso, como espaço de armazenamento ou tempo de processamento.
- **Amplo acesso via rede** – Todas as funcionalidades estão disponíveis pela rede, através de mecanismos padronizados de acesso, utilizados por diferentes tipos de clientes ou dispositivos.
- **Recursos compartilhados** – Todos os recursos são agregados de forma que possam ser oferecidos a múltiplos consumidores, com unidades sendo atribuídas a um ou outro cliente de acordo com a demanda. Deve existir uma incerteza a respeito da localização física dos recursos oferecidos, tais como espaço de armazenamento, memória e processamento.
- **Elasticidade rápida** – Os recursos são alocados e liberados automaticamente de maneira eficiente de acordo com a demanda. Esse processo é transparente para os usuários, que devem entender a existência de um número ilimitado de recursos.

- **Serviços mensuráveis** – O provedor de serviços deve ter à sua disposição ferramentas para monitorar e reportar o uso de cada tipo de recurso.

Observando essas características, pode-se notar a baixa necessidade de interação humana (“Auto-serviço sob demanda”), alta conectividade (“Amplo acesso via rede”) e utilização do mesmo recurso por diversas entidades (“Recursos compartilhados”). A partir dessas características, é possível também tecer diversos questionamentos sobre a segurança da computação em nuvem. Nas próximas seções, esses questionamentos são explicitados, formando a base para a construção do modelo de suporte para a fase de Planejamento da ISO/IEC 27001.

Ainda na definição do NIST são especificados 3 (três) modelos de serviços:

- **Software como Serviço** (SaaS – *Software as a Service*) – Acesso a uma aplicação a partir de clientes diferentes, como é o caso do acesso a partir de um navegador web.
- **Plataforma como Serviço** (PaaS – *Platform as a Service*) – Disponibilização de plataformas de desenvolvimento para utilização do cliente, como por exemplo uma plataforma de criação de software.
- **Infraestrutura como Serviço** (IaaS – *Infrastructure as a Service*) – Alocação de recursos de infraestrutura referentes a processamento, armazenamento ou comunicação.

No mercado esses três serviços básicos foram combinados e transformados nas mais variadas ofertas para computação em nuvem, gerando até um novo termo para descrever esse fenômeno: Tudo como Serviço (EaaS ou XaaS – *Everything as a Service).* Além disso, em muitos casos os serviços de nuvem oferecidos passam a ser dependentes entre si. Por exemplo, é comum que aplicações no modelo SaaS utilizem serviços de armazenamento no modelo IaaS.

Em nenhum desses modelos é oferecida ao cliente visibilidade ou controle sobre a infraestrutura de hardware ou software que suporta o serviço prestado. Isso resulta em mais camadas de abstração da infraestrutura e, portanto menor grau de controle para o cliente final. Por um lado isso é uma vantagem para os clientes, que não precisam se preocupar com quase nenhum aspecto de infraestrutura, como é esperado do processo de terceirização. Por outro lado, essa característica traz

diversos pontos de dúvida quando se considera a segurança das informações armazenadas nessa infraestrutura.

Finalmente, o NIST especifica 4 (quatro) modelos de implantação:

- **Nuvem Privada** – Somente disponível para uma única organização, fornecendo serviços para várias unidades dentro dessa organização.
- **Nuvem Comunitária** – Disponível para diversas organizações com um interesse comum.
- **Nuvem Pública** – Disponível para o público em geral
- **Nuvem Híbrida** – Combinação dos modelos acima, utilizando tecnologias padronizadas para portabilidade de dados e aplicações

A existência de nuvens comunitárias e públicas traz um efeito muito interessante relacionado à computação em nuvem: a possibilidade de utilização da tecnologia por diversos tipos de organizações e com tamanhos variados. Na computação em nuvem, ao contrário de outros modelos de terceirização, existe a necessidade de pouca customização e esforço para se dar início à prestação de serviços. Assim, os investimentos necessários são menores, abrindo espaço para empresas menores utilizarem esse tipo de serviço.

Também contribui para uma maior utilização por organizações diversas, a característica de serviços mensuráveis da computação em nuvem. Não é interesse de nenhuma organização pagar por recursos não utilizados. Isso é o que acontece no modelo de terceirização típica, onde normalmente se paga um valor fixo mensal. Já nos serviços de computação em nuvem, a situação é diferente, pois a tecnologia utilizada permite a cobrança por unidade de recursos – hora, gigabyte ou sessão – utilizada.

Aliada a técnicas da Web 2.0[9], boa parte das soluções em computação em nuvem está disponível via web, ou possui API (*Application Program Interface*) desenhadas para viabilizar o acesso aos recursos da nuvem por qualquer aplicativo ou dispositivo. Não existem níveis mínimos para contratação – uma organização pode solicitar desde uma unidade de recurso até centenas e pagar por isso um preço que escala de maneira linear. De um lado, isso atraiu pequenas organizações

[9] Web 2.0 é um termo utilizado para descrever aplicações web onde o conteúdo apresentado é carregado de forma dinâmica e muitas vezes interativa

que não podem arcar com custos de aquisição de infraestrutura própria, mas dependem dela para operar seus negócios. Do outro lado, os provedores de computação em nuvem conseguiram capturar uma faixa de clientes que não estava disposta a pagar altas mensalidades para a contratação de serviços.

Outro ponto a destacar para a computação em nuvem é que é possível encontrar cada vez mais colaboradores dentro de uma organização que utilizam essa tecnologia pela facilidade que ela oferece e a variedade de serviços disponíveis. Em muitos casos, o serviço utilizado para benefício pessoal é o mesmo serviço na nuvem disponibilizado para a organização na qual ele atua. Assim a computação em nuvem começa a diminuir a separação entre a infraestrutura organizacional e a infraestrutura pessoal do usuário, o que também pode ser preocupante do ponto de vista de segurança da informação.

Ao que tudo indica, a flexibilidade oferecida por esse modelo deverá ser acompanhada por um maior entendimento, tanto por organizações como pelos indivíduos, do que se constitui a segurança da informação. Organizações precisarão investir mais recursos na conscientização de usuários dos serviços de nuvem sobre esse assunto, de forma que tais usuários consigam identificar novos riscos a sua frente e evitá-los, sem depender de controles previamente estabelecidos.

4.3. MOBILIDADE

Talvez a mais clara tendência existente no cenário externo às organizações é a necessidade de mobilidade cada vez maior das pessoas. Todos precisam estar conectados todo tempo, seja para obter novas informações, conversar com parceiros e clientes ou executar quaisquer atividades profissionais. O desenvolvimento de tecnologias de comunicação sem fio mais baratas e de maior qualidade possibilitam que essa necessidade seja cada vez melhor atendida. A mobilidade está sendo largamente incorporada dentro dos ambientes organizacionais e, portanto, deve também ser considerada na análise desse cenário externo.

Por causa da mobilidade, dispositivos diferentes cada vez mais são utilizados para realizar todo tipo de atividades. A explosão do uso de telefones *smartphones*, *tablets* e computadores portáteis fizeram com que os serviços normalmente

disponibilizados apenas para os *desktops* fossem disponibilizados também para esses dispositivos. Antes reservados a tarefas simples como a leitura de e-mail, os novos dispositivos possuem recursos mais que suficientes para realização de tarefas cada vez mais complexas, como edição de vídeo, navegação web e manipulação de documentos.

Nesse novo contexto, ocorrem mudanças de paradigmas de trabalho para as organizações. Por exemplo, ao trabalhar com uma ferramenta SaaS (*Software-as-a-Service*) que está disponível na Internet, o funcionário não está mais limitado a usá-la quando conectado localmente à rede do trabalho. Como apresentado, uma das características da computação em nuvem é o acesso de diversos clientes (“Amplo Acesso via Rede”). Na verdade, o usuário não está mais limitado à utilização de meios de acesso fornecidos pela organização da qual faz parte. Assim, é cada vez mais comum o uso de dispositivos pessoais, conectados à Internet para realização de trabalhos profissionais.

Cada novo dispositivo utilizado traz consigo um pacote novo, formado por sistema operacional, funcionalidades, método de acesso, protocolos e grau de conhecimento do usuário. Com isso, também trazem novas falhas, incompatibilidades, *bugs* de *software* e lacunas de recursos que podem originar diversos tipos de ameaças. Soma-se a tudo isso o fato de boa parte dos fabricantes desses dispositivos estarem preocupados com a inclusão de novas funcionalidades nos seus produtos, deixando a segurança em segundo plano (LEAVITT, 2011).

Controles típicos aplicados em segurança incluem testes, homologação e aceitação de dispositivos. Nesse novo cenário, onde novos dispositivos aparecem de acordo com a vontade dos usuários, isso não é possível. Assim, é importante repensar a forma de lidar com segurança para esses dispositivos dentro do contexto de mobilidade.

4.4. CONSIDERAÇÕES FINAIS

As tendências tecnológicas que se apresentam no cenário externo atual trazem, definitivamente, muitos benefícios para as organizações que as adotam.

Entre esses benefícios estão a maior escalabilidade, maior flexibilidade, maior velocidade para configuração e menores custos de implantação e manutenção.

No entanto, a utilização dessas tecnologias exige uma série de mudanças internas que devem ser levadas em consideração pela organização. Uma das avaliações mais importantes a serem feitas está relacionada à segurança da informação.

No caso da terceirização de infraestrutura e TIC e computação em nuvem, as informações da organização passam a estar sob o controle de terceiros. Isso significa que a organização precisa se certificar que esses são capazes de atender requisitos de segurança especificados por ela. No caso da mobilidade, a informação da organização passa a ser acessada de diversas localidades, através de infraestrutura, em muitos casos, desconhecida. Novamente, a organização precisa se atentar para esse ponto.

Quando consideradas em conjunto, essas tendências tecnológicas criam ainda mais riscos para a segurança da organização. Esses riscos serão analisados nos próximos capítulos, como base para a construção do modelo de suporte proposto.

5. RISCOS IDENTIFICADOS PARA O CENÁRIO EXTERNO

Com base no apresentado, fica claro que mudanças significativas estão em andamento dentro das organizações devido a novas tendências tecnológicas. No passado o trabalho era feito basicamente durante o horário comercial, fisicamente dentro da empresa, suportado por infraestrutura própria e por funcionários da própria organização. Atualmente o trabalho é executado a qualquer horário, de qualquer lugar, através de qualquer dispositivo, suportado amplamente por infraestrutura contratada de terceiros na modalidade de serviços.

Quando combinada com a necessidade das organizações atuais de proteger as informações necessárias ao seu negócio, essas mudanças geram uma série de incertezas relacionadas à segurança. Por causa disso, existe interesse em caracterizar quais são essas incertezas e propor soluções para elas. A seguir é apresentado um levantamento dessas incertezas com base em estudos relacionados às três tendências tecnológicas apresentadas anteriormente: terceirização de infraestrutura de TIC, computação em nuvem e mobilidade.

De forma a criar as bases para a construção do modelo de suporte proposto, objetivo principal dessa pesquisa, foram também listados e consolidados os riscos identificados referentes a cada tendência tecnológica. A versão completa das listas está disponível nos ANEXOS A, B e C.

Para a criação dessas listas de riscos foram adotadas algumas medidas. Dentro da teoria de análise de riscos, sabe-se que um risco é uma combinação entre uma vulnerabilidade em um ativo de informação, a probabilidade de uma ameaça explorar a vulnerabilidade e o impacto do ataque à informação (GERBER e VON SOLMS, 2005). Assim, dada uma vulnerabilidade ou ameaça identificada, a existência do risco depende do contexto de cada organização, ou seja, à existência de uma ameaça e vulnerabilidade associáveis entre si. Colocando de outra forma:

- Ativo de informação – Elemento que contém ou lida com a informação. Ex.: servidor, funcionário, processo de fechamento de orçamento.
- Vulnerabilidade de Segurança – Uma fraqueza do ativo de informação que permite que uma ameaça o explore. Ex.: versão desatualizada de sistema operacional, falta de treinamento, processo não documentado.

- Ameaça de Segurança – Potencial acontecimento que faz com que um ativo se comporte de maneira indesejável. Ex.: atacantes externos (*hackers*), vírus de computador, fenômenos naturais (enchentes, furações).
- Impacto – Representação quantitativa ou qualitativa do ativo de informação mediante a exploração de uma vulnerabilidade por uma ameaça de segurança. Ex.: moeda corrente, reputação, confiança.
- Risco de Segurança – Combinação do impacto com a probabilidade de exploração de uma vulnerabilidade por uma ameaça a um ativo de informação.

Para alguns dos estudos citados a seguir, são mencionados riscos de segurança, com as devidas ressalvas a respeito de vulnerabilidades e ameaças. No entanto, muitos estudos e relatórios não apresentam esse mesmo rigor. Assim, são apresentadas listas apenas de ameaças, vulnerabilidades, ou mesmo termos menos técnicos como “preocupações” ou “dúvidas”. Nesses casos, foi adotada a premissa da existência de um contexto tal que o risco se torne real, para que esse risco pudesse ser apresentado.

Finalmente, para facilitar o entendimento é feita uma categorização dos mesmos com o seu grau de relacionamento com processos, pessoas e tecnologia. Também são feitas análises qualitativas que funcionam como um guia preliminar para a construção do modelo de suporte proposto nesse trabalho.

5.1. ANÁLISE – TERCEIRIZAÇÃO DE INFRAESTRUTURA DE TIC

A terceirização pode ser resumida na troca do controle sobre os dados e serviços disponibilizados pela infraestrutura atual pelo acesso ao conhecimento e experiência de gestão disponibilizada pelo provedor de serviços. No entanto, a responsabilidade sobre a segurança dos serviços prestados continua na organização, o que traz a necessidade de um efetivo gerenciamento do serviço prestado pelo provedor de serviços (JAKOUBI, TJOA, *et al.*, 2010). Assim, a segurança é uma das principais preocupações existente na terceirização de

infraestrutura de TIC (KHIDZIR, MOHAMED e ARSHAD, 2010) e, portanto envolve decisões importantes. Nessa troca, deve ser objetivo da organização tentar reduzir ao máximo os riscos causados pelas novas ameaças trazidas pela terceirização. Infelizmente, esse objetivo parece não ser perseguido pela maioria das organizações (DOOMUM, 2008).

A Tabela 1 a seguir apresenta alguns exemplos de riscos identificados referentes à terceirização de TIC. A lista completa, sobre a qual se baseiam as considerações a seguir, está disponível no

ANEXO A – RISCOS – TERCEIRIZAÇÃO DE INFRAESTRUTURA DE TIC.

ID	DESCRIÇÃO DO RISCO	REFERÊNCIA	CLASSIFICAÇÃO
RT.1	Risco de não conformidade com legislação aplicável	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos
	...		
RT.20	Risco de ameaças internas como o acesso indevido a dados, divulgação de dados confidenciais e pouco treinamento em conscientização e segurança	(DOOMUM, 2008)	Pessoas
	...		
RT.22	Risco de não existência de recursos de segurança física como câmeras, sistemas de controle de incêndio e acordos de nível de serviço e segurança	(DOOMUM, 2008)	Tecnologia

Tabela 1 - Exemplos de riscos identificados referentes à Terceirização da Infraestrutura de TIC

Observando os riscos mapeados de uma maneira geral nota-se uma predominância daqueles relacionados a processos. Isso deve-se ao fato de que a prestação de serviços envolve certo grau de padronização de processos para o atendimento a diversos tipos de clientes. Em muitos casos, isso obriga as organizações a se adequarem aos processos do provedor de serviço, apesar de muitas organizações esperarem justamente o contrário. Se o alinhamento dos processos básicos de gestão da infraestrutura em questão é uma tarefa complexa, o alinhamento de práticas de segurança com o provedor de serviços é ainda mais.

A organização precisa estar ciente que a transferência da infraestrutura exigirá um esforço grande e um alinhamento profundo com o terceiro de forma a garantir a usabilidade adequada das soluções. Impactos na usabilidade oferecida a usuários são uma das principais causas de incidentes de segurança, uma vez que estes tendem a criar desvios buscando evitar controles de segurança para agilizar o seu trabalho. Muitas vezes esses desvios significam evitar procedimentos que estão atrapalhando seu trabalho, ou que sejam considerados improdutivos ou não alinhados ao seu *modus operandi*. Infelizmente grande parte dos procedimentos que dependem de infraestrutura terceirizada recai nessa categoria.

Considere-se o seguinte caso: um vendedor que utiliza um telefone IP para realizar vendas por todo o país. A organização onde ele trabalha não tem em suas políticas a necessidade de vinculação de chamadas realizadas para outros estados. A organização decide realizar a transferência da gestão de telefonia IP para um terceiro, que possui entre suas melhores práticas solicitar de todos os usuários o uso de códigos de chamadas interurbanas específicas. O vendedor, na tentativa de evitar o impacto na usabilidade do sistema de telefonia (e em alguns casos, agilidade) prefere deixar o código em um adesivo no telefone. Além disso, passa a utilizar o celular disponibilizado pela empresa, pois esse não possui esse tipo de controle.

No caso descrito acima, fica claro que uma falta de alinhamento entre a organização e o provedor de serviços de gerenciamento de telefonia IP causou falhas de segurança (compartilhamento de código) e aumento de custos (aumento do uso de celular), ambas com impacto para a organização.

Em uma organização atual, onde boa parte da infraestrutura tende a ser baseada em serviços de terceiros, essas situações tendem a ser cada vez mais recorrentes e precisam ser evitadas. Logicamente, em diversos casos o terceiro pode trazer técnicas e conhecimentos que aumentem o grau de segurança da informação da organização, mas esses precisam ser internalizados e assimilados antes de usados de forma generalizada pela organização.

Com relação à tecnologia, os riscos identificados são referentes à infraestrutura de propriedade do terceiro disponibilizada como serviço. Nesse tipo de situação, existe uma incerteza pelo lado do cliente quanto aos controles de segurança aplicados. Recomenda-se nesse tipo de situação que a organização se certifique de que o provedor de serviços contratado possui controles rígidos de segurança e

aplica melhores práticas de maneira consistente. Existem atualmente no mercado certificações específicas para demonstrar esse comprometimento, como a própria ISO/IEC 27001 e o SAS 70 – *Security Auditing Standards* 70 (DOOMUM, 2008). Os acordos de serviço assinados devem ser baseados em políticas de segurança próprias exigindo o comprometimento do provedor em ter conformidade com essas políticas.

Finalmente, foi identificado apenas um risco relacionado a pessoas, mas que é muito relevante. Da mesma forma que o cliente deve se certificar a respeito de controles tecnológicos do provedor de serviços, ele deve também garantir que os profissionais desse provedor estão devidamente treinados com relação à segurança. A partir do momento que esses profissionais passam a ter acesso às informações dos clientes, espera-se que eles a tratem com o mesmo grau de responsabilidade que esses.

Em algumas organizações existe a percepção que parte dos riscos identificados não é tão importante, uma vez que o provedor de serviços, devido ao uso de recursos especializados e a experiência com diversos clientes, tende a oferecer um grau cada vez maior de segurança física e lógica para os dados da organização. No entanto, a concentração cada vez maior de ativos valiosos na mesma localidade transforma esse provedor em um alvo de maior valor para ataques. Além disso, o provedor segue procedimentos estabelecidos ao longo do tempo, que podem não estar alinhados com as necessidades da organização e podem estar influenciados pelos mesmos procedimentos executados para outros clientes. Assim, determinadas operações com informações, como concessão de acesso, armazenamento e processamento de dados, podem ser realizadas de maneira automática, mas inadequada do ponto de vista de segurança para uma organização específica.

5.2. ANÁLISE – COMPUTAÇÃO EM NUVEM

A computação em nuvem é uma tecnologia recente, que foi introduzida no dia a dia organizacional em uma época em que o mercado está mais criterioso com relação à segurança. Dessa forma, esse tema sempre apareceu como uma

preocupação frequente nas discussões sobre essa tendência tecnológica, o que fez com que muitas pesquisas já tenham sido conduzidas com esse foco.

Isso não significa, no entanto, que os serviços atualmente disponíveis no mercado apresentam uma solução clara para o problema. É necessário considerar que, apesar da preocupação com a segurança da informação, muito da tecnologia utilizada como suporte à computação em nuvem também é recente, em especial a virtualização de dispositivos. A falta de conhecimento sobre essas tecnologias gera muitas dúvidas tanto do ponto de vista dos provedores de serviço como do ponto dos seus clientes.

Por causa do grande número de pesquisas, já existem publicações que funcionam como guia para identificação de riscos em computação em nuvem, compilando esses riscos e apresentando formas de mitigá-los. O próprio NIST – *National Institute for Standards and Technology*, na publicação "Usando o paradigma de computação em nuvem de forma segura e efetiva", traz uma compilação dos principais desafios para a computação em nuvem (NIST, 2011). O CPNI – *Center for Protection of National Infrastructure*, agência de proteção de infraestrutura governamental na Europa, apresenta uma lista de riscos identificados na computação em nuvem (CPNI, 2010). Indo por uma linha mais abrangente, a CSA – *Computer Security Alliance*, identifica uma série de domínios de interesse para a computação em nuvem (CSA, 2009).

A Tabela 2 a seguir apresenta alguns exemplos de riscos identificados referentes à computação em nuvem. A lista completa, sobre a qual se baseiam as considerações a seguir, está disponível no ANEXO B – RISCOS – COMPUTAÇÃO EM NUVEM.

ID	DESCRIÇÃO DO RISCO	REFERÊNCIA	CLASSIFICAÇÃO
RC.1	Risco de incompatibilidade das aplicações utilizadas na nuvem, dificultando a recuperação ou replicação de dados armazenados para outros locais	(CPNI, 2010)	Processos
	...		
RC.32	Risco de maior dificuldade de controle da segurança para os clientes que utilizam serviços de computação em nuvem	(NIST, 2011)	Pessoas

	...		
RC.36	Risco de falhas dos provedores de serviços não alcançarem RTOs e RPOs internos, além do risco de potenciais paradas definitivas de serviços	(CPNI, 2010)	Tecnologia

Tabela 2 - Exemplos de riscos identificados referentes à Computação em Nuvem (RTO = *Recovery Time Objective*; RPO – *Recovery Point Objective*)

Apesar de poder ser considerado um modelo de terceirização de infraestrutura, nota-se uma grande diferença entre os riscos identificados para aquela tendência tecnológica e computação em nuvem. Enquanto que lá a maior parte está relacionada a processos, aqui a maioria ainda está relacionada à tecnologia em si.

Serviços de computação em nuvem, seja ele PaaS, IaaS ou SaaS tendem a se apoiar fortemente em virtualização. A virtualização é uma forma de tornar simples a tarefa de gerenciamento de uma grande quantidade de recursos através da alocação de servidores lógicos em servidores físicos. Isso permite, por exemplo, a divisão de memória física entre várias máquinas virtuais, a movimentação de máquinas virtuais entre servidores e assim por diante. Essas técnicas facilitam o trabalho de gerenciamento de capacidade e disponibilidade para os provedores de computação em nuvem.

No entanto, apesar de trazer todas essas vantagens, essa é uma tecnologia recente, que está sendo massivamente adotada pelo mundo. Garantir a efetiva separação dos ambientes virtuais entre diversos clientes é um grande desafio. Permitir que essas máquinas virtuais apresentem todas as características de segurança dos sistemas físicos é ainda mais complexo.

Apesar da maioria dos riscos estar voltada à tecnologia, isso não significa que não existem muitos risco também voltados a processos. Da mesma forma que na terceirização de infraestrutura de TIC típica, existe a necessidade de compatibilização de processos organizacionais com os do provedor de serviços. Na medida em que a baixa interação humana está na essência da computação em nuvem cria-se uma resistência ainda maior a customizar e adaptar processos que atendem diversos clientes. Assim, como pode ser observado na Tabela 2, surgem diversos riscos do ponto de vista de processos.

Somam-se a esses riscos ainda aqueles que têm origem nas incertezas existentes ao lidar com nova tecnologia. Como exemplo, pode-se citar a dificuldade

de atender regulamentações e leis relacionadas à privacidade da informação e propriedades dos dados. Uma vez que as informações organizacionais podem estar armazenadas em qualquer ponto da nuvem, corre-se o risco de em determinado momento crítico a organização não estar conforme com uma dessas regulamentações. Infelizmente regulamentações tendem a caminhar em passos muito mais lentos que novas tecnologias, ficando defasadas rapidamente. No entanto, isso não é justificativa para a organização se deixar sua informação desprotegida.

É interessante notar que boa parte dos riscos mapeados ainda é focada na necessidade da organização de controlar a relação com o terceiro que oferece serviços de computação em nuvem, mas esquecem-se da necessidade de controlar a utilização dos serviços de computação em nuvem pelos seus usuários.

A computação em nuvem vem trazendo novos paradigmas para a o ambiente de trabalho. Talvez um dos mais claros seja a possibilidade de trabalho remoto através de aplicações no formato SaaS. No passado, aplicações disponibilizadas através da web costumavam apresentar um conjunto limitado de funções da versão local. A falta de funcionalidades causa desconforto nos usuários, que acabam vendo ai uma desvantagem para o trabalho remoto. Com as aplicações criadas na nuvem é diferente: a usabilidade das aplicações é sempre a mesma, pois elas foram concebidas desde o início para esse tipo de uso. Isso viabiliza o trabalho remoto.

Entretanto, o trabalho remoto pode ser executado de diversos tipos de ambientes, seguros ou não. Isso traz uma série de riscos referentes a computação em nuvem. Por exemplo, uma organização não pode garantir a segurança das informações que trafegam na rede doméstica de cada um que trabalha remotamente. Além disso, o acesso remoto não necessariamente é feito de dispositivos homologados ou testados pela organização e, portanto, sujeitos a todo tipo de ataque. Somado a tudo isso, existe a própria questão de conscientização do usuário sobre esses riscos. As facilidades do trabalho doméstico e a sensação de equivalência de funcionalidades pode criar uma falsa segurança. Assim, ele pode não tomar medidas de precaução, assumindo que o mesmo grau de segurança do ambiente da organização estará disponível no seu local de trabalho.

A organização precisa considerar todos esses riscos durante a migração de infraestrutura para a nuvem. Na relação entre organização e terceiro, as soluções típicas atualmente envolvem a definição de mecanismos contratuais, como acordos

de confidencialidade e acordos de nível de serviço. Na relação entre a organização e a pessoa tudo depende da capacidade da organização em criar uma cultura consciente dos riscos de segurança, que é um dos pontos onde existem maiores dificuldades atualmente (LACEY, 2010), (CHIA, MAYNARD e RUIGHAVER, 2002), (STANTON, STAM, *et al.*, 2005). O modelo de suporte proposto por essa pesquisa tem como objetivo deixar clara essas necessidades logo no inicio do processo de criação de uma abordagem de segurança estruturada para a organização.

5.3. ANÁLISE – MOBILIDADE

As questões de segurança em relação à mobilidade ficam cada vez mais relevantes devido à popularização de dispositivos como *smarthphones* e *tablets*. Atualmente, esses dispositivos sofreram grandes incrementos na sua capacidade de processamento e memória, além de apresentarem cada vez mais opções de conectividade. Assim, eles se aproximam cada vez mais dos computadores pessoais. Não é surpresa que as ameaças existentes para os *notebooks* e *laptops* de antes comecem a ser vistas proliferando em dispositivos móveis. De fato, observa-se o surgimento de uma série de códigos maliciosos destinados a ataques a esses dispositivos. Esses ataques têm os objetivos mais diversos, como o roubo de informações, controle remoto e monitoração. Assim, muitas organizações começaram a perceber o risco dos dispositivos móveis.

A Tabela 3 a seguir apresenta alguns exemplos de riscos identificados referentes à computação em nuvem. A lista completa, sobre a qual se baseiam as considerações a seguir, está disponível no ANEXO C – RISCOS – MOBILIDADE.

ID	DESCRIÇÃO DO RISCO	REFERÊNCIA	CLASSIFICAÇÃO
RM.1	Risco de não conhecimento e não cumprimento das políticas de segurança para dispositivos móveis	(GOODE, 2010)	Processos
	...		
RM.4	Risco de acesso a *sites* perigosos sem restrições, devido a maior confiança depositada nos dispositivos móveis	(LEAVITT, 2011)	Pessoas

	...		
RM.5	Risco de controle de dispositivos móveis para a formação de botnets	(LEAVITT, 2011)	Tecnologia

Tabela 3 - Exemplos de riscos identificados referentes à Mobilidade

Da mesma forma que acontece com a computação em nuvem, boa parte dos riscos identificados diz respeito à tecnologia. No entanto, os riscos não se devem ao desconhecimento a respeito da tecnologia. Eles estão relacionados ao fato de já existirem tantas ameaças conhecidas que podem facilmente ser transportadas para dispositivos móveis.

Somado às ameaças já conhecidas, existem algumas particularidades tecnológicas preocupantes na mobilidade que devem ser consideradas. Por exemplo, os dispositivos móveis propriamente ditos ou os cartões de memória utilizados são frequentemente perdidos ou roubados. Outro exemplo está relacionado à liberdade de acesso proporcionada pela mobilidade. Atualmente as aplicações mais diversas estão sendo criadas para dispositivos móveis, tornando-os clientes de qualquer tipo de serviço, inclusive na nuvem. Assim os dispositivos móveis podem se tornar portas de entrada para a infraestrutura da organização que estão terceirizando sua infraestrutura através de provedores de serviço.

Além disso, é necessário pensar também nos riscos relacionados a processos e pessoas – esses dispositivos se tornaram parte do dia a dia das organizações da mesma forma que desktops e notebooks. Portanto, essas organizações precisam começar a considerá-los como ferramentas de trabalho, sobre as quais deve existir uma gestão do ponto de vista de segurança. Precauções como a gestão de contratos com fornecedores de conectividade, controle do ciclo de vida de ativos e conscientização dos usuários a respeito das informações armazenadas precisam se tornar mais comuns do que acontece atualmente.

5.4. ANÁLISE CONSOLIDADA

Nas seções anteriores foram apresentados os riscos identificados para cada uma das tendências tecnológicas que caracterizam o cenário externo atual. A Tabela

4 apresenta a contabilização dos riscos identificados, incluindo a separação quanto a relação à tecnologia, processos e pessoas.

	TECNOLOGIA	PROCESSOS	PESSOAS	TOTAL
Terceirização da infraestrutura de TIC	2	19	1	**22**
Computação em nuvem	29	31	4	**64**
Mobilidade	13	3	1	**17**
TOTAL	**44**	**53**	**6**	**103**

Tabela 4 - Resultados da compilação dos riscos identificados para cada tendência tecnológica

A tabela dá indícios do quão abrangente é a visão de segurança para cada tendência considerada. É interessante notar a baixa quantidade de riscos que podem ser relacionados diretamente a pessoas, independente da tendência considerada. Apesar de colaboradores e funcionários atuarem de forma determinante na segurança da informação, parece existir um grande receio a explicitar riscos que dependem delas. Entretanto, como apresentado anteriormente, frente a um cenário onde todas essas tendências estão consideradas, a segurança cada vez mais vai depender da atuação das pessoas. Isso devido a necessidade de adaptação rápida, identificação e adaptação a novas ameaças no momento em que elas surgem.

Isso não significa que a tecnologia e processos irão perder a importância do ponto de vista de segurança. A aplicação de controles em tecnologia e processos são as principais defesas que a organização tem para proteger sua informação. No entanto, frente ao novo cenário, esse tipo de controle precisa ser considerado de forma natural, uma vez que se torna essencial para a organização. Isto é, a segurança em infraestrutura tecnológica e processos não poderá mais ser algo incorporado posteriormente a sua implantação.

As seções 5.1, 5.2 e 5.3 fizeram uma análise segmentada dos riscos identificados para terceirização de infraestrutura de TIC, computação em nuvem e mobilidade, respectivamente. Conforme apresentado na introdução desse trabalho, a abordagem típica em Gestão de Segurança para mitigar novos riscos é a

identificação de um controle de segurança e sua implementação, através de uma análise de riscos. De fato, os trabalhos utilizados como referência tendem a sugerir formas de mitigar o risco específico que foi identificado (CPNI, 2010), (KHIDZIR, MOHAMED e ARSHAD, 2010), (NIST, 2011), (GOODE, 2010).

A análise das tendências tecnológicas em separado, por essa abordagem, tende a levar a controles específicos, criadas especificamente para mitigar cada risco identificado. Esses controles, apesar de buscarem a manutenção das propriedades de confidencialidade, integridade e disponibilidade da informação, acabam tendo como alvo a tecnologia em si. Seguindo a mesma abordagem o resultado é uma série de controles aplicados para mitigar riscos diversos, que podem ser similares entre si.

Nesse momento, se a organização possui um ciclo de gestão de segurança maduro, é provável que uma causa raiz comum seja identificada para os riscos identificados. Aí cabe a organização assimilar essa situação e modificar a sua abordagem de acordo. Por exemplo, na ISO/IEC 27001, a fase de Atuação do ciclo PDCA visa uma análise crítica dos resultados do último ciclo que busca esse tipo de revisão. Infelizmente, realizar esse tipo de análise exige um grau de compreensão sistêmica e conhecimentos específicos que muitas organizações não tem a sua disposição.

Além disso, o cenário externo atual dificulta um pouco essa abordagem. Isso porque a quantidade de novas tecnologias e riscos associados que as organizações precisam assimilar é muito grande. Combinada com a dinamicidade e as incertezas quanto às novas tendências tecnológicas, a análise crítica do cenário se torna muito difícil.

Essa situação pede uma atuação diferente, que permita as organizações terem a visão global da segurança no cenário externo. Vê-se necessária uma nova abordagem que analise esse cenário como um todo e não cada tendência tecnológica e riscos associados em separado. Dessa forma as organizações poderiam aprender mais rapidamente a identificar as preocupações mais comuns e atuar sobre elas diretamente, antes que elas se tornem riscos maiores para a informação.

Analisando as compilações de riscos apresentadas, agora sob uma ótica unificada como discutido acima, é possível identificar uma série de temas em comum. Por exemplo, nota-se uma grande preocupação em garantir a conformidade

com políticas e regulamentações ao transferir a infraestrutura para terceiros, sejam eles provedores de serviços típicos ou de nuvem. Também existem diversos riscos relacionados à falta de conhecimento sobre novas tecnologias, como a virtualização e dispositivos móveis.

TEMA	DESCRIÇÃO	RISCOS MAPEADOS
[T.1]	Baixa confiança na capacidade de execução dos serviços acordados	**8**
[T.2]	Baixa confiança na capacidade de atendimento a requisitos específicos	**3**
[T.3]	Pouco conhecimento de vulnerabilidades de novas tecnologias	**19**
[T.4]	Incerteza sobre integração de processos com base em serviços	**18**
[T.5]	Dificuldade para escolha do melhor serviço para a empresa	**6**
[T.6]	Potenciais não conformidades com melhores práticas, políticas e regulamentações	**21**
[T.7]	Dificuldade de integração da infraestrutura da empresa com nova tecnologia	**5**
[T.8]	Incapacidade de controle adequado de dados armazenados fora da empresa	**16**
[T.9]	Não utilização de soluções adequadas de segurança para infraestrutura terceira	**7**

Tabela 5 - Temas de segurança identificados com base nos riscos mapeados pelo trabalho

A Tabela 5 apresenta uma lista desses temas, juntamente com a quantidade de riscos associados a cada um deles. As listas completas de riscos desse trabalho disponíveis nos anexos apresentam o tema associado a cada um deles, identificados de acordo com as linhas dessa tabela.

Listar esses temas mais abrangentes ajuda a identificar quais são as preocupações típicas que as organizações têm ao lidar com o cenário externo e a as preparar melhor para eles. Nessa pesquisa esses temas formam a base para a definição de que modificações devem ser introduzidas no modelo de suporte proposto para a fase de Planejamento da ISO/IEC 27001.

5.5. CONSIDERAÇÕES FINAIS

A análise de referências na literatura e no mercado indica uma série de riscos já mapeados para as tendências tecnológicas que caracterizam o cenário externo.

Com relação a terceirização de infraestrutura de TIC, a maior parte desses riscos está relacionada a integração de processos entre a organização e o provedor de serviços. Já na computação em nuvem, devido ao uso de tecnologias desconhecidas, uma quantidade maior de riscos relacionados a essas soluções pode ser encontrada. Com relação à mobilidade, existe também maior ênfase em riscos de tecnologia, mas devido a quantidade de ameaças que podem ser transferidas do mundo dos computadores pessoais para o mundo móvel.

Nota-se uma baixa quantidade de riscos que podem ser atribuídos a pessoas, independente da tendência tecnológica analisada. Isso se deve provavelmente às origens de segurança que estão profundamente ligadas a aspectos tecnológicos e ao receio de vincular a segurança de um sistema a pessoas.

Analisando todos os riscos em conjunto podem ser identificados alguns temas em comum, apresentados na Tabela 5. Esses temas refletem as preocupações típicas que aparecem na integração das tendências tecnologias ao dia a dia das organizações. Eles serão utilizados como base para a construção do modelo de suporte proposto.

6. ESPECIFICAÇÃO DE REQUISITOS DO MODELO DE SUPORTE

Considerando os objetivos estabelecidos para o trabalho e o exposto com relação à Gestão de Segurança da Informação e o cenário externo considerado, definem-se a seguir os requisitos do modelo de suporte desenvolvido. Esses requisitos são divididos entre requisitos primários e secundários.

Os requisitos primários são os considerados essenciais para permitir uma real utilização por praticantes de segurança. Os requisitos secundários refletem aspectos mais conceituais, mas que também devem estar presentes no modelo.

6.1. REQUISITOS PRIMÁRIOS

Foram identificados os seguintes requisitos primários:

- **Apresentar conformidade com processos de gestão de segurança existentes na ISO/IEC 27001** – O modelo de suporte não deve buscar a substituição de processos já estabelecidos dentro da norma, visto que existe um consenso que esses constituem as melhores práticas para Gestão de Segurança;

- **Permitir a integração com os fluxos típicos de atividades existentes na fase de Planejamento da ISO/IEC 27001** – O modelo deve ser baseado nos passos típicos seguidos por praticantes de segurança para as atividades da fase de Planejamento. A partir desses passos, o modelo deve apresentar quais adequações e recomendações são necessárias em cada atividade.

- **Permitir à organização visualizar potenciais lacunas nos resultados de seus esforços em segurança frente ao novo cenário** – O modelo deve indicar para a organização quais são os pontos de

atenção a considerar para adequar a abordagem interna de segurança e prepará-la para o cenário externo.

- **Apresentar referências a práticas de segurança que possam ser utilizadas para preencher as lacunas identificadas** – O modelo deve apresentar sugestões de como executar as alterações propostas, criando assim um ponto de partida para a organização. Cada organização pode buscar customizar essas práticas de acordo com o seu contexto interno.

6.2. REQUISITOS SECUNDÁRIOS

Como requisitos secundários, tem-se:

- **Apresentar abordagem específica para definição de políticas de segurança –** Uma vez que a fase de Planejamento da ISO/IEC 27001 tem como uma de suas atividades principais a definição de políticas de segurança, o modelo de suporte deve apresentar uma abordagem específica para essa atividade;

- **Apresentar abordagem específica para a gestão de riscos** – Uma vez que a fase de Planejamento da ISO/IEC 27001 tem como uma de suas atividades principais execução dos processos de Gestão de Riscos, o modelo de suporte deve apresentar uma abordagem específica para essa atividade;

- **Considerar as principais tendências tecnológicas do cenário externo** – O modelo de suporte deve apresentar conclusões sobre a terceirização de infraestrutura de TIC, computação em nuvem e mobilidade;

- **Considerar riscos específicos de cada tendência tecnológica do cenário externo** – O modelo de suporte deve ser baseado em riscos já identificados pelo mercado para cada uma das tendências tecnológicas;

- **Considerar riscos existentes do uso combinado das tecnologias disponíveis no cenário externo** – A combinação de tendências tecnológicas do cenário externo gera situações novas, que normalmente não são consideradas ao analisar cada tendência individualmente. O modelo de suporte deve conseguir indicar a necessidade de consideração de riscos gerados a partir desse tipo de combinação.

- **Apresentar simples utilização por praticantes de segurança** – O modelo não pode adicionar uma complexidade demasiada para sua utilização durante a revisão de processos do SGSI;

- **Promover a mudança de foco de segurança de aspectos tecnológicos para aspectos de pessoas e processos –** O modelo deve contemplar o papel e a importância das pessoas e dos processos na proteção da informação;

- **Promover a aproximação dos conceitos de "Informação" e "Segurança da Informação"** – O modelo deve permitir a organização buscar a proteção da mesma informação em suas diversas formas, independente da mídia onde ela está armazenada;

- **Considerar as resistências de pessoas com relação a controles de segurança** – O modelo deve levar em consideração a necessidade de tornar atrativos para as pessoas novos controles de segurança.

- **Considerar a crescente fusão de ambientes profissionais e pessoais** – O modelo de suporte deve considerar a realidade de que a infraestrutura da organização e a infraestrutura pessoal são agora cada

vez mais utilizadas para as mesmas atividades, sejam elas relacionadas ao trabalho ou não.

6.3. CONSIDERAÇÕES FINAIS

Nesse capítulo foram apresentados os principais requisitos identificados para a construção do modelo de suporte proposto. Os requisitos foram divididos em primários e secundários.

Os requisitos primários são considerados importantes para que praticantes de segurança consigam considerá-lo dentro de suas abordagens para a fase de Planejamento do SGSI. Os requisitos secundários visam garantir que o modelo de suporte irá apresentar um embasamento conceitual necessário referente ao cenário externo.

7. MODELO DE SUPORTE PROPOSTO

Conforme apresentado na seção 3.4 desse trabalho, a fase de Planejamento da ISO/IEC 27001 é focada em duas atividades principais:

- Definição da Política de Segurança da Informação; e
- Gestão de Riscos de Segurança.

Com o objetivo de manter a compatibilidade com processos de gestão de segurança já existentes, o modelo de suporte é dividido em duas partes, cada uma correspondendo a uma dessas atividades.

A construção de cada uma das partes do modelo de suporte passou por três etapas distintas:

1. Etapa 1 – Descrição de processo básico de referência – Identificação na literatura de referência(s) ao processo típico utilizado para a atividade em questão.
2. Etapa 2 – Definição de pontos de verificação – Consolidação dos resultados de pesquisa referentes a formas de endereçar as preocupações identificadas na seção 5.4 (Temas de Segurança), resultando em pontos de checagem para cada etapa do processo básico.
3. Etapa 3 – Construção do modelo de suporte – Inserção dos pontos de verificação definidos dentro do processo básico descrito na Etapa 1.

A seguir são apresentados os resultados de cada uma dessas etapas para as duas atividades da fase de Planejamento da ISO/IEC 27001.

7.1. SUPORTE A DEFINIÇÃO DE POLÍTICAS DE SEGURANÇA

A política de um SGSI baseado na ISO/IEC 27001 deve conter um direcionamento geral para a organização com relação à segurança da informação. Ela estabelece os objetivos gerais que devem ser perseguidos por todos no que diz

respeito à proteção da informação (DOHERTY e FULFORD, 2006). Por causa disso é um consenso que a política de segurança é o principal documento para a divulgação de práticas adequadas de segurança da informação.

Entre os requisitos primários do trabalho está a identificação de lacunas existentes nas práticas atuais de segurança frente ao cenário externo. Essa identificação só é viável através de uma mudança da cultura organizacional referente à segurança da informação e a sua elevação de uma prática pontual para uma prática natural do dia a dia.

Por um lado entende-se que a política é a principal forma de disseminação da cultura de segurança na organização (VON SOLMS e VON SOLMS, 2004), e por outro se nota a necessidade de transformar a cultura organizacional de segurança frente ao cenário externo. Um modelo de suporte à definição de políticas deve ser capaz de auxiliar o desenvolvimento de políticas visando a adaptação da cultura organizacional para esse cenário externo descrito anteriormente.

7.1.1. DESCRIÇÃO DE PROCESSO DE REFERÊNCIA

A ISO/IEC 27001 não apresenta de maneira clara qual é a sua recomendação para o processo de definição de políticas de segurança. Dessa forma, essa pesquisa procurou estabelecer um processo a partir de informações encontradas na literatura, mesmo que de maneira desestruturada. Esse processo é utilizado nas demais etapas da construção do modelo de suporte.

Como será observado a seguir, a ISO ainda oferece um direcionamento para o conteúdo que a política de segurança deve oferecer. Felizmente, esses direcionamentos podem ser combinados com outras fontes na literatura para a definição de uma estrutura que dá origem ao processo utilizado como referência.

Fonte 1 – ISO/IEC – *Information Technology – Guidelines for the management of IT Security – Part 3* (ISO/IEC TR 13335-3, 1998)

A ISO deixou de incorporar aspectos desejados para políticas na última versão da sua norma relacionada à gestão de riscos (ISO/IEC 27005, 2011). No entanto, a

versão anterior, ISO/IEC 13335-3, apresentava de forma mais detalhada o conteúdo esperado para uma política de segurança da informação. Este inclui:

- Escopo e propósito;
- Objetivos de segurança com respeito a obrigações regulatórias e legais, e objetivos de negócio;
- Requisitos de segurança de TI, em termos de confidencialidade, integridade, disponibilidade, rastreabilidade, autenticidade e confiabilidade da informação;
- Administração da segurança da informação, cobrindo responsabilidades individuais e da organização;
- Abordagem de gestão de riscos que é adotada pela organização;
- Formas para determinar as prioridades de implantação de controles são determinadas;
- Nível geral de segurança e risco residual buscado pela organização;
- Qualquer regra geral para controle de acesso (controle de acesso lógico como controle de acesso físico para prédios, salas, sistemas e informação).
- Abordagem para conscientização e treinamento de segurança da organização;
- Procedimentos gerais para checar e manter a segurança;
- Informações gerais relacionadas à segurança de pessoal;
- Formas de comunicação da política para todos os envolvidos;
- Circunstâncias nas quais a política deverá ser revisada;
- Método de controle de alterações na política.

Além disso, deixa-se claro que a política deve receber apoio e aprovação da direção executiva.

Fonte 2 – ISO/IEC 27001/27002 – *Information Technology – Security Techniques – Information Security Management Systems* (ISO/IEC 27001, 2005)

A ISO oferece na norma principal da sua série 27000 mais indicações sobre o conteúdo necessário para a política de segurança do SGSI:

- Inclusão de um modelo que defina os objetivos e estabeleça um senso geral de direção e princípios para ações relacionadas à Segurança da Informação.
- Consideração sobre os requisitos legais e regulatórios, e obrigações contratuais de segurança.
- Alinhamento com o contexto da gestão de risco da organização na qual será estabelecido e mantido o SGSI.
- Estabelecimento de critérios usados para avaliar os riscos.
- Aprovação da política pela gestão.

A política de segurança do SGSI é um documento que deve englobar o conteúdo da política de segurança da informação. No entanto, isso não significa que esses precisam ser dois documentos separados. A ISO/IEC 27002 oferece mais detalhes a respeito do conteúdo que deve conter a política de segurança da informação:

- Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação.
- Uma declaração do comprometimento da direção, apoiando as metas e os princípios da segurança da informação, alinhada com os objetivos e as estratégias do negócio.
- Um método para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise e avaliação de risco.
- Breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
    - Conformidade com a legislação e com requisitos regulamentares e contratuais;

  - Requisitos de conscientização, treinamento e educação em segurança da informação;
  - Gestão de continuidade de negócio;
  - Consequências das violações na política de segurança da informação.
- Definição das responsabilidades gerais e específicas na gestão de segurança da informação, incluindo o registro dos incidentes de segurança da informação.
- Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

Fonte 3 – *Building an Effective Information Security Policy Architecture* (BACIK, 2008)

Esse livro apresenta um processo básico para criação de uma arquitetura completa de políticas de segurança da informação, da onde podem ser extraídos alguns elementos básicos de uma política de segurança. Por arquitetura de políticas entenda-se a série de diretrizes, separadas em documentos diversos, cada um com um nível de abstração sobre elementos de informação.

- Revisar itens com riscos altos, médios e baixos.
- Listar itens que devem ser documentados.
- Adquirir suporte da organização para a política.
- Criar uma equipe para definição da política e local de armazenamento da mesma.
- Desenvolver arquitetura de políticas, tópicos, prioridades, responsabilidades por funções de segurança e glossário.
- Desenvolver e implantar a arquitetura da política.
- Conscientização a respeito da política de segurança.

Ainda no mesmo livro, são apresentados os tópicos típicos a serem incluídos em uma política de segurança corporativa, considerando o nível mais alto da arquitetura proposta:

- Práticas para operação segura;
- Guias de conduta para usuários no que diz respeito a uso de recursos;
- Procedimento para resolver conflito de interesses;
- Conformidade (em geral) com legislações e outros documentos;
- Comunicação corporativa (interna/externa);
- Autoridade e responsabilidade corporativa;
- Privacidade;
- Risco;
- Segurança da informação;
- Propriedade e classificação de ativos;
- Segurança física;
- Continuidade de negócios e recuperação de desastres;

Com base nas fontes apresentadas, nota-se que alguns tópicos são frequentemente citados como importantes para o desenvolvimento de uma política de segurança da informação adequada. São eles:

- Escopos e objetivos;
- Requisitos gerais sobre a informação;
- Método de gestão de risco;
- Conscientização e treinamento a respeito de segurança da informação;
- Responsabilidades sobre a gestão da segurança;
- Comprometimento da direção com as diretrizes da política;
- Comunicação da política;

Combinando esses elementos, é possível estabelecer um processo de referência para a definição de políticas de segurança da informação, apresentado na Figura 3. É importante observar que o objetivo aqui é apenas criar uma fundação sobre a qual o modelo de suporte pode ser construído. Ele não deve ser tomado como uma referência completa para o desenvolvimento de políticas de segurança da

informação. Cada organização deve buscar desenvolver uma abordagem própria, adequada para suas necessidades e alinhada com a sua estratégia.

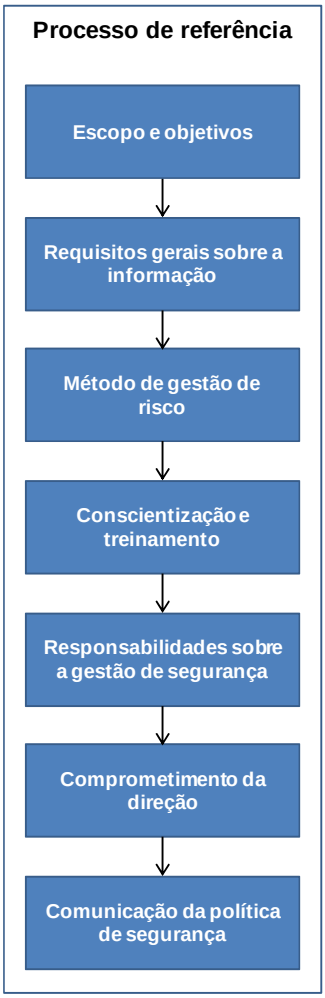

Figura 3 - Processo de referência para definição de políticas de segurança

7.1.2. DEFINIÇÃO DE PONTOS DE CHECAGEM

Os temas apresentados na seção 5.5 representam preocupações que organizações provavelmente irão ter ao lidar com a introdução das tecnologias presentes no novo cenário. Essas preocupações provavelmente irão aparecer após diversos ciclos do seu sistema de gestão, através de análises críticas.

A ideia por trás da definição de pontos de checagem é explicitar essas preocupações mais cedo no ciclo, permitindo o melhor planejamento do SGSI para os riscos do novo cenário. A Tabela 6 indica como ocorre a relação entre os pontos de checagem definidos e os temas de segurança.

Todos os pontos de checagem aqui definidos foram extraídos das pesquisas realizadas para o trabalho (indicados pelas respectivas fontes) ou são conclusões derivadas dessas pesquisas.

	Tema / **Ponto de checagem**	**[T.1]**	**[T.2]**	**[T.3]**	**[T.4]**	**[T.5]**	**[T.6]**	**[T.7]**	**[T.8]**	**[T.9]**
	Escopo e objetivos									
PC.1	Avaliar se o foco do escopo é efetivamente a informação			**X**					**X**	**X**
PC.2	Avaliar se existe inserção da segurança nas atividades diárias	**X**	**X**		**X**	**X**	**X**			
PC.3	Avaliar os incentivos à obediência aos controles	**X**	**X**				**X**			**X**
	Requisitos gerais sobre a informação									
PC.4	Avaliar a abstração das mídias usadas para guardar a informação			**X**				**X**	**X**	**X**
	Método de gestão de risco									
PC.5	(Modelo de suporte específico para gestão de riscos)	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
	Conscientização e treinamento sobre segurança									
PC.6	Avaliar se a conscientização de segurança é vista como resultado			**X**	**X**	**X**	**X**	**X**	**X**	**X**
PC.7	Avaliar a customização do programa de conscientização				**X**		**X**	**X**		
	Responsabilidades sobre a gestão da segurança									
PC.8	Avaliar a distribuição da responsabilidade sobre a segurança	**X**	**X**				**X**		**X**	**X**
	Comprometimento da direção e Comunicação da política de segurança									
PC.9	Avaliar se existe a comunicação por exemplos						**X**			**X**
PC.10	Avaliar a hierarquia de políticas de segurança			**X**	**X**			**X**	**X**	**X**

Tabela 6 - Relação entre pontos de checagem estabelecidos para suporte à definição de políticas de segurança e temas de segurança identificados

A seguir é apresentado um detalhamento dos pontos de checagem, já seguindo a mesma ordem do processo de referência apresentado. Logo após a apresentação de cada ponto de checagem, é detalhado o racional que levou a vinculação dos mesmos aos temas na Tabela 6.

7.1.2.1. Escopo e objetivos

PC.1	**Avaliar se o foco do escopo é efetivamente a informação**
	As organizações não podem mais definir um escopo limitado para a segurança da informação, que a isente de lidar com incidentes não previstos. A segurança é um alvo móvel, com velocidade cada vez mais alta. Assim as organizações devem estabelecer metas de manter a segurança em todos os níveis do seu SGSI, iniciando-se pela política de segurança. Assim, o escopo do SGSI, na política de segurança da informação, deve ser estabelecido com base na informação em si, e não em termos de áreas, processos ou equipes específicas. Devem ser previstos na política os novos tipos de informações que podem ser encontradas. Exemplificando, um escopo definido como incluindo uma equipe de planejamento estratégico não especifica que tipo de informação utilizada por essa equipe que deve ser protegida. Além disso, não deixa claro que um documento gerado por essa equipe e enviado para outro time deve também ser protegido por essa outra equipe. Ao especificar a informação em si no escopo (“Documentos de Planejamento Estratégico” no exemplo anterior), dá-se flexibilidade para a política de segurança, que busca proteger a informação onde quer que ela esteja. Isso inclui a infraestrutura externas, de terceiros, como acontece ao utilizar a terceirização de TIC, computação em nuvem e mobilidade.

O PC.1 visa garantir que a organização especifique um escopo para o SGSI focado na informação em si e não em processos, pessoas ou infraestrutura que lidem com essa informação. Com isso a organização

reduz a dificuldade de especificar todos os ambientes onde seus dados podem estar armazenados, preocupação expressas no T.8. Além disso, esse ponto de checagem diminui a necessidade de especificar todas as soluções tecnológicas e de segurança desses ambientes, as quais podem ser desconhecidas no novo cenário tecnológica. Essa necessidade é expressa nos temas T.3 e T.9.

PC.2	**Avaliar se existe inserção da segurança nas atividades diárias**

(LACEY, 2010)

A segurança deve estar realmente inserida na cultura organizacional. Esse deve ser um dos objetivos traçados na política de segurança. Para tal, a política deve demonstrar o interesse da organização em preparar seus colaboradores, parceiros e fornecedores para tratar de segurança de maneira natural em todo tipo de atividade.

A segurança não pode ser vista como algo “a mais” e sim como uma obrigação de todos os colaboradores para o bem da organização. Dessa forma, eles passarão a executar suas atividades considerando a segurança.

O PC.2 visa assegurar que a segurança seja discutida em todos os níveis e processos da organização, sejam eles executados por colaboradores, terceiros ou parceiros. Assim, esse ponto busca reduzir as preocupações expressas pelo T.1, T.2, T.4, T.5 e T.6, que são aquelas voltadas à coordenação e integração de processos entre terceiros e organização.

PC.3	**Avaliar os incentivos à obediência aos controles**

(CHIA, MAYNARD e RUIGHAVER, 2002)

A organização precisa deixar claro para colaborares e terceiros que os controles de segurança existem para eliminar riscos bem específicos e reais e que, portanto, devem ser obedecidos. Assim, é crítico que entre os

objetivos da política de segurança esteja à necessidade de reforçar a obediência a controles de segurança.

No entanto, o grande desafio é fazer com que a obediência aos controles seja consciente, tirando o tema da segurança da informação da obscuridade. No passado não podia se esperar que pessoas conhecessem segurança e entendessem as razões de cada controle. O novo cenário externo está mudando paradigmas, incluindo esse. Na medida em que mais pessoas estão utilizando as novas tecnologias para fins próprios, conceitos de segurança começam a ser aplicáveis às suas informações.

As organizações precisam começar a utilizar esse conhecimento adquirido espontaneamente pelos seus colaborares para construir uma maior conscientização sobre a importância dos controles de segurança.

Com o PC.3 busca-se evitar que as práticas de segurança deixem de ser encaradas com seriedade, seja por colaboradores ou por terceiros. Essa preocupação é refletida nos temas T.1, T.2 e T.9. Como em muitos casos o desrespeito aos controles leva às não conformidades, esse ponto também está relacionado ao T.6.

7.1.2.2. Requisitos gerais sobre a informação

PC.4	**Avaliar a abstração das mídias usadas para guardar a informação**

(KHANMOHAMMADI, 2010)

É necessário deixar claro na política de segurança o que a organização considera como informação a ser protegida. No entanto, essa definição exige o entendimento do conceito que a informação pode assumir diversas formas, de acordo com a mídia utilizada para seu armazenamento.

A informação é normalmente associada a objetos e documentos, como CDs, apresentações, documentos impressos e afins. Dentro de uma infraestrutura móvel e baseada em serviços de terceiros, esses tipos de mídia deixam de ser visíveis. Nesse ambiente, não é possível prever onde informação será armazenada. Ela pode estar bem mais dispersa do que em

um ambiente controlado pela organização. Além disso, essa informação está mais relacionável e disponível para o acesso por um público bem maior.

A política precisa indicar que a informação da organização não está mais presa aos limites físicos dos escritórios e que, mesmo assim, precisa ser protegida.

O PC.4 procura eliminar a associação típica da informação com mídias específicas, buscando focar a organização na informação em si, da mesma forma que o PC.1. Sendo assim, ele está vinculado aos temas T.3, T.8 e T.9. No entanto, vai além, pois deixa evidente a necessidade de abstrair as tecnologias usadas para o armazenamento de dados e as incertezas relacionadas à sua adoção. Essas incertezas são expressas no T.7.

7.1.2.3. Método de gestão de risco

PC.5	(Modelo de suporte específico para gestão de riscos)
	A política de segurança da informação deve conter os parâmetros gerais relacionados à gestão de risco. Esses parâmetros podem ser derivados do modelo de suporte especificado nesse trabalho.

Visto que o modelo de suporte para gestão de riscos apresenta pontos de checagem que cobrem todos os temas de segurança, o PC.5 do modelo de suporte para definição de políticas de segurança é vinculado a todos os temas de segurança.

7.1.2.4. Conscientização e treinamento sobre segurança

PC.6	Avaliar se a conscientização de segurança é vista como resultado

(LACEY, 2010), (CORRISS, 2010)

A política de segurança da informação deve estabelecer um programa de conscientização sobre segurança que seja aplicável no dia a dia organizacional. A conscientização deve ser encarada como um objetivo desse programa e não pode ser confundida com as ações tomadas dentro do programa, tais como treinamentos, campanhas, etc. Os meios para alcançar a conscientização podem ser adaptados de acordo com o perfil da organização, indo desde lembretes diários a todos os colaboradores até apresentação de casos reais como exemplos.

Treinamentos de segurança da informação são interessantes para explicar conceitos básicos de segurança, mas não devem ser encarados como única forma de alcançar a conscientização. Entre outras formas, podem ser citadas campanhas em sites internos, distribuição de panfletos explicativos, palestras com profissionais da área de gestão de segurança, simulações de casos reais, estudos de caso, etc.

O PC.6 busca garantir que exista uma campanha de segurança continuamente ativa no dia a dia da organização. Essas campanhas visam deixar os colaboradores preparados para lidar com o maior número de situações possíveis, independente do conhecimento (T.3, T.4, T.7) e controle (T.5, T.8 e T.9) da empresa sobre as inovações tecnológicas e serviços utilizados. Esse ponto contribui também diretamente para a conformidade com políticas de segurança internas, sendo assim vinculado também ao T.6.

PC.7	Avaliar a customização do programa de conscientização

(CORRISS, 2010)

O desenvolvimento da cultura de segurança na organização depende de exemplos práticos. Para tal, o programa de conscientização deve ser adaptado de forma a se encaixar em situações reais de risco para a organização. A política de segurança deve estabelecer as bases para que esse tipo de conscientização seja desenvolvido na organização.

Por exemplo, é possível desenvolver programas de conscientização focados em equipes específicas, baseados nas informações típicas utilizadas por cada uma delas. Também pode-ser considerar a criação de programas extraordinários para situações de mudanças tecnológicas ou introdução de novos processos.

O PC.7 especifica uma característica importante que deve ser seguida no programa de conscientização, que é a customização das ações para melhor adaptação a processos e equipes específicas na organização. Uma correta inserção de aspectos de segurança em processos específicos da organização pode facilitar a integração desses processos com novos serviços e tecnologias. Por isso, esse ponto de checagem é vinculado aos temas T.4 e T.7. Visto que esse tipo de treinamento também visa a garantir a conformidade, o ponto de checagem é também vinculado ao T.6.

7.1.2.5. Responsabilidades sobre a gestão de segurança

PC.8	Avaliar a distribuição da responsabilidade sobre a segurança

Dentro do novo cenário externo, a organização não tem total controle sobre as informações enviadas para infraestrutura de terceiros no formato de arquivos, bancos de dados, etc. Manter controle e rastreabilidade sobre toda essa informação se torna muito complicado.

Uma forma de mitigar esse tipo de situação é colocar, dentro da política de segurança, uma responsabilidade cada vez maior dos

colaboradores e terceiros sobre a garantia de segurança dessas informações.

Com o PC.8 o modelo de suporte procura deixar claro para todas as entidades envolvidas com a segurança, sejam elas colaboradores ou terceiros quais são as suas responsabilidades. Assim, busca-se diminuir incertezas expressas pelos temas T.1 e T.2, T.8 e T.9, relacionadas a capacidades de terceiros para execução de serviços. Além disso, procura reduzir a chance de não conformidades causadas por colaboradores, expressa pelo T.6.

7.1.2.6. Comprometimento da direção e comunicação

PC.9	**Avaliar se existe a comunicação por exemplos**

(KNAPP, MARSHALL, *et al.*, 2006), (CORRISS, 2010)

Apesar de o formato textual ser normalmente necessário para divulgação da política (e para fins de auditorias), ele tende a ser ignorado na maior parte das organizações.

Dada à relevância da comunicação da política de segurança frente ao cenário externo descrito, o fato do documento escrito ser ignorado não deve ser uma justificava para desconhecimento sobre as diretrizes de segurança. Recomenda-se que seja feito um trabalho específico de conscientização com os níveis superiores da hierarquia.

Dessa forma, ambos os problemas de demonstração do comprometimento da direção e de comunicação da política de segurança são resolvidos de uma maneira única e compatível com as necessidades da organização.

O ato de comunicar por exemplos, verificado através do PC.9, busca reforçar a necessidade de obediência aos controles para os colaboradores. Dessa forma, os temas relacionados são o T.6 e T.9 (mesmos do PC.3).

PC.10	**Avaliar a hierarquia de políticas de segurança**

(BACIK, 2008)

Convém que a política de segurança da informação seja apresentada em diferentes níveis de abstração. Cada nível da hierarquia deve detalhar de maneira mais específica algum ponto da política.

Níveis diferentes de detalhamento devem ser utilizados de acordo com o contexto, permitindo assim que as pessoas aprendam a reagir de maneira adequada em um grande número de situações diferentes.

A criação de uma hierarquia de políticas, verificada através do PC.10, permite a organização flexibilizar a forma com que promove os controles de segurança existentes. Isso acontece devido a possibilidade de criar políticas bem generalistas e outras bem específicas, por exemplo, voltadas a tendências tecnológicas e suas integrações com processos específicos. Dessa forma, esse ponto de checagem se vincula aos temas T.3, T.4, T.7, T.8 e T.9.

7.1.3. CONSTRUÇÃO DO MODELO DE SUPORTE

O modelo de suporte proposto para a definição de políticas de segurança complementa processo de referência apresentado para essa atividade. Além disso, oferece um guia para a organização no desenvolvimento de uma cultura de segurança adequada ao cenário externo descrito.

No total são inseridos 10 pontos de checagem dentro dos 7 passos típicos para essa atividade, observados na Figura 4. Mesmo que os passos seguidos pela organização não seja exatamente o descrito no processo de referência, é possível utilizar os pontos de checagem. Basta que a organização deseje considerar na sua política de segurança o conteúdo apresentado.

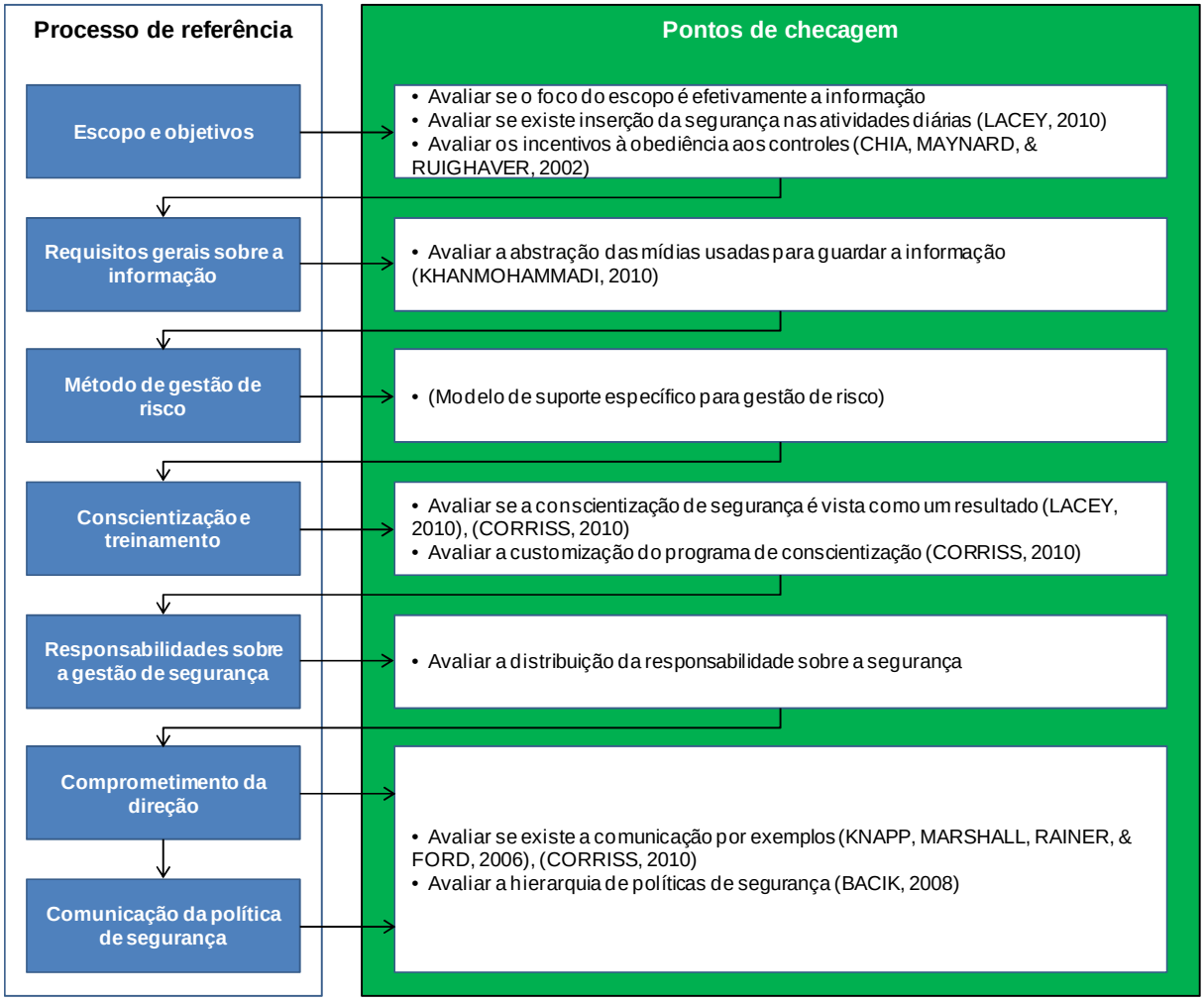

Figura 4 - Modelo de suporte para definição de políticas de segurança

7.2. SUPORTE A GESTÃO DE RISCOS

A gestão de riscos é o conjunto de atividades que está no núcleo do SGSI proposto pela ISO/IEC 27001. Através dele cria-se uma estruturada para a organização monitorar os níveis de segurança da informação. Isso é feito por meio de revisões periódicas dos níveis de risco, antes e depois da implantação de controles de segurança.

No entanto, como é visto a seguir, a efetividade do processo de gestão de riscos depende da organização ser capaz de executar várias atividades importantes, entre elas:

- Reconhecer exatamente quais são as informações da organização;
- Definir como essas informações estão relacionadas entre si;
- Identificar onde essas informações estão armazenadas;
- Identificar características dos meios de armazenamento, como ameaças e vulnerabilidades;
- Conciliar o grau de controle que possui sobre as informações e meios de armazenamento com suas necessidades de visibilidade sobre a situação de cada bloco de informação;
- Conseguir avaliar o impacto da perda de informações de maneira consistente;

Comparando a lista acima frente aos temas de preocupação com o novo cenário descritos na seção 5.4 vemos que existem diversos conflitos que precisam ser solucionados.

O modelo de suporte aqui proposto busca apresentar esses conflitos diretamente na fase de Planejamento da ISO/IEC 27001. Com isso, a organização pode melhor desenhar um método mais realista frente ao cenário externo, consciente das dificuldades que ele traz.

7.2.1. DESCRIÇÃO DE PROCESSO DE REFERÊNCIA

Conforme apresentado no capítulo 3.4, a Gestão de Risco é uma das atividades da etapa de Planejamento de um SGSI. Para o desenvolvimento do modelo de suporte, é importante entender como se desenvolve o processo típico dessa atividade.

Ao contrário do que acontece com a criação de Políticas de Segurança, a ISO apresenta na norma ISO/IEC 27005 um modelo bem claro de como deve ser executada essa atividade. Assim, com objetivo de manter o alinhamento com o SGSI proposto por essa entidade, utilizaremos a referência apresentada na norma.

A Figura 5 apresenta o processo de referência proposto pela ISO/IEC 27005. Na sequência, são descritos quais são as atividades a serem executadas, representadas por esta mesma figura.

Estabelecimento de escopo

A primeira etapa do processo de referência busca a definição de diretrizes gerais para condução de todo o processo. Nessa etapa são reunidas todas as informações da organização relevantes para a gestão de segurança da informação. Com isso busca-se o desenvolvimento de uma abordagem para tratamento de risco coerente com os objetivos da organização.

Nessa etapa, o passo mais crítico é a definição do escopo da gestão de risco. O escopo da análise corresponde à delimitação de uma área da organização que irá passar pela análise de riscos. Essa área deve ser delimitada de acordo com os interesses da organização em relação à segurança da informação. Em geral o escopo da gestão de riscos corresponde ao escopo do SGSI da organização, também definido na política de segurança.

Ainda nessa etapa é definida uma abordagem para condução da gestão de risco, no que diz respeito à profundidade e detalhamento dos impactos. É recomendado que seja escolhida uma abordagem mista, que combine análises superficiais rápidas de todo o escopo com análises detalhadas para ativos específicos considerados mais críticos do ponto de vista de segurança(ISO/IEC 27005, 2011).

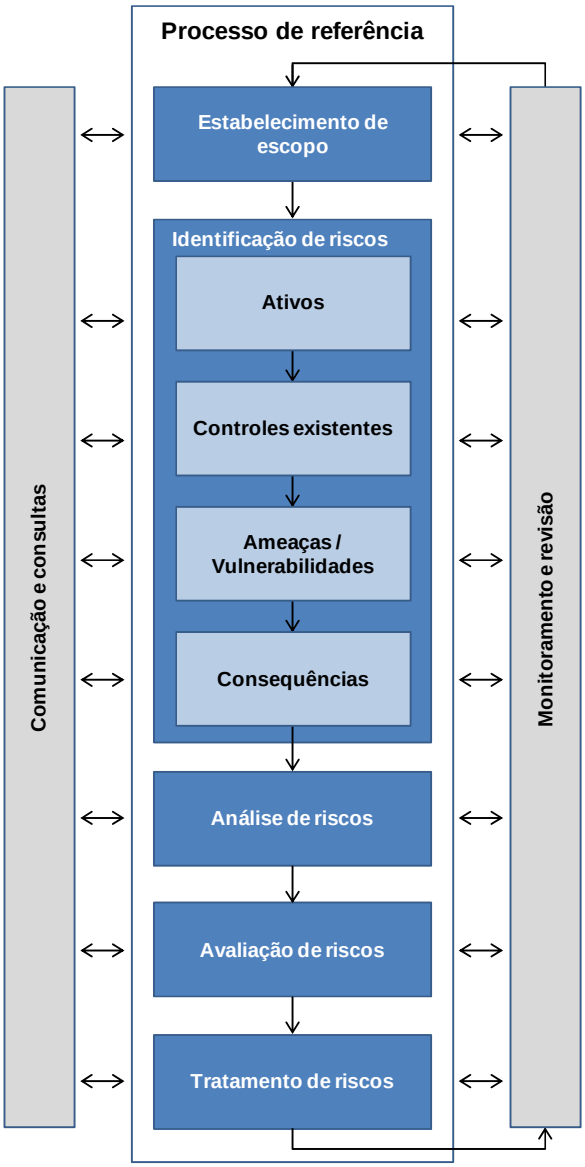

Figura 5 - Processo de referência para gestão de riscos (ISO/IEC 27005, 2011)

Finalmente, nessa etapa também são definidos critérios básicos que devem guiar todo o processo de gestão de riscos, como critérios de avaliação, critérios para análise de impactos e critérios de aceitação de riscos. A definição de critérios nessa etapa é importante para garantir que avaliações de riscos executadas em momentos diferentes e por times diferentes em contextos semelhantes produzam também resultados semelhantes.

Quando se leva em consideração todas as observações feitas a respeito do cenário externo, nota-se que existem diversos pontos de atenção a serem observados na etapa de Estabelecimento de Contexto. O cenário externo descrito

apresenta uma dinamicidade que dificulta a especificação de um escopo fixo de ativos para a gestão de riscos. Além disso, a escolha de uma abordagem detalhada torna-se, em muitos casos, impossível devido à falta de conhecimento e autoridade sobre os serviços de terceiros utilizados.

Identificação de riscos

A segunda etapa do processo de referência busca detalhar o escopo selecionado e obter mais informações sobre ele. Essa etapa pode ser dividida em 5 subatividades principais:

- **Levantamento de ativos** – Consiste na identificação dos ativos de informação que estão dentro do escopo de análise definido. Ativo de informação é tudo aquilo que pode conter ou transformar uma informação da organização. Exemplos:
  - Ambiente onde a informação será manipulada;
  - Processos executados sobre a informação;
  - *Software* utilizado pelos colaboradores;
  - *Hardware* utilizado pelos colaboradores;
  - Colaboradores que tem contato com a informação;
  - Terceiros que tem contato com a informação;
  - Documentos em mídia impressa;
  - Documentos em mídia digital;
  - Marca da organização;

- **Levantamento de vulnerabilidades** – Para cada ativo identificado, são identificadas as vulnerabilidades existentes. O levantamento de vulnerabilidades normalmente deve partir do responsável pelo ativo de informação. A responsabilidade pode ser determinada de maneiras diferentes de acordo com o tipo de ativo. Por exemplo: o responsável por um ambiente pode ser a pessoa mais sênior que trabalha naquele ambiente; o responsável por um documento pode ser a pessoa que criou a primeira revisão de um documento, ou que criou o modelo de daquele documento.

- **Levantamento de ameaças** – Para cada ativo identificado, também deve ser analisadas quais são as potenciais ameaças que podem explorar suas vulnerabilidades. Da mesma forma, é interessante que o responsável pelo ativo fique encarregado de identificar ameaças existentes. É importante notar que a existência de uma ameaça não significa que o ativo representa um risco para a organização – é necessária a existência de uma vulnerabilidade naquele ativo que possa ser explorada pela ameaça identificada.

- **Levantamento de controles existentes** – São levantados, por ativo do escopo, quais controles de segurança já estão sendo utilizados. Controles de segurança são os mecanismos implantados e ações executadas com o objetivo de mitigar alguma vulnerabilidade ou ameaça. Assim, o levantamento de controles existentes evita gastos com análises e implantação de novos controles para ameaças e vulnerabilidades já tratadas.

- **Levantamento de consequências** – Também para cada ativo são identificadas as consequências da sua perda, parada ou falha para os negócios da organização (incidentes de segurança da informação). Nesse momento o levantamento deve ser feito de forma preliminar, visando uma caracterização completa do ativo, mesmo que não seja possível quantificar numericamente os impactos de cada incidente.

Novamente, quando se considera o cenário externo descrito anteriormente, observa-se que as atividades descritas aqui podem ter sua eficácia seriamente afetada quando executadas em organizações inseridas nesse contexto. A dificuldade de obter informações e controlar infraestrutura baseada em serviços de terceiros dificulta não só o levantamento de vulnerabilidades ou ameaças, mas a própria definição de ativos que devem ser considerados no escopo da gestão de riscos.

Análise de riscos

A terceira etapa do processo de Gestão de Riscos visa à medição do risco vinculado a cada ativo existente dentro do escopo definido pela organização. Para tal procura-se estabelecer valores numéricos para a chance de uma vulnerabilidade ser explorada por uma ameaça e também para as consequências de um incidente de segurança envolvendo esses ativos. Compondo esses dois valores, chega-se a uma representação (qualitativa ou quantitativa) do risco para determinado ativo da informação.

Avaliação de riscos

A etapa de avaliação de riscos consiste na definição do que deverá ser feito com relação a cada risco identificado. Entre as opções comuns estão a de tratamento de riscos, aceitação de riscos e transferência dos riscos. Quando a organização define que o risco deverá será tratado, deve ser desenvolvido um plano de tratamento de riscos. Aqui são utilizados os critérios de avaliação e aceitação definidos na primeira etapa do modelo.

Tratamento de riscos

A última etapa da gestão de riscos é a definição de controles que deverão ser implantados para reduzir o risco a níveis aceitáveis pela organização. Com a definição do plano de tratamento de riscos finaliza-se o ciclo da Gestão de Riscos e, dentro do âmbito do SGSI, pode dar-se início a etapa de Implantação do ciclo PDCA (*Plan, Do, Check, Act*).

7.2.2. DEFINIÇÃO DE PONTOS DE CHECAGEM

Assim como no modelo criado para a elaboração de políticas de segurança, foram definidos também diversos pontos de checagem para a construção do modelo de suporte para Gestão de Riscos. Os mesmos temas apresentados na seção 5.4 também foram utilizados aqui como referência para a definição dos pontos de checagem.

A Tabela 7 indica como se dá a relação entre os pontos de checagem definidos para essa atividade e os temas de segurança identificados anteriormente.

	Tema / **Ponto de checagem**	**[T.1]**	**[T.2]**	**[T.3]**	**[T.4]**	**[T.5]**	**[T.6]**	**[T.7]**	**[T.8]**	**[T.9]**
	Estabelecimento de escopo									
PC.11	Avaliar quais são os escopos dos terceiros	**X**	**X**	**X**	**X**	**X**		**X**		
PC.12	Avaliar a seleção de serviços considerados no escopo			**X**	**X**	**X**		**X**		
	Identificação de riscos (Levantamento de ativos)									
PC.13	Avaliar a consideração de dispositivos dos terceiros								**X**	**X**
PC.14	Avaliar a consideração de ambientes de trabalho remoto							**X**	**X**	**X**
PC.15	Avaliar a consideração de ambientes dos terceiros							**X**	**X**	**X**
	Identificação de riscos (Levantamento de controles existentes)									
PC.16	Avaliar as funcionalidades de segurança dos terceiros	**X**	**X**	**X**		**X**	**X**			**X**
	Identificação de riscos (Levantamento de vulnerabilidades e ameaças)									
PC.17	Avaliar informações sobre a infraestrutura obtidas via terceiros	**X**	**X**	**X**	**X**	**X**		**X**		**X**
PC.18	Avaliar as vulnerabilidades de serviços consideradas	**X**		**X**	**X**	**X**			**X**	
PC.19	Avaliar o foco dado para pessoas e processos		**X**	**X**	**X**		**X**		**X**	
	Análise de riscos									
PC.20	Avaliar a experiência dos provedores de serviços	**X**	**X**			**X**				

	Avaliação de riscos									
PC.21	Avaliar os riscos juntamente com os provedores		**X**	**X**					**X**	
	Tratamento de riscos									
PC.22	Avaliar o alcance dos programas de conscientização			**X**	**X**		**X**			**X**
PC.23	Avaliar o isolamento de ambientes diferentes de trabalho			**X**				**X**	**X**	**X**
PC.24	Avaliar a possibilidade de acesso remoto seguro								**X**	**X**
PC.25	Avaliar a obtenção de outras garantias além de SLAs	**X**	**X**		**X**					

Tabela 7 - Relação entre pontos de checagem estabelecidos para suporte gestão de riscos e temas de segurança identificados

(SLA – *Service Level Agreement*)

A seguir é apresentado um detalhamento dos pontos de checagem, já seguindo a mesma ordem do processo de referência apresentado. Logo após a apresentação de cada ponto de checagem, é detalhado o racional que levou a vinculação dos mesmos aos temas na Tabela 7.

7.2.2.1. Estabelecimento de escopo

PC.11	**Avaliar quais são os escopos dos terceiros**
	(KHIDZIR, MOHAMED e ARSHAD, 2010) Muitos provedores de serviços permitem um determinado grau de visibilidade sobre a infraestrutura utilizada, incluindo modelos de equipamentos, topologias, protocolos e outros detalhes. Esse tipo de informação é relevante para uma definição adequada do escopo. A organização contratante deve, portanto procurar fornecedores que podem prover esse tipo de informação quando solicitada. Além disso, a organização deve buscar analisar os serviços oferecidos do ponto de vista da informação – determinados serviços podem ser excluídos do escopo se for entendido que eles não suportam processos que lidam com informações críticas para o negócio. Esse tipo de

consideração pode reduzir bastante a carga de trabalho e complexidade do processo de gestão de riscos.

Com o PC.11 busca-se o entendimento correto da forma de atuação dos provedores de serviços, de forma a facilitar a especificação do escopo da gestão de riscos. Ao compreender melhor a atuação dos provedores de serviços a organização mitiga as preocupações expressas pelos temas T.1, T.2, T.3, T.4 e T.7. Além disso, um correto entendimento dos escopos de terceiros atuais pode facilitar uma transição para outros no futuro, o que vincula o PC.11 ao T.5 também.

PC.12	**Avaliar a seleção de serviços considerados no escopo**

Não é viável exigir de serviços de computação em nuvem o mesmo grau de informação sobre a infraestrutura utilizada que é possível obter sobre uma infraestrutura própria e dedicada. A tecnologia no qual esse tipo de serviço é baseado foi criada de forma a aceitar um alto grau de incerteza com relação a, por exemplo, localização dos recursos alocados, ou configuração real dos mesmos.

A tendência é que o detalhamento da infraestrutura desse tipo de serviço seja excluído do escopo de gestão de riscos. Caso a organização sinta a necessidade de ter esse nível de detalhamento da informação, existe uma grande possibilidade que computação em nuvem não seja o modelo mais adequado de serviços para suportar o tipo de atividade executado.

Isso não exclui dos provedores de computação em nuvem a responsabilidade de oferecer informações e evidências de que o serviço oferecido garanta o grau de segurança adequado. Esses provedores devem estar em conformidade com as melhores práticas de segurança da informação e devem oferecer justificativas adequadas do ponto de vista de segurança.

No entanto, a dificuldade em detalhar a infraestrutura não significa que as informações armazenadas em provedores externos possam ser

desconsideradas totalmente. Caso esse provedor esteja lidando com informações sensíveis, é possível ainda considerar o serviço em si dentro do escopo ao invés da infraestrutura fornecida.

No PC.12 é sugerida a consideração de serviços dentro do escopo de ativos da gestão de riscos para casos onde não é possível uma correta visão da infraestrutura de suporte a esses serviços. Ao trabalhar com um nível de abstração maior, a organização pode reduzir a sua chance de tomar decisões fundamentadas em informações incorretas sobre a infraestrutura e riscos associados. Assim, esse ponto de checagem é vinculado aos temas T.3 e T.7. Além disso, uma correta consideração dos serviços prestados por terceiros desde o início da análise de risco pode facilitar a integração dos processos da empresa com o uso desses serviços. Daí o vínculo com o T.4. Finalmente, caso esse nível de abstração não seja adequado para os requisitos da organização, pode-se buscar outro provedor, o que vincula esse ponto de checagem também ao tema T.5.

7.2.2.2. Identificação de Riscos (Levantamento de Ativos)

PC.13	**Avaliar a consideração de dispositivos dos terceiros**

O levantamento de ativos da organização deve considerar equipamentos móveis, como *smartphones* e *tablets*, sejam eles fornecidos pela própria organização ou não. Uma das tendências mais fortes no cenário externo, a mobilidade, criou a necessidade de a organização conviver com dispositivos externos sendo utilizados para ou no trabalho, assim como dispositivos corporativos sendo utilizados para atividades pessoais. É crítico que essa necessidade não seja ignorada no momento da descrição de ativos de informação.

É possível que a organização prefira adotar uma abordagem mista para esses dispositivos, separando-os entre aqueles fornecidos pela própria organização e aqueles fornecidos por terceiros. Dessa forma, no

momento de avaliação dos riscos para cada categoria, a primeira pode ser tratada de maneira diferente que a segunda.

A inclusão de dispositivos de terceiros proposta pelo PC.13 leva a um novo nível de maturidade a respeito da consideração da informação da empresa, independente da localização da mesma. Assim esse ponto de checagem está vinculado aos temas T.8 e T.9.

PC.14	**Avaliar a consideração de ambientes de trabalho remoto**

Da mesma forma que a mobilidade traz a necessidade de considerar diferentes dispositivos de terceiros, é também necessário considerar o ambiente utilizado para acesso desses dispositivos. Atualmente o acesso à informação é realizado a partir de diversos tipos de ambientes, tais como residências, restaurantes e *lan houses*. Esses ambientes não oferecem as mesmas medidas de segurança que o ambiente organizacional. No entanto, esse tipo de ambiente precisa ser considerado na análise de riscos.

Novamente, é possível adotar uma abordagem mista nesses casos, tratando a infraestrutura utilizada por usuários remotos como um conjunto diferente de ativos daquele relacionado à infraestrutura da própria empresa.

A consideração dos ambientes remotos avaliada pelo PC.14 permite, da mesma forma que o PC.13, que a organização adote uma postura mais madura, focada na informação. No entanto, incorpora também a necessidade de permitir que a infraestrutura de trabalho remoto se integre de maneira adequada à infraestrutura da organização. Sendo assim, esse ponto de checagem é vinculado aos temas T.7, T.8 e T.9.

PC.15	**Avaliar a consideração de ambientes dos terceiros**

A infraestrutura utilizada pelos prestadores de serviços precisa ser considerada de alguma forma na análise de risco. De acordo com as

informações obtidas sobre essa infraestrutura, diferentes medidas podem ser aplicadas do lado da organização para garantir a segurança da informação.

Essa análise deve levar em consideração antes de tudo que tipo de informação trafega na infraestrutura e quais ativos primários são dependentes dela. Como resultado dessa análise pode-se decidir obter mais informações junto ao fornecedor sobre os componentes da infraestrutura oferecida. Quando isso não é possível, é importante considerar pelo menos o serviço oferecido pelo terceiro dentro do levantamento de ativos.

A escolha entre o detalhamento completo da infraestrutura ou apenas dos serviços deverão resultar também em escolhas sobre o grau de risco associado. Maior visibilidade implica em geral em maior controle dos riscos e menores investimentos em controles, enquanto que menor visibilidade implica em menor controle dos riscos e maiores investimentos em controles.

Da mesma forma que o PC.14, o PC.15 está vinculado aos temas T.7, T.8 e T.9. No entanto, ao invés de verificar a consideração de ambientes de trabalho remoto, leva a mesma ideia para os ambientes dos terceiros, ou seja, provedores de serviços ou outras localidades onde a informação da organização pode estar presente.

7.2.2.3. Identificação de Riscos (Levantamento de Controles Existentes)

PC.16	**Avaliar as funcionalidades de segurança dos terceiros**

(MÜLLER, HAN, *et al.*, 2011)

Durante o levantamento de controles existentes, é importante verificar com os provedores quais são as funcionalidades de segurança existentes nos serviços prestados. Logicamente, isso só será possível quando existe um canal de comunicação aberto para obtenção desse tipo de informação.

Existe uma tendência que riscos dos serviços fornecidos por terceiros sejam superdimensionados por falta de conhecimento sobre as funcionalidades de segurança oferecidas. A etapa de levantamento de controles existentes deve minimizar esse efeito.

O PC.16 procura avaliar se a organização está se informando sobre as funcionalidades de segurança disponibilizadas por novas tecnologias. Dessa forma, busca mitigar parte das preocupações expressas nos temas T.1, T.2, T.3 e T.9. Visto que a não consideração de determinadas funcionalidades de segurança pode levar a falhas de conformidade, também está vinculado ao tema T.6. Uma vez que a avaliação de funcionalidades pode facilitar a decisão a respeito da troca ou continuação com o provedor de serviços, esse ponto está também vinculado ao T.5.

7.2.2.4. Identificação de Riscos (Levantamento de Ameaças/Vulnerabilidades)

PC.17	**Avaliar informações sobre a infraestrutura obtidas via terceiros**

(CPNI, 2010), (CSA, 2009)

É importante que os responsáveis pelo ativo sejam envolvidos no processo de levantamento de vulnerabilidades, ameaças e controles existentes.

No caso de infraestrutura terceirizada, os indicados para a participação desse tipo de trabalho são os próprios fornecedores dos serviços. Esses possuem o conhecimento necessário sobre a infraestrutura para identificar potenciais vulnerabilidades e ameaças. Logicamente, as informações obtidas precisam passar por uma análise cuidadosa quanto a sua transparência.

Esse tipo de consulta também pode oferecer informações importantes sobre formas mais seguras de integrar os serviços com o restante da infraestrutura. Além disso, pode trazer soluções para futuros problemas de segurança causados por dificuldades de integração de tecnologia e processos.

No PC.17, procura-se avaliar se a organização leva em consideração nas suas análises eventuais informações fornecidas por terceiros a respeito de ameaças e vulnerabilidades que precisam ser consideradas. A consideração dessas informações pode levar a uma melhor escolha de serviços oferecidos e melhor avaliação dos riscos oferecidos, o que vincula esse ponto de checagem ao T.5. Além disso, devido às suas características, esse ponto de checagem é vinculado aos temas T.1, T.2, T3, T.4, T.7 e T.9.

PC.18	**Avaliar as vulnerabilidades de serviços consideradas**

Quando a organização utiliza serviços de terceiros, é possível que não se possa detalhar ameaças e vulnerabilidades da infraestrutura que suporta esses serviços. Nesses casos, é necessário que o próprio serviço seja analisado em busca de vulnerabilidades que possam afetar o acesso a informação.

Como exemplo, podem ser citadas vulnerabilidades como sobrecarga de enlaces de dados, indisponibilidade de conexão, quedas de servidores. Ao lidar com esse tipo de vulnerabilidade, podem ser sugeridos controles adicionais como a utilização de provedores múltiplos e a exigência de níveis de serviço customizados.

O PC.19 tenta eliminar a necessidade de detalhamento de todas as características de elementos da infraestrutura de terceiros durante o processo de gestão de riscos, buscando ao invés disso a avaliação do serviço prestado. Com isso, a organização ganha um grau de confiança maior a respeito dos riscos com os quais está lidando, e foge de potenciais falhas causadas por falta de visibilidade sobre a infraestrutura do terceiro. A melhor capacidade de analisar os serviços prestados, proporcionada pelo seguimento desse ponto de checagem, o vincula aos temas T.1, T.4 e T.5. Já a eliminação da necessidade de conhecimento detalhado da infraestrutura o vincula aos temas T.3 e T.8.

PC.19	**Avaliar o foco dado para pessoas e processos**

(LACEY, 2010)

A variedade e dinamicidade do cenário externo descrito impedem o mapeamento de todas as possíveis vulnerabilidades existentes na infraestrutura, em especial quando consideramos o uso de infraestrutura, dispositivos e ambientes de terceiros. Além disso, fatores como mobilidade e integração de ambientes profissional e pessoal tornam ainda mais difíceis a tarefa de mapear as vulnerabilidades ou de criar controles para mitigação.

Assim, é necessária uma maior atenção para as vulnerabilidades existentes com relação a pessoas e processos. A gestão de segurança irá sempre esbarrar na dificuldade de conscientização de usuários sobre a importância de controles. No entanto, mais do que nunca, é necessário que elas estejam conscientes sobre o seu impacto na segurança organizacional.

Da mesma forma que é importante para a organização considerar os serviços disponíveis durante a análise de riscos, também é necessário considerar pessoas e processos. Esse é o foco do PC.19. As pessoas, desde que bem treinadas, podem fazer com que situações inesperadas sejam contornadas de forma a manter a segurança das informações. Assim, esse ponto de checagem está vinculado aos temas T.2, T.4 e T.6. Processos bem montados e pessoas conscientes sobre o seu papel de segurança podem ajudar a eliminar os efeitos da falta de conhecimento sobre as novas tendências tecnológicas. Por isso, o ponto também é vinculado aos temas T.3 e T.8.

7.2.2.5. Análise de Riscos

PC.20	Avaliar a experiência dos provedores de serviços

A aparente falta de controle e visibilidade sobre a infraestrutura terceirizada não pode criar na organização o receio durante a análise de riscos dos serviços associados.

A contratação de terceirização de infraestrutura de TIC ou computação em nuvem é motivada também pelo conhecimento técnico e experiência oferecida pelo provedor. Isso deve ser levado em consideração na análise de riscos.

Por um lado deve-se esperar que os riscos causados pela dificuldade de integração de processo entre provedor e organização sejam maiores do que se a infraestrutura fosse toda interna. Por outro lado, os riscos esperados devido a problemas técnicos devem ser menores, visto que o provedor de serviço possui normalmente requisitos e padrões de segurança mais rígidos a serem seguidos.

A análise da experiência dos provedores e uso dessa durante a análise de risco é o objetivo do PC.20. Uma correta avaliação dessa experiência pode ajudar a mitigar as preocupações expressas pelos temas T.1, T.2 e T.5.

7.2.2.6. Avaliação de Riscos

PC.21	Avaliar os riscos juntamente com os provedores

(CPNI, 2010), (CSA, 2009)

Ao utilizar provedores de serviços para terceirização de TIC ou computação em nuvem, é importante que exista um canal de comunicação aberto para reportar os resultados das avaliações de riscos executadas. Esse tipo de comunicação deve acontecer antes do plano de tratamento de riscos.

Através da troca de informações com o provedor de serviços é possível verificar se os riscos identificados são justificáveis. Além disso, o provedor pode indicar quais são as ações recomendadas para evitar investimentos desnecessários do lado do cliente.

Ao validar parte dos riscos observados com os provedores, proposta do PC.21, a organização busca aumentar o seu conhecimento sobre o cenário externo e melhor embasar os controles a serem implantados. Dessa forma, pode-se vincular o ponto de checagem aos temas T.2, T.3 e T.8.

7.2.2.7. Tratamento de Riscos

PC.22	**Avaliar o alcance dos programas de conscientização**

(CORRISS, 2010)

A execução de programas de conscientização de usuários é um controle típico presente em diversas iniciativas de segurança. No entanto em muitos casos esse tipo de programa aborda o problema de forma simplista, atacando apenas incidentes típicos como divulgação de senhas, acesso a *sites* restritos, etc.

Considerando o cenário externo descrito, esse tipo de abordagem perde grande parte da sua efetividade, uma vez que os incidentes nesse cenário não são facilmente identificáveis ou associáveis aos incidentes básicos descritos.

Por isso é necessária uma evolução dos programas de conscientização em segurança, com maior foco em tópicos mais conceituais em segurança da informação. Entre esses tópicos deve ser dado destaque à identificação e à reação adequada para novos incidentes de segurança.

O objetivo do PC.22 é levar aos programas de conscientização da organização conceitos mais básicos de segurança, visando assim preparar os colaboradores para identificação natural de diferentes tipos de incidentes. Com isso, mesmo com pouco conhecimento a respeito da infraestrutura de terceiros ou de novas tecnologias, a organização pode alcançar uma melhor proteção da informação. Assim, os temas relacionados a esse ponto de checagem são os T.3, T.4 e T.9. Visto que parte do programa de conscientização e divulgar a política de segurança da organização, o ponto de checagem em análise também é vinculado ao T.6.

PC.23	**Avaliar o isolamento de ambientes diferentes de trabalho**

A mesma tecnologia de virtualização, que traz tantas novas complexidades para a segurança quando utilizada em serviços oferecidos por provedores de computação pode também trazer soluções.

Uma forma cada vez mais comum de lidar com a multiplicidade de equipamentos de usuários é a criação de ambientes virtuais que são acessados de dispositivos diferentes. Nesses ambientes padronizados e isolados o usuário pode trabalhar com limites mínimos de segurança.

Esse tipo de recursos só torna-se viável a partir do momento em que os dispositivos e os enlaces de comunicação utilizados oferecerem o poder de processamento e banda necessários.

O PC.23 busca avaliar se não é interessante para a organização fazer uso de tecnologias de virtualização para criação de ambientes de trabalho isolados. A criação desses ambientes facilitaria a integração de infraestrutura terceira com a da organização, como por exemplo, dispositivos móveis. Sendo assim, esse ponto de checagem pode ser vinculado ao T.7. Além disso, esse recurso de isolamento pode garantir uma maior proteção das informações mesmo sem muito conhecimento sobre a infraestrutura utilizada pelo terceiro. Dessa forma, pode-se relacionar o ponto de checagem também aos temas T.3, T.8 e T.9.

PC.24	Avaliar a possibilidade de acesso remoto seguro

Apesar de a mobilidade permitir que o usuário tenha em qualquer lugar recursos de processamento e memória suficientes para executar muitas funções, ainda existem limitações. Uma delas, muito importante, é que existirá sempre a necessidade de acesso a informações centralizadas.

Sendo assim, a organização precisa estar preparada para fornecer formas de acesso seguro a seus colaboradores móveis. No novo cenário esse tipo de controle de segurança deixa de ser uma exclusividade de grandes empresas e passa a ser um serviço indispensável para o trabalho.

A disponibilização de formas de acesso remoto seguro proposta pelo PC.24 visa principalmente a integração de infraestrutura terceira – no caso, a disponível no ambiente remoto – com a da organização de forma a proteger as informações trocadas entre elas. Por causa disso, relaciona-se esse ponto de checagem apenas aos temas T.8 e T.9.

PC.25	Avaliar a obtenção de outras garantias além de SLAs

(JAKOUBI, TJOA, *et al.*, 2010)

Uma forma típica de lidar com terceiros do ponto de vista de segurança da informação é o estabelecimento de Acordos de Nível de Serviço (SLA – *Service Level Agreement*) que levassem em consideração aspectos de segurança. Esse tipo de acordo serve como base de defesa da organização no caso de algum causado por falhas de conduta do terceiro quanto à informação.

Por causa disso é comum que para os novos serviços de terceirização e de computação em nuvem também sejam solicitados SLAs. No entanto, no novo cenário tecnológico, o SLA pode criar apenas uma falta sensação de segurança. Por causa disso, o SLA não deve ser visto como o único controle disponível à organização para garantir a segurança.

A organização precisa estar preparada para implantar outros tipos de controle para mitigar os riscos identificados, como por exemplo, a utilização

de um segundo provedor do serviço, a criação de infraestrutura própria de backup, e assim por diante.

Antes do estabelecimento do SLA, a organização precisa se certificar da viabilidade e disposição do terceiro para trabalhar em conjunto para adaptação de processos de segurança da informação.

O PC.25 procura verificar que a organização está trabalhando focada realmente na proteção da informação e no risco de ataques. Para tal, propõe a busca por outros controles de segurança além dos SLAs para aumentar o grau de segurança da informação. A busca por uma maior confiabilidade frente a prestação de serviços dos provedores terceiros permite criar o vínculo desse ponto de checagem aos temas T.1, T.2 e T.4.

7.2.3. CONSTRUÇÃO DO MODELO DE SUPORTE

O modelo de suporte proposto para gestão de riscos, apresentado na Figura 6 complementa o processo de referência descrito para essa atividade. Como pode ser observado são inseridos 15 pontos de checagem a serem verificado ao longo das 8 principais etapas típicas da atividade. A representação gráfica do modelo indica os momentos mais adequados para a análise de cada ponto de checagem. Dessa forma, busca-se o desenvolvimento de uma ferramenta prática a ser utilizada na execução desse processo.

As descrições apresentadas para cada ponto de checagem fornecem um direcionamento sobre quais resultados devem ser esperados com a observação de cada ponto.

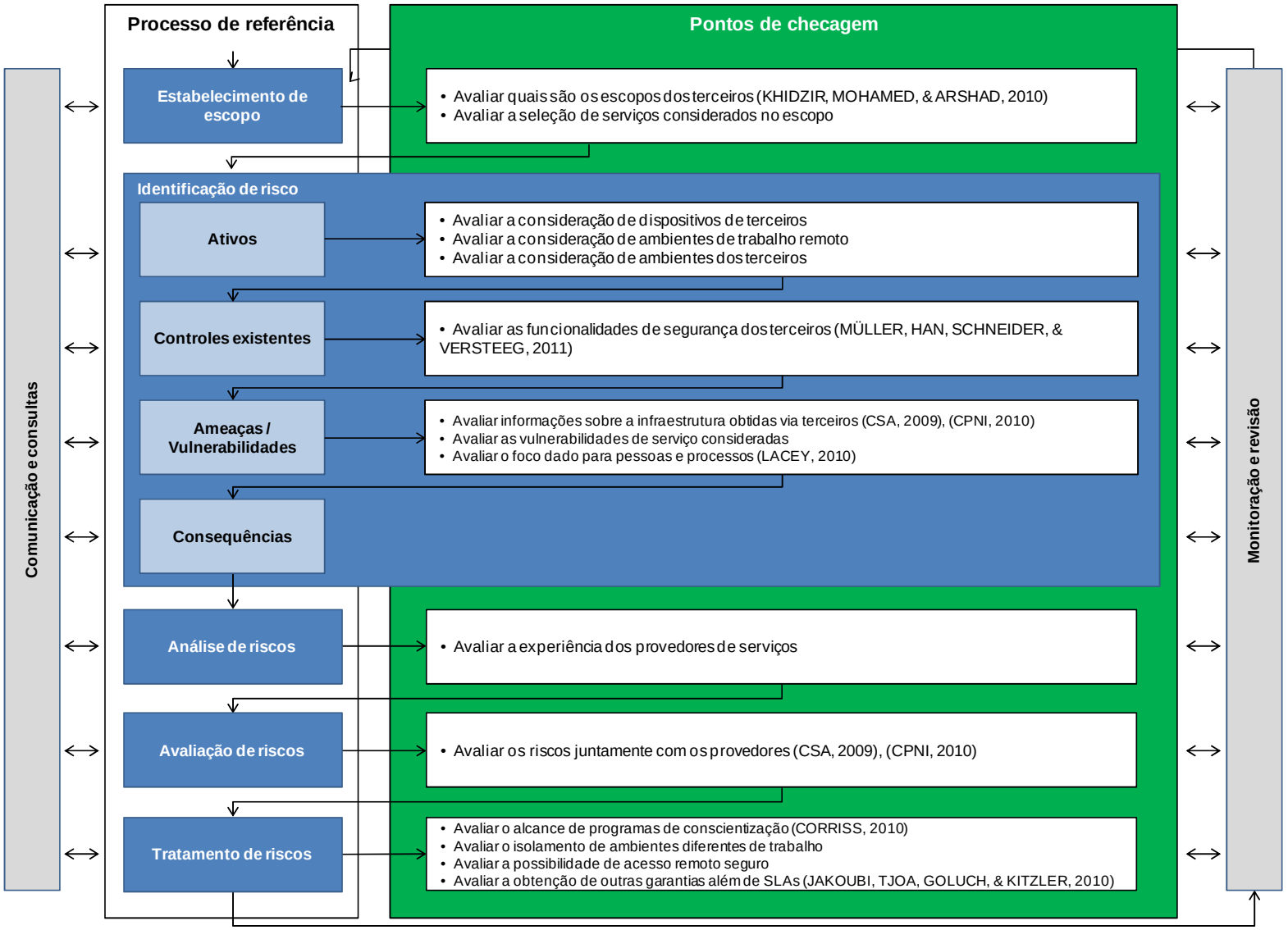

Figura 6 - Modelo de suporte a gestão de riscos

7.3. CONSIDERAÇÕES FINAIS

Os modelos de suporte foram fundamentados em uma análise a respeito dos temas de preocupação com segurança identificados na sessão 5.5. Esses temas, por sua vez, tiveram origem nos riscos identificados para a terceirização de infraestrutura de TIC, computação em nuvem e mobilidade.

Os temas foram confrontados com conclusões de estudos da literatura sobre os desafios de segurança existentes em cada tendência tecnológica e com relação à implantação de SGSIs em gera. A partir desse confronto, foram definidos diversos pontos de checagem, os quais são utilizados para modificar os fluxos de atividades típicas da fase de Planejamento da ISO/IEC 27001.

Cada um dos modelos de suporte criados deve ser utilizado como uma referência, adaptando os comentários apresentados em cada ponto de checagem para o contexto da organização. A correta adaptação da abordagem para definição de políticas de segurança e gestão de risco deve proporcionar à organização uma melhor preparação para proteger suas informações frente ao novo cenário tecnológico.

8. VALIDAÇÃO VIA ESTUDO DE APLICABILIDADE

Com o objetivo de analisar a aplicação do modelo de suporte proposto em uma situação real, foi conduzido um estudo de aplicabilidade, cujos resultados são aqui apresentados.

O estudo foi conduzido em uma empresa, aqui identificada como INTEGRA, parte de um grande grupo brasileiro, aqui identificado como INFRA. A INTEGRA atua no setor de integração de soluções de Tecnologia da Informação e Comunicação (TIC). O grupo INFRA atua em grandes projetos de infraestrutura por meio de empresas de engenharia que o compõe.

Esse capítulo divide-se nas seguintes seções:

- **Contextualização da INTEGRA** – Apresenta um breve histórico da empresa e sua situação em relação à infraestrutura;
- **Gestão de Segurança na INTEGRA** – Detalha a situação do SGSI da empresa e a certificação ISO/IEC 27001;
- **Impactos do cenário externo para a INTEGRA** – Mostra como as tendências tecnológicas externas estão sendo trabalhadas dentro da empresa e as discussões existentes quanto à segurança;
- **Integração aos processos de referência** – Verifica se a empresa se encaixa dentro dos processos utilizados como base para construção do modelo de suporte;
- **Aplicação do modelo de suporte** – Realiza uma análise do grau de mudanças necessárias no caso de uma eventual aplicação do modelo de suporte proposto no trabalho.

8.1. CONTEXTUALIZAÇÃO DA INTEGRA

O grupo INFRA foi fundado há mais de 50 anos no Brasil. Através da atuação em grandes projetos para empresas de telecomunicação o grupo adquiriu grande quantidade de conhecimento nessa área. Em 2000, observando o potencial

crescimento do mercado criou a INTEGRA. Essa empresa passou a concentrar todos os projetos e investimentos do grupo no setor de TIC.

Desde a sua fundação até hoje, a INTEGRA já passou por diversas transformações organizacionais profundas, voltadas à adequação de seus negócios. Essas alterações foram motivadas principalmente pelas constantes mudanças do mercado de tecnologia, comuns até hoje. Por causa disso, a INTEGRA precisou alterar muitas vezes seus processos de gestão e o portfólio de serviços e produtos oferecidos ao mercado. Atualmente a INTEGRA é uma das maiores integradora de soluções de TIC do Brasil e conta com mais de 600 funcionários.

No seu ramo de atuação, a INTEGRA se especializou em combinar equipamentos de diversos fabricantes para criar soluções que atendem as necessidades de diversos tipos de clientes. Para tal, a INTEGRA conta com uma extensa lista de parceiros de negócios responsáveis por fornecer os equipamentos necessários para a construção dessas soluções. A combinação desses blocos exige alto grau de conhecimento técnico, o qual a INTEGRA oferece na forma de serviços profissionais. Esse conhecimento e a experiência da INTEGRA tornaram-se grandes fatores de diferenciação no mercado, motivando empresas de grande porte a buscarem os serviços da INTEGRA. Além da integração de sistemas, a INTEGRA também oferece serviços de consultoria, para a análise das necessidades do cliente, e de suporte, para manutenção das soluções vendidas. Durante boa parte da sua história a INTEGRA teve como principais clientes grandes operadoras de redes de telecomunicação brasileiras. Mais recentemente, esse cenário mudou com a entrada de muitos clientes de outras verticais do mercado, como saúde, óleo e gás, mineração, etc.

Devido ao seu ramo de trabalho, a INTEGRA precisa contar com uma infraestrutura de TIC muito robusta e flexível. Essa infraestrutura inclui inicialmente todas as soluções comuns de uma empresa típica – servidores de arquivos, e-mail, *Enterprise Resource Planning* (ERP), etc. Além disso, inclui uma grande quantidade de soluções específicas, semelhantes as que a INTEGRA vende para seus clientes – telepresença, videoconferência, telefonia, colaboração, mensageria, redes sociais, etc. Dessa forma, além de aproveitar os benefícios que essas soluções trazem para o trabalho, a INTEGRA utiliza o seu próprio ambiente para demonstrações para seus clientes.

Para garantir a qualidade dos serviços prestados, a INTEGRA conta com um avançado sistema de gestão, responsável pelo controle de todas as operações da organização. Como resultado desse sistema de gestão, a INTEGRA já recebeu a certificações da ISO 9000, ISO/IEC 20000 e ISO/IEC 27001, voltadas respectivamente a qualidade, serviços e segurança da informação.

8.2. GESTÃO DE SEGURANÇA NA INTEGRA

Todas as empresas do grupo INFRA lidam diretamente com grandes clientes no Brasil, através de projetos de durações variadas executados nas suas diversas áreas de atuação. Além disso, elas têm associações com diversas entidades externas: fornecedores fixos, fornecedores temporários, institutos de pesquisa e parceiros de negócio. Assim, existe uma grande quantidade de informações que precisa ser trocada diariamente entre essas entidades. Buscando prezar proteção dessas informações, o grupo INFRA decidiu investir na criação de um Sistema de Gestão de Segurança da Informação (SGSI), utilizando como base a norma ISO/IEC 27001. Os processos de gestão de segurança e o escopo do SGSI cobrem todas as áreas da empresa.

Devido a algumas demandas de clientes, o grupo INFRA contratou auditorias externas para a certificação do seu SGSI. No entanto, na certificação de todas as empresas foi incluída apenas a área, equipe e processos responsáveis pela engenharia comercial. Esse escopo de certificação, válido para todas as empresas do grupo, foi o resultado de uma análise estratégica que apontou um alto grau de sensibilidade das informações manipuladas por essa área. Devido a uma forte cultura de gestão, a certificação ISO/IEC 27001 foi conquistada pela primeira vez em 2006, logo após a implantação do SGSI. Essa foi uma das primeiras certificações da norma que aconteceram no Brasil. Desde então, as principais empresas do grupo, entre elas a INTEGRA, passam regularmente por auditorias de certificação. Depois de alguns anos, em 2010, a INTEGRA, também como resultado de uma análise estratégica, decidiu estender o seu escopo de certificação para toda a empresa.

A INTEGRA possui um sistema de documentação no qual armazena as informações relacionadas a todos seus sistemas de gestão, incluindo o SGSI. Uma

vez que a INTEGRA mantém seus diversos sistemas de gestão combinados e integrados com os processos organizacionais. A documentação de cada sistema foi adaptada para convergir com os processos internos, o que resultou em uma segmentação não convencional de informações. Felizmente, a INTEGRA mantém uma tabela de correlação entre os itens da norma ISO/IEC 27001 e as seções do seu sistema de documentação.

Para fins da análise conduzida nesse estudo de caso, a seguir são descritos os principais elementos do SGSI da INTEGRA, já separando-os dentro das fases do ciclo PDCA da ISO/IEC 27001.

Planejamento (*Plan*)

A INTEGRA dedica diversas seções da sua documentação para os resultados dessa fase do ciclo. São elas:

- **Considerações gerais do SGSI** – Contém o reconhecimento do valor dos ativos de informação para a empresa e a declaração do escopo atual do SGSI;
- **Política da Informação Corporativa** – Contém declarações a respeito das responsabilidades sobre a informação, requisitos para ativos de informação e o modelo utilizado para classificação da informação;
- **Política de Segurança da Informação** – Contém os principais conceitos relacionados à segurança da informação corporativa, tais como propriedades da informação a serem protegidas;
- **Levantamento e Classificação dos Ativos** – Contém parte dos aspectos do processo de gestão de riscos, tais como a finalidade da gestão de riscos, a importância da precisão sobre a classificação e instruções para classificação de riscos voltados às propriedades da informação;
- **Avaliação e Gerenciamento de Riscos** – Contém outros aspectos do processo da gestão de riscos, entre eles o método de cálculo de riscos e níveis de riscos aceitáveis;

- **Responsabilidades sobre o SGSI** – Contém maiores detalhes a respeito das responsabilidades pelo SGSI em si e também sobre determinados ativos de informação. Indica também quem são os membros do Grupo Gestor de Segurança da Informação, responsável pelas análises críticas do SGSI demais processos relacionados;
- **Divulgação do SGSI** – Apresenta como a política de segurança da informação deverá ser divulgada.

Execução (*Do*)

Dado o caráter mais direto dessa etapa do SGSI, a INTEGRA dedica uma seção de documentação:

- **Tratamento de riscos** – Contém diretrizes para criação de controles que sigam o plano de tratamento de riscos estabelecido durante o Planejamento.

Checagem (*Check*)

Com relação à fase de Checagem, a INTEGRA dedica também uma seção da documentação:

- **Gerenciamento de indicadores** – Contém uma especificação de como deve ser conduzida a avaliação de conformidade do SGSI. Especifica que os objetivos do SGSI devem ser acompanhados através de registros de incidentes de segurança, planos de ação, controles e pesquisas internas. Também indica que deverão acontecer comparações de indicadores históricos para avaliação da evolução do SGSI.

Atuação (*Act*)

Para a etapa de Atuação, a INTEGRA apresenta as seguintes seções de documentação:

- **Análise crítica, monitoramento e revisão do sistema** – Contém uma especificação de como devem ser conduzidas as revisões periódicas de riscos e quais são os tipos de ação de melhoria esperadas dessas revisões;
- **Tratamento de não-conformidades** – Contém uma especificação de quais devem ser as ações corretivas e preventivas para garantir a manutenção dos níveis de risco previstos pela organização.
- **Auditorias internas** – Contém detalhes a respeito de responsabilidades, métodos e resultados para condução de auditorias de verificação do SGSI.

O sistema de documentação da INTEGRA armazena informações que sofrem poucas alterações ao longo do tempo. Além dessas, o SGSI da INTEGRA gera uma série de outros documentos de suporte, alterados periodicamente:

- **Planejamento** – Inventário de ativos e resultados da análise de risco;
- **Checagem** – Controle e acompanhamento dos planos de ação;
- **Atuação** – Resultados das revisões periódicas voltadas à análise crítica.

Atualmente, a INTEGRA executa um ciclo PDCA uma vez a cada 12 meses. Durante os primeiros anos, na criação do SGSI, esse ciclo era de 6 meses, devido à necessidade de reforçar as alterações de processos na organização.

8.3. IMPACTOS DO CENÁRIO EXTERNO PARA A INTEGRA

Como grande parte das empresas do seu setor de atuação, a INTEGRA está inserida no cenário tecnológico descrito na seção 4. Como pode ser observado a seguir, ela faz uso da terceirização de infraestrutura de TIC, computação em nuvem e mobilidade, integrando essas tecnologias aos seus negócios.

8.3.1. TERCEIRIZAÇÃO DA INFRAESTRUTURA DE TIC

Desde a sua fundação o grupo INFRA buscou melhoras nas operações de suas diversas empresas, identificando sinergias entre elas. A área de TIC foi escolhida como uma potencial área para compartilhamento de recursos entre as empresas. Como parte da sua estratégia de TIC, o grupo decidiu, em 2003, fazer a terceirização completa de infraestrutura para um provedor de serviços externo. Essa terceirização abrangia todas as soluções comuns entre as empresas, como servidores de arquivos, e-mail e ERP.

A partir de 2010 a INTEGRA passou a oferecer de maneira mais efetiva serviços de terceirização de infraestrutura de TIC para seus clientes. Esses serviços são prestados por uma área interna da INTEGRA. Sendo assim, não fazia mais sentido que o grupo INFRA utilizasse serviços externos. Assim, o papel do provedor externo para o grupo foi assumido por um provedor interno, dentro da própria INTEGRA. No entanto, para todos os efeitos, a INTEGRA, assim como todas as empresas do grupo INFRA, são tratadas simplesmente como mais um cliente desse provedor interno.

A transição inicial da infraestrutura para o provedor externo em 2003 foi bem complexa, exigindo a absorção de equipes por terceiros, movimentação física de equipamentos, adequação de processos e de estrutura de custeio. Como na época a certificação ISO/IEC 27001 já estava válida, a INTEGRA foi obrigada a negociar com o provedor externo que as políticas de segurança da informação seriam seguidas no novo ambiente. Logicamente isso resultou em alterações também do ponto de vista dos processos de segurança. Felizmente, devido ao porte do provedor externo, muitas das medidas necessárias de segurança já existiam, pois tinham sido implantadas para outros clientes.

Na segunda transição, para o provedor interno, novamente foram necessárias diversas mudanças, tais como contratação de equipes, treinamento, adequação de infraestrutura de servidores, movimentação de equipamentos, etc. O provedor interno, de porte bem menor, não possuía todos os controles necessários para a manutenção dos níveis de risco previstos no SGSI da INTEGRA. Assim, entre as mudanças, uma das principais foi à adequação da infraestrutura da área de serviços para garantir que todos os controles existentes no ambiente do provedor externo fossem mantidos.

Dessa forma pode-se notar que a INTEGRA tem grande experiência com a terceirização de infraestrutura de TIC. Não só ela utiliza atualmente esses serviços fornecidos por um provedor interno como também presta esses serviços para clientes.

8.3.2. COMPUTAÇÃO EM NUVEM

A INTEGRA foi uma das primeiras empresas a utilizar serviços disponibilizados por provedores de nuvem, reconhecendo o valor desse tipo de plataforma. Por causa dessa experiência, atualmente processos importantes de negócio da INTEGRA utilizam plataformas de computação em nuvem, através de aplicações no modelo *Software-as-a-Service* (SaaS).

O primeiro deles, utilizado na área de Engenharia Comercial, é um software de Gerenciamento do Relacionamento com Clientes (*Customer Relationship Management* – CRM). Esse *software* armazena diversas informações a respeito de oportunidades de negócio em andamento com cada cliente. Apenas alguns membros da equipe possuem acesso para cadastro de novas informações no software. No entanto, muitas equipes precisam ter acesso às informações armazenadas – dessa forma, existem diversos relatórios gerados que são disponibilizados sistematicamente pela ferramenta.

O segundo deles, utilizado pela área de Serviços, é um software de Gerenciamento de Serviços de IT (*IT Service Management* – ITSM). Nele são recebidos e cadastrados todos os incidentes e solicitações dos clientes. Além disso, esse *software* está integrado com plataformas locais, para coleta de alarmes de infraestrutura. Todos os incidentes gerados são acessados por uma equipe de analistas e especialistas.

A INTEGRA utiliza também uma plataforma de conferências no formato SaaS, para realização de reuniões internas e externas. Essa plataforma permite, além da conversa por voz e vídeo, a troca de conteúdo entre os participantes da reunião, tais como apresentações e documento,

A utilização desses sistemas, como acontece para maior parte de aplicações SaaS, foi definida primariamente devidos às diversas vantagens encontradas. Entre as vantagens estão o custo adequado, a facilidade de administração e a flexibilidade.

No entanto, a INTEGRA tem diversos questionamentos a respeito da segurança dessas aplicações, visto que muitas das informações armazenadas nelas são bem sensíveis do ponto de vista do SGSI. A sensibilidade das informações se deve ao alto impacto gerado por uma eventual quebra de confidencialidade, integridade ou disponibilidade.

8.3.3. MOBILIDADE

A INTEGRA também está profundamente inserida no contexto da mobilidade. Dada a grande interação com entidades externas (clientes, parceiros e fornecedores), a INTEGRA precisa disponibilizar dispositivos móveis para que seus funcionários possam trabalhar fora do escritório. Recentemente ocorreu uma atualização de todos os aparelhos celulares corporativos para *smartphones* e, em menor número, *tablets.* Os equipamentos disponibilizados possuem uma série de aplicativos pré-configurados. Entre esses, incluem-se clientes para acesso a toda a infraestrutura corporativa, incluindo aquela terceirizada com o provedor interno e aquelas disponibilizadas pelos provedores de nuvem.

Além dos dispositivos corporativos, existem hoje inúmeros dispositivos pessoais sendo utilizados para acesso à infraestrutura. Esses dispositivos são utilizados principalmente para o trabalho de profissionais que não receberam equipamentos corporativos. Por causa disso, a INTEGRA reconhece que não pode simplesmente bloquear o acesso desses funcionários à infraestrutura, uma vez que isso iria impactar as operações da empresa. Isso gera atualmente uma grande discussão a respeito possibilidade ou não da INTEGRA incentivar o uso de dispositivos pessoais para o trabalho.

Recentemente, como mais um passo para aumento da mobilidade de seus profissionais, a INTEGRA instituiu um programa de trabalho remoto. Nesse programa, alguns funcionários, de acordo com regras específicas, podem realizar trabalhos de suas residências.

8.4. INTEGRAÇÃO AOS PROCESSOS DE REFERÊNCIA

Analisando o apresentado anteriormente, nota-se que a INTEGRA, conforme especificado pela ISO/IEC 27001, executa as duas atividades principais previstas na fase de Planejamento: definição da Política de Segurança e a Gestão de Risco.

Para fins de aplicação do modelo de suporte proposto ao caso da INTEGRA, a seguir é feita uma análise de como os resultados dessa fase nessa empresa se encaixam com os processos de referência identificados nas seções 7.1.1 e 0. Para cada passo do processo de referência são apresentadas evidências da sua execução.

8.4.1. DEFINIÇÃO DE POLÍTICA DE SEGURANÇA

A INTEGRA executa o processo de referência para políticas de segurança, apresentado na Figura 3, conforme demonstrado na Tabela 8.

Passos do processo de referência	**Evidências na documentação do SGSI INTEGRA**
Escopo e objetivos	• Considerações gerais do SGSI
Requisitos gerais sobre a informação	• Política da Informação Corporativa • Política de Segurança da Informação
Metodologia de gestão de risco	• Levantamento e Classificação dos Ativos • Avaliação e Gerenciamento de Riscos
Conscientização e treinamento	• Divulgação do SGSI
Responsabilidades sobre a gestão de segurança	• Política da Informação Corporativa • Responsabilidades sobre o SGSI
Comprometimento da direção	• Responsabilidades sobre o SGSI
Comunicação da política de segurança	• Política de Segurança da Informação • Divulgação do SGSI

Tabela 8 - Evidências referentes ao processo de referência para definição de políticas de segurança

Além dessas evidências, a INTEGRA possui outros registros que demonstram a execução de cada passo do processo de referência, tais como:

- Apresentações utilizadas em treinamentos internos de segurança (Conscientização e treinamento);
- Lembretes e dicas sobre segurança apresentados na rede corporativa (Conscientização e treinamento);
- Carta de aprovação da política de segurança pela direção da empresa (Comprometimento da direção).

8.4.2. GESTÃO DE RISCO

Da mesma forma, a INTEGRA executa o processo de referência para gestão de risco, apresentado na Figura 5, conforme demonstrado na Tabela 8.

Passos do processo de referência	**Evidências na documentação do SGSI INTEGRA**
Estabelecimento de contexto	• Levantamento e classificação de ativos
Identificação de riscos (Levantamento de Ativos)	• Levantamento e classificação de ativos
Identificação de riscos (Levantamento de controles existentes)	• Levantamento e classificação de ativos
Identificação de riscos (Levantamento de ameaças/vulnerabilidades)	• Levantamento e classificação de ativos
Identificação de riscos (Levantamento de consequências)	• Levantamento e classificação de ativos
Análise de riscos	• Avaliação e Gerenciamento de Riscos
Avaliação de riscos	• Avaliação e Gerenciamento de Riscos
Tratamento de riscos	• Avaliação e Gerenciamento de Riscos • Tratamento de riscos

Tabela 9 - Evidências referentes ao processo de referência para gestão de riscos

A INTEGRA também apresenta outras evidências que podem ser consideradas:

- Planilha de levantamento de ativos de informação (Identificação de Riscos);
- Declaração de aplicabilidade de controles da ISO/IEC 27002 (Análise de Riscos);
- Planos específicos para tratamento de riscos (Tratamento de riscos).

8.5. APLICAÇÃO DO MODELO DE SUPORTE

Uma vez entendido que a INTEGRA executa os processos de referência identificados nesse trabalho para a definição de políticas e análise de risco, pode-se analisar os resultados da aplicação dos modelos de suporte.

Para cada um dos pontos de checagem de cada modelo, é apresentado a seguir uma análise frente a situação da INTEGRA. Também é apresentada uma avaliação qualitativa do tamanho da lacuna existente entre a situação proposta pelo modelo de suporte e a situação atual, seguindo o seguinte critério de classificação da Tabela 10 abaixo.

Ajuste	Critério
Baixo	A análise do SGSI da organização indica que a ação proposta pelo ponto de checagem analisado já é executada na organização. Dessa forma, podem ser observados indícios dos resultados dessa ação no sistema em seu estado atual. A organização, portanto, terá baixo ou nenhum esforço para alterar a sua abordagem devido a esse ponto de checagem.
Médio	A análise do SGSI da organização indica que a ação proposta pelo ponto de checagem analisado ainda não é executada de maneira completa na organização. Dessa forma, podem ser observados indícios parciais dos resultados dessa ação no sistema em seu estado atual. A organização, portanto, terá de realizar um esforço mediano para alterar a sua abordagem devido a esse ponto de checagem.
Alto	A análise do SGSI da organização indica que a ação proposta pelo ponto de checagem analisado ainda não é executada na organização. Dessa forma, não podem ser encontrados indícios dos resultados dessa ação no sistema em seu estado atual. A organização, portanto, terá de realizar um grande esforço para alterar a sua abordagem devido a esse ponto de checagem.

Tabela 10 - Critérios para avaliação dos pontos de checagem frente ao SGSI da INTEGRA

8.5.1. DEFINIÇÃO DE POLÍTICAS DE SEGURANÇA

A Tabela 11 a seguir apresenta uma análise da situação da INTEGRA frente aos pontos de checagem do modelo de suporte para definição de políticas de segurança, apresentado na seção 7.1.2. As conclusões da análise foram feitas com base no conteúdo dos documentos mencionados na seção 8.2.

	Ponto de checagem	Análise INTEGRA	Ajuste
PC.1	Avaliar se o foco do escopo é efetivamente a informação	O escopo atual do SGSI é completo, no entanto ainda é expresso em termos de áreas e equipes da INTEGRA. Isso faz com que a mesma informação, quando utilizada por áreas diferentes, tenham níveis de riscos associados diferentes.	Médio
PC.2	Avaliar se existe inserção da segurança nas atividades diárias	Os sistemas de gestão da qualidade e de serviços estão incorporados ao dia a dia da empresa, uma vez que os controles desses sistemas trazem maior visibilidade sobre os processos operacionais. No entanto, o sistema de gestão de segurança ainda é tratado como um módulo a parte a ser mantido. Essa situação dificulta a alteração de cultura proposta pelo modelo de suporte.	Alto
PC.3	Avaliar os incentivos à obediência aos controles	Não existe histórico de desrespeito consciente a controles de segurança. No entanto, incidentes de não são reconhecidos, e, portanto não são identificados e reportados.	Médio
PC.4	Avaliar a abstração das mídias usadas para guardar a informação	Muitos dos ativos de informação reconhecidos pela empresa ainda são associados a mídias físicas e equipamentos onde estão armazenados. A política não procura mudar essa mentalidade através da abstração da mídia física utilizada para armazenar a informação.	Alto
PC.5	(Modelo de suporte específico para gestão de riscos)	A política de segurança contempla o método de gestão de riscos. Uma análise desse método frente ao modelo de suporte pode ser encontrada na seção 8.5.2.	
PC.6	Avaliar se a conscientização de segurança é vista como um resultado	O treinamento de segurança executado para todos os funcionários trata apenas dos incidentes típicos de segurança (documentos esquecidos, senhas compartilhadas, etc.), ainda sem consideração do cenário externo. A agenda do treinamento ainda não consideram conceitos mais básicos e abstratos de segurança.	Alto
PC.7	Avaliar a customização do programa de conscientização	Apesar de executar um programa de conscientização periodicamente, esse não é customizado para cada uma das áreas de atuação dentro da empresa.	Alto
PC.8	Avaliar a distribuição da responsabilidade sobre a segurança	A política estabelece já estabelece a responsabilidade de todos os funcionários com qualquer informação da empresa.	Baixo
PC.9	Avaliar se existe a comunicação por exemplos	Foram realizados treinamentos específicos a respeito de segurança para gerentes e diretores, o que fez com que muitos executivos passassem a agir de acordo com os controles estabelecidos no SGSI.	Baixo
PC.10	Avaliar a hierarquia de políticas de segurança	A INTEGRA não possui uma hierarquia definida de políticas de segurança, mas possui diretrizes mais específicas sobre o uso seguro de alguns recursos da infraestrutura. Também não possui ainda políticas específicas sobre o uso de serviços de computação em nuvem ou mobilidade.	Alto

Tabela 11 - Análise dos pontos de checagem do modelo de suporte para definição de políticas de segurança

8.5.2. GESTÃO DE RISCO

A Tabela 12 a seguir apresenta uma análise da situação da INTEGRA frente aos pontos de checagem do modelo de suporte para gestão de risco, apresentado na seção 7.2.2. As conclusões da análise foram feitas com base no conteúdo dos documentos mencionados na seção 8.2.

	Ponto de checagem	Análise INTEGRA	Ajuste
PC.11	Avaliar quais são os escopos dos terceiros	Uma vez que o escopo da política de segurança ainda é definido com base em áreas e times, a gestão de risco com foco em informação ainda não é executada. A INTEGRA procura ter visibilidade sobre a infraestrutura do provedor interno de serviços. O mesmo não pode ser dito a respeito da infraestrutura dos provedores de nuvem.	Alto
PC.12	Avaliar a seleção de serviços considerados no escopo	Parte dos serviços dos provedores de nuvem é considerados dentro da análise de risco, assim com os serviços do provedor interno.	Baixo
PC.13	Avaliar a consideração de dispositivos dos terceiros	Os dados armazenados em dispositivos de terceiros não são reconhecidos como parte da infraestrutura da empresa ou dentro do escopo do SGSI, mesmo quando utilizados para trabalho.	Alto
PC.14	Avaliar a consideração de ambientes de trabalho remoto	A política de trabalho remoto apresenta alguns pré-requisitos referentes a infraestrutura utilizada nas residências dos profissionais. No entanto o mesmo não pode ser dito a respeito da infraestrutura em outros locais, onde o trabalho também pode ser executado. A análise de risco não considera esses ambientes.	Alto
PC.15	Avaliar a consideração de ambientes dos terceiros	Os ambientes do provedor interno e dos provedores de nuvem não são considerados dentro da análise de riscos.	Alto
PC.16	Avaliar as funcionalidades de segurança dos terceiros	As funcionalidades de segurança das soluções utilizadas pelo provedor interno são conhecidas e consideradas. O mesmo não ocorre para provedores de nuvem.	Médio
PC.17	Avaliar informações sobre infraestrutura obtidas via terceiros	O provedor interno de serviços aponta regularmente alterações em suas operações para a análise de riscos. O mesmo não ocorre para provedores de nuvem.	Médio
PC.18	Avaliar as vulnerabilidades de serviço consideradas	Algumas vulnerabilidades de serviço, como indisponibilidade causada por falhas de infraestrutura são reconhecidas no levantamento de riscos. No entanto essa análise não cobre todos os serviços utilizados pela empresa.	Médio
PC.19	Avaliar o foco dado para pessoas e processos	Poucas áreas reconhecem pessoas como ativos de informação a serem protegidos. Nenhum processo faz parte da estrutura de levantamento de ativos. Em geral apenas mídias físicas, equipamentos e ambientes são considerados como ativos de informação.	Alto

PC.20	Avaliar a experiência dos provedores de serviços	A capacidade do provedor interno de serviços do ponto de vista de segurança é reconhecida, uma vez que a equipe é capacitada pela própria empresa. Os provedores de nuvem utilizados possuem reputação sólida nos mercados que atuam, aumentando a confiança da empresa.	Baixo
PC.21	Avaliar os riscos juntamente com os provedores	O provedor interno é incluso apenas como mais uma área dentro do escopo do SGSI, mas ainda não existe a cultura de validação de riscos dos serviços prestados junto a ele. Nunca foi tentado o contato com provedores de nuvem para validação de riscos identificados.	Alto
PC.22	Avaliar o alcance dos programas de conscientização	O programa de conscientização utilizado não considera o treinamento para identificação de incidentes variados, dentro do contexto criado pelo cenário externo. Recentemente foram emitidas algumas recomendações a respeito de comportamento em redes sociais.	Alto
PC.23	Avaliar o isolamento de ambientes diferentes de trabalho	Apesar de soluções de virtualização de estação de trabalho fazerem parte da oferta da INTEGRA, a empresa não utiliza essa tecnologia internamente. Existem estudos em andamento para levantar a aplicabilidade dela para determinadas equipes e áreas.	Médio
PC.24	Avaliar a possibilidade de acesso remoto seguro	Existe a disponibilização de acesso remoto seguro para todos os seus funcionários, através de diversos tipos de dispositivos. Recentemente, foi instituído um programa para trabalho em residência.	Baixo
PC.25	Avaliar a obtenção de outras garantias além de SLAs	A grande maioria dos controles implantados para serviços de terceiros é baseado em SLAs.	Alto

Tabela 12 - Análise dos pontos de checagem do modelo de suporte para gestão de riscos

8.6. CONSIDERAÇÕES FINAIS

A INTEGRA é reconhecida no mercado como uma empresa com práticas de gestão sólidas. Como exemplos desse reconhecimento podem ser citadas as certificações de seus sistemas de gestão da qualidade (ISO 9000), serviços (ISO/IEC 20000) e segurança (ISO/IEC 27000). O SGSI estabelecido com base nessa última é um modelo de referência citado repetidamente no mercado pela sua qualidade.

Além disso, a INTEGRA é uma empresa que possui um alto grau de qualificação técnica em tecnologia. Não só vende soluções para as maiores empresas do Brasil, mas também faz o projeto dessas soluções. Somando a isso, está acostumada a fazer uso de novas tecnologias dentro da sua infraestrutura.

Finalmente, o grupo INFRA, do qual a INTEGRA faz parte, está acostumado a se adaptar a diferentes mudanças do mercado. A INTEGRA, por sua vez, já sofreu diversas adaptações internas por causa disso.

Nessa situação, poderia se imaginar que a INTEGRA seria uma das mais fortes candidatas a se adaptar rapidamente às alterações do ponto de vista de segurança causadas pelo cenário externo e apresentadas por esse trabalho. No entanto, isso não acontece, como se pode observar pela análise dos pontos de checagem do modelo de suporte, onde muitos foram classificados com ajustes necessários nos níveis “Médio” e “Alto”.

Isso porque a abordagem de segurança proposta pela ISO/IEC 27001 frente ao novo cenário requer algumas adaptações. A empresa aqui analisada, assim como muitas outras semelhantes, encontram dificuldades para adaptar essa abordagem frente a grandes modificações de cenário. No cenário externo atual, isso pode levar a falhas de proteção das informações. O modelo de suporte proposto identifica essas dificuldades e oferece às organizações uma forma de oferecer uma proteção mais adequada às suas informações.

9. CONCLUSÕES

Nesse capítulo são apresentados os principais comentários a respeito do trabalho apresentado, contribuições e desafios futuros relacionados ao tema.

9.1. ANÁLISE CRÍTICA E AVALIAÇÃO DE REQUISITOS

Ao mesmo tempo em que a gestão da segurança da informação ganhou visibilidade nos últimos anos, ela também incorporou desafios. O cenário externo sempre influenciou diretamente os esforços dos profissionais de segurança. Nos últimos anos, o surgimento de novas tendências tecnológicas como terceirização de infraestrutura de TIC, computação em nuvem e mobilidade criaram um cenário diferente. Nesse, as organizações passam a ser suportadas por uma infraestrutura muito flexível e altamente dependente de serviços de terceiros. Isso torna muito mais complexa a tarefa de manter o controle adequado da informação, exigindo mudanças profundas na abordagem de segurança da informação.

O fato de alterações serem necessárias não significa que as melhores práticas de segurança da informação, como as consideradas dentro da norma ISO/IEC 27001, devem ser descartadas. Nessa pesquisa esse padrão é utilizado para mostrar como mudanças na fase de planejamento do SGSI podem ser melhor consideradas frente a esses novos requisitos de segurança.

Para tal, esse trabalho partiu dos riscos de segurança identificados pelo mercado e relatados em artigos da área para cada uma das três tendências tecnológicas aqui consideradas. Esses riscos foram inicialmente analisados em separado, criando um entendimento mais detalhado do cenário externo e suas implicações para segurança. Os riscos foram compilados e analisados em conjunto, dando origem a uma lista de temas de preocupação típicos com segurança. Esses temas explicitam as causas mais comuns para a existência de riscos associados ao cenário externo.

Os temas foram combinados com soluções também levantadas na análise do cenário externo e resultados de pesquisas sobre mudanças de cultura de segurança em organizações e em pessoas. O resultado foram listas de pontos de checagem a

ser verificados pela organização durante a execução da fase de Planejamento da ISO/IEC 27001. Esses pontos visam trazer para mais cedo no processo de definição do SGSI problemas que tendem a ser descobertos apenas após diversas iterações do ciclo PDCA proposto pela norma.

Finalmente, os pontos de checagem foram organizados graficamente com base nos processos de referência para as atividades principais da fase de Planejamento da ISO/IEC 27001: Definição de Políticas de Segurança e Gestão de Riscos. Assim, foram definidos os modelos de suporte propostos por essa pesquisa. Ambos modelos de suporte seguem estrutura semelhante: para cada passo do processo de referência são introduzidos desvios para verificação de pontos derivados das análises.

Conforme a seção 1.3, o modelo de suporte deve estar de acordo com alguns requisitos primários e secundários. Abaixo são reapresentados os requisitos primários estabelecidos e discutidos os resultados alcançados.

Conformidade com processos de gestão de segurança existentes na ISO/IEC 27001

A própria descrição do problema para pesquisa foi feita em termos das fases do ciclo PDCA dessa norma. Assim, era de se esperar que o trabalho desenvolvido sobre esse escopo também estivesse alinhado com a norma. De fato, isso ocorre: os modelos de suporte propostos foram criados justamente para atender as atividades principais da fase de Planejamento da ISO/IEC 27001: definição da política de segurança e análise de risco.

Era possível, no entanto, que esse requisito deixa-se de ser atendido ao longo do trabalho, criando modelos que não estivessem de acordo com as práticas e conceitos propostos pela norma. Para evitar esse problema, sempre que necessário, foram buscadas referências dentro da série 27000 da ISO. Assim, por exemplo, durante o estabelecimento de processos de referência (vide a seguir) esse série foi uma fonte primária de pesquisa.

Além disso, diversos conceitos da norma são também referenciados ao longo da construção dos modelos de suporte, para sustentação das análises. Entre eles estão: revisões contínuas do ciclo PDCA, defesa da informação em si e não de meios de armazenamento e importância da definição de políticas e análise de riscos.

A importância desse requisito se mostra quando se considera a necessidade de utilização direta por praticantes de segurança. Modelos de suporte que não apresentassem conformidade com a ISO/IEC 27001 poderiam gerar dúvidas quanto ao momento ideal para consulta e assimilação das recomendações. Além disso, a conformidade com a norma também facilita a utilização em diversos contextos organizacionais.

Integração a fluxos típicos de atividades existentes na fase de Planejamento da ISO/IEC 27001

Conforme apresentado nas seções 7.1.1 e 0 a construção do modelo de suporte para cada uma das atividades da fase de Planejamento teve uma etapa inicial de identificação de um processo de referência. Essa etapa buscou quais são os fluxos típicos de trabalho executados durante cada atividade. No entanto, dado o requisito de conformidade com a ISO/IEC 27000, essa norma deveria ser um ponto de partida identificação de processos de referência.

Com relação à primeira atividade, definição de políticas de segurança, a série não apresenta um fluxo específico para essa atividade. No entanto, apresenta algumas diretrizes a respeito do conteúdo das políticas, as quais foram levadas em consideração e combinadas com outras fontes na definição do processo de referência. Já com relação à segunda atividade, gestão de riscos, um fluxo pode ser diretamente encontrado na ISO/IEC 27005. Esse fluxo foi adotado no trabalho como referência.

Os modelos de suporte se integram a esses fluxos típicos na medida em que criam desvios a cada passo do processo de referência. Esses desvios são utilizados para inserção de pontos de checagem a serem verificados antes da retomada do fluxo normal do processo. Assim, fica claro para o praticante de segurança como utilizar os modelos de suporte.

A importância desse requisito está na necessidade de resultados que possam ser efetivamente incorporados no desenvolvimento das atividades. A gestão da segurança é por si só, uma atividade complexa, já que lida com mudanças de cenário internas e externas ao mesmo tempo. A inserção de um modelo de suporte para auxiliar na assimilação de mudanças externas é válida. No entanto se o modelo exige grandes mudanças internas de processos, ele desafia o seu próprio propósito.

Permitir a organização visualizar potenciais lacunas nos resultados de seus esforços em segurança frente ao novo cenário

Os modelos de suporte propostos agem no sentido de eliminar lacunas existentes na abordagem de gestão de segurança das organizações em dois momentos.

Inicialmente, eles trazem para o primeiro plano a necessidade de dar atenção e assimilar novidades tecnológicas pró-ativamente. Com o atual cenário externo, mesmo que a organização não adote novas tecnologias rapidamente, existe a chance algum contato com elas. Sejam através de interações com parceiros, fornecedores e clientes, ou através de funcionários e colaboradores, as informações da organização podem ser armazenadas ou manipuladas utilizando infraestruturas e processos desconhecidos.

Dessa forma, a abordagem de segurança da organização precisa estar preparada para esse tipo de situação. Os modelos de suporte se baseiam fortemente nas novas tendências tecnológicas que caracterizam o cenário externo. Trazem também formas da organização se preparar para as novas possibilidades de manipulação da informação, como as descritas acima.

Em segundo lugar, os modelos de suporte ajudam a organização a identificar riscos de segurança referentes ao novo cenário mais rapidamente. Em geral, seguindo a abordagem clássica do ciclo PDCA as causas raízes para incidentes recorrentes ou semelhantes são identificadas após algumas interações do ciclo. Uma vez identificadas essas causas, são disparadas alterações de políticas e procedimentos para evitar novos incidentes.

Os pontos de checagem adiantam esse processo de análise iterativa, uma vez que eles foram já por sua vez consolidados a partir dos riscos típicos relacionados ao novo cenário. Assim, os modelos de suporte podem ajudar a organização a identificar mais rapidamente lacunas referentes a essas novas tecnologias e potencialmente lacunas referentes a variações dessas tecnologias.

Apresentar referências a práticas de segurança que possam ser utilizadas para preencher as lacunas identificadas

No detalhamento de cada um dos pontos de checagem sugeridos para os modelos de suporte nas seções 7.1.2 e 0, são apresentadas formas de lidar com os desafios do novo cenário externo. Essas práticas são resultado da pesquisa realizada sobre as novas tendências tecnológicas e problemas encontrados nas abordagens de segurança atuais.

Além das práticas apresentadas, são comentados também os objetivos ou resultados esperados da utilização das mesmas. Com isso, a organização pode melhor customizar cada uma delas para o seu contexto, desde que consiga atingir o objetivo esperado.

Dado o método utilizado para construção dos modelos de suporte, é provável também que situações de risco novas que venham aparecer no futuro já tenham sido consideradas dentro de algum ponto de checagem. Dessa forma, pode-se dizer que os modelos propostos podem funcionar de maneira preventiva para novos riscos relacionados a novas tecnologias ou variações das tendências tecnológicas consideradas.

A Tabela 13 apresenta os requisitos secundários estabelecidos e avaliação frente aos resultados alcançados.

Objetivo secundário	Avaliação do modelo de suporte
Apresentar abordagem específica para definição de políticas de segurança	Foi criado um modelo específico para a definição de políticas de segurança, visto a importância dessa atividade para o SGSI.
Apresentar abordagem específica para a gestão de riscos	Foi criado um modelo específico para a gestão de riscos, visto a importância dessa atividade para o SGSI e a necessidade de manter a coerência com as políticas de segurança definidas.
Considerar as principais tendências tecnológicas do cenário externo	O modelo considera as três tendências tecnológicas principais identificadas para o cenário – terceirização de infraestrutura de TIC, computação em nuvem e mobilidade.

Considerar riscos específicos de cada tendência tecnológica do cenário externo	Para cada uma das tendências o modelo levou em consideração riscos identificados pelo mercado e relatados em estudos e artigos relacionados.
Considerar riscos existentes do uso combinado das tecnologias disponíveis no cenário externo	Além de uma análise em separado, o modelo leva em consideração uma análise consolidadas dos riscos apresentados.
Apresentar simples utilização por praticantes de segurança	O modelo apresenta um formato de fácil utilização, utilizando pontos de checagem que devem ser verificados a cada passo do Planejamento do SGSI.
Promover a mudança de foco de segurança de aspectos tecnológicos para aspectos de pessoas e processos	O modelo de suporte apresentado inclui diversos pontos de checagem focados em conscientização de equipes
Promover a aproximação dos conceitos de “Informação” e “Segurança da Informação”	O modelo de suporte busca em todos os seus pontos de checagem o foco da organização na segurança da informação
Considerar as resistências de pessoas com relação a controles de segurança	Os pontos de checagem propostos no modelo buscam promover a obediência aos controles através de conscientização dos colaboradores e exemplos da direção
Considerar a crescente fusão de ambientes profissionais e pessoais	O modelo apresenta pontos de checagem voltados tanto dispositivos como ambientes de terceiros

Tabela 13 - Avaliação do atendimento dos requisitos secundários do modelo de suporte

Considerando os dois modelos em conjunto, nota-se uma sinergia importante entre eles. O modelo de suporte a definição de políticas de segurança da informação transforma a visão típica de segurança focada em aspectos tecnológicos para uma visão mais ampla, que foca em pessoas e processos. Com isso cria uma fundação mais adequada para a utilização do modelo de suporte a gestão de riscos. Esse, por sua vez, reforça a mesma visão através de modificações bem específicas que devem ser realizadas na abordagem de análise de risco.

O modelo de suporte para definição de políticas busca a transformação organizacional através de uma alteração da cultura de segurança da informação. Essa alteração é vista por diversos estudos como essencial para o sucesso na proteção da informação nas próximas décadas. Conforme Lacey (2010) muito bem explica: “Alcançar esses objetivos requer que nós repensemos tanto a essência da gestão de segurança como a natureza do conhecimento, habilidades, e organização exigidas por esse ambiente de negócios em constante mudança. Em um mundo futuro onde cidadão estão totalmente conectados e serviços são entregues de

dentro de uma “nuvem” na Internet, a maior vantagem nas funções de segurança não será articular políticas legais e arquiteturas técnicas, mas mudar a percepção e comportamento de milhares de gestores, clientes e usuários”.

Uma vez construída essa base sólida para gestão de segurança, o modelo de suporte de gestão de riscos busca colocá-la em prática. Este apresenta de maneira mais detalhada quais devem ser os pontos principais para consideração de serviços de terceiros e a mobilidade. Através de modificações no foco da análise de risco, a organização pode criar iniciativas para dar cargo à transformação cultural que é necessária, sem deixar de lado os aspectos tecnológicos, ainda essenciais para a prática de segurança.

Outro ponto importante dos modelos é reforçar a necessidade de customização da gestão de segurança. As melhores práticas existem, mas devem ser adaptadas para melhor servir cada organização. Considerando o cenário externo descrito, essa recomendação se torna ainda mais essencial. Se no passado gestores de segurança utilizavam políticas de segurança copiadas da Internet e listas de ameaças e vulnerabilidades pré-definidas, agora eles deverão reunir profissionais capacitados dentro da organização para desenvolver uma abordagem customizada para o seu contexto.

O cenário externo pede uma evolução da abordagem de gestão de segurança. Esta envolve deixar de lado a dependência existente em soluções tecnológicas para criar equipes e processos capazes de lidar com segurança da informação ao participarem desse novo cenário. Conclui-se que as modificações propostas nesse trabalho para a abordagem típica de gestão de segurança da informação constituem um passo importante nesse caminho.

9.2. CONTRIBUIÇÕES

Alterações na abordagem de segurança são essenciais para continuar garantindo níveis aceitáveis de proteção da informação frente ao novo cenário tecnológico. Esse trabalho incorpora diversas visões sobre gestão de segurança na forma de um modelo de suporte que visa à adaptação de uma abordagem típica para gestão de segurança. No caso, a abordagem utilizada para a fase de Planejamento do SGSI proposto pela ISO/IEC 27001.

A contribuição principal desse trabalho para a área de gestão de segurança é o modelo de suporte propriamente dito. Conforme apresentado na seção 2.3, alguns modelos de suporte para a implantação do SGSI já foram criados. No entanto, o aqui introduzido apresenta o diferencial de ser focado na fase de Planejamento do ciclo PDCA. Conforme apresentado, essa é uma das fases que mais gera dúvidas durante a criação de um SGSI, uma vez que envolve resultados pouco palpáveis, como a definição de políticas e gestão de riscos. A existência de um modelo de suporte para praticantes de segurança nessas condições é bem vinda, na medida em que permite uma pré-avaliação dos resultados de cada atividade.

Para as demais fases do ciclo PDCA – em especial a de Execução – as organizações possuem outras fontes de referência, muitas delas disponíveis na própria série 27000 da ISO. Além disso, uma vez definidos os riscos e controles a serem implantados durante o Planejamento, existe uma variedade grande de fornecedores e soluções disponíveis. Essas soluções estão ficando cada vez mais completas, oferecendo funcionalidades de monitoração e sugestão de correções, importantes para as fases de Checagem e Atuação.

Uma segunda contribuição importante é a definição de um modelo de suporte direcionado a um cenário tecnológico específico, que afeta cada vez mais organizações. No caso, estamos falando daquele caracterizado pelo uso intenso de terceirização de infraestrutura de TIC, computação em nuvem e mobilidade. Nesse contexto, o baixo nível de controle sobre as informações exige uma diferenciação do modo de lidar com gestão de segurança. O modelo de suporte oferece diretrizes para abordar esse problema aos responsáveis por essa atividade. Mais do que isso cria um modelo de comportamento a ser seguido para organizações que se encontrarão em situações semelhantes.

Além dessas contribuições principais, a pesquisa conduzida traz também contribuições secundárias. Primeiramente, é importante destacar a consideração em conjunto de diversas tendências tecnológicas para análise de segurança, o que até então não foi observado na literatura. No levantamento realizado, nenhum trabalho havia ainda analisado as tendências de terceirização de infraestrutura de TIC, computação em nuvem e mobilidade dentro de um contexto unificado. Em geral reconhece-se que essas tendências fazem parte de um cenário, mas as análises são sempre direcionadas a uma ou outra.

Deve-se notar que o enfoque independente é importante, pois permite maior profundidade nas análises de riscos em cada tecnologia. No entanto, omite o quanto essas tendências estão relacionadas e quais são as raízes comuns existentes para os riscos identificados. Além disso, a análise das tecnologias em separado tende a levar a soluções bem específicas, essencialmente focadas em tecnologia. A abordagem em conjunto leva a identificação de problemas mais intrínsecos aos processos de gestão de segurança. Nesse trabalho a análise em conjunto resultou na lista de temas de segurança apresentada na seção 5.4, que foi fundamental para a definição dos pontos de checagem introduzidos no modelo de suporte.

Outra contribuição secundária do trabalho é a introdução de um método que poderá ser utilizado futuramente para adaptação de abordagens de segurança a cenários tecnológicos. Dada a constante evolução tecnológica, é bem possível que no futuro sejam encontrados contextos semelhantes que exijam abordagem semelhante. O método aqui proposto apresenta um caminho para adaptar rapidamente políticas e gestão de risco à nova situação externa.

É bem provável que o mesmo método possa também ser adaptado a outros padrões de gestão de segurança da informação, diferentes da ISO/IEC 27001. Conforme observado por TSOHOU, KOKOLAKIS, *et al.* (2010), boa parte dos modelos existentes possuem fases ou blocos de atividades que se relacionam com a as fases do ciclo PDCA da ISO/IEC 27001. Sendo assim, a criação de um versão generalizada do modelo de suporte aqui proposto exigiria, em um primeiro momento, a identificação de onde estão as atividades da fase de Planejamento dentro desses outros modelos. Em um segundo momento, os mesmos pontos de checagem aqui apresentados poderiam ser utilizados nessas atividades.

Logicamente não faz sentido utilizar modelos de suporte para todo tipo de situação – no caso desse trabalho foi identificado um cenário altamente disruptivo,

que exigia esse tipo de solução. As práticas típicas de gestão de segurança já cobrem a maior parte das situações do dia a dia, envolvendo inclusive novos riscos do cenário externo. Além disso, a validade de um modelo de suporte generalista não sobrepõe a contextualização e customização de abordagens de segurança para uma organização específica.

Também como contribuição está a sugestão de um processo de referência para definição de políticas de segurança com base nas diretrizes obtidas a partir da série 27000 da ISO. Esse processo contempla o fluxo de trabalho e conteúdo crítico que deve constar nesse documento.

Finalmente, como contribuição final está o reconhecimento que não existe mais espaço no mundo de segurança para abordagens reativas. E esse conceito não é restrito a apenas soluções tecnológicas: deve ser válido também para processos e pessoas. A ideia de pró-atividade para gestão de segurança se materializa no modelo de suporte na consolidação dos riscos identificados para o cenário nos temas de segurança. Esses temas procuram não só preparar a organização para os riscos já existentes, mas também para eventuais riscos futuros que possam surgir. Isso é possível na medida em que os temas de segurança refletem causas comuns para diferentes tipos de riscos.

Uma vez que as organizações estão cada vez mais dependentes de serviços e mobilidade, é necessário que processos sejam concebidos pensando em segurança da informação e as pessoas estejam preparadas para agir de acordo. A gestão da segurança deve deixar de ser tratada como uma funcionalidade a mais, tornando-se mais natural no dia a dia das organizações.

9.3. TRABALHOS FUTUROS

O trabalho possui algumas limitações que podem ser investigadas em trabalhos futuros.

A fase de Planejamento da ISO/IEC 27001 é uma das mais críticas para a criação do SGSI e, portanto é o foco dos modelos de suporte propostos. No entanto, é possível que exista o interesse no desenvolvimento de modelos semelhantes para as demais fases. Provavelmente modelos de suporte para as fases de Implantação, Checagem e Atuação teriam formatos bem diferentes dos aqui desenvolvidos, visto que as atividades dessas etapas são diferentes das demais e elas tendem a ser bem mais extensas que o Planejamento. Organizações focadas no desenvolvimento de um SGSI precisam de todo o suporte que lhes for oferecido.

A segunda limitação do trabalho diz respeito à caracterização do cenário externo analisado. O trabalho aqui apresentado considerou o risco de três tendências principais envolvidas nesse cenário: terceirização de infraestrutura de TIC, computação em nuvem e mobilidade. No entanto, é de se esperar que outras tendências, menos evidentes, mas vinculadas a essas principais existam, cada qual com os seus respectivos riscos e, portanto, necessidade de consideração na gestão de segurança. Entre elas, podemos citar a fusão dos ambientes profissional e pessoal, a utilização de redes sociais e o início da inserção de novos tipos de dispositivos no dia a dia que estão conectados a rede (TVs, aparelhos de som, sinalização digital, etc.). Quanto mais completa for a visão do cenário externo, melhor será o levantamento de requisitos necessários para a gestão de segurança da informação.

Finalmente, o trabalho não considerou a execução de testes quantitativos para a determinação da eficácia do modelo de suporte proposto. A pesquisa aqui desenvolvida buscou criar um caminho para a verificação da eficácia do modelo, com base em critérios pré-definidos e modelos da literatura. Qualquer pesquisa nessa área, da mesma maneira que o modelo de suporte proposto, deve buscar a integração com a ISO/IEC 27001. Isso porque a norma apresenta recomendações de como medir a eficácia dos controles implantados no SGSI. Assim, seria interessante utilizar esses parâmetros para avaliar os resultados de um ciclo do processo sem a utilização do modelo de suporte e com sua utilização.

10. REFERÊNCIAS

ABBAS, H. et al. Addressing dynamic issues in information security management. **Information Management & Computer Security**, 19, n. 1, 2011. 5-24.

ALBRECHTSEN, E. A qualitative study of user's view on information security. **Computers & Security**, p. 276-289, 2007.

AMOROSI, D. Time to avoid the Droid? **InfoSecurity**, p. 6-9, 2011.

ANDERSON, J. A.; RACHAMADUGU, V. **Information Security Guidance for Enterprise Transformation**. Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC`06). [S.l.]: [s.n.]. 2006.

ARCE, Í.; LEVY, E. The Weakest Link Revisited. **IEEE Security & Privacy**, 2003.

BACIK, S. **Building an Effective Information Security Policy Architecture**. [S.l.]: CRC Press, 2008.

BASKERVILLE, R.; DULIPOVICI, A. The theorical foundations of knowledge management. **Knowledge Management Research & Practice**, 2006.

BELLONE, J.; DE BASQUIAT, S.; RODRIGUEZ, J. Reaching escape velocity - A practiced approach to information security management system implementation. **Information Management & Computer Security**, 16, 2008. 49-57.

BELSIS, P.; KOKOLAKIS, S. Information systems security from a knownledge management perspective. **Information Management & Computer Security**, 2005.

BISHOP, M. **Computer Security:** Art & Science. [S.l.]: Addison-Wesley, 2003.

BOEHMER, W. **Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001**. The Second International Conference on Emerging Security Information, System and Technologies (SECURWARE 2008). Cap Esterel, France: IEEE Computer Society. 2008. p. 224-231.

CHIA, P. A.; MAYNARD, S. B.; RUIGHAVER, A. B. **Understanding Organizational Security Culture**. Sixth Pacific Asia Conference on Information Systems (PACIS2002). Tokyo: [s.n.]. 2002.

CORRISS, L. **Information Security Governance:** Integrating Security into the Organizational Culture. Workshop on Governance of Technology Information, and Policies. [S.l.]: [s.n.]. 2010.

CPNI. **Information Security Briefing 01/2010 - Cloud Computing**. Centre for Protection of National Infastructure. [S.l.]. 2010.

CSA. **Security Guidance for Critical Areas of Focus in Cloud Computing V2.1**. Cloud Security Alliance. [S.l.]. 2009.

DOHERTY, N. F.; FULFORD, H. Aligning the information security policy with the strategic information systems plan. **Computers & Security**, 2006.

DOOMUM, M. R. Multi-level information system security in outsourcing domain. **Business Process Management Journal**, 2008. 849-857.

FURNELL, S. Why users cannot use security. **Computers & Security**, 2005.

GARTNER. Gartner Identifies the Top 10 Strategic Technologies for 2011. **Gartner Newsroom**, 19 Outubro 2010. Disponivel em: <http://www.gartner.com/it/page.jsp?id=1454221>. Acesso em: 05 Janeiro 2013.

GARTNER. Gartner Identifies the Top 10 Strategic Technologies for 2012. **Gartner Newsroom**, 08 out. 2011. Disponivel em: <http://www.gartner.com/it/page.jsp?id=1826214>. Acesso em: 05 jan. 2013.

GARTNER. Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond. **Gartner**, 01 dez. 2011. Disponivel em: <http://www.gartner.com/it/page.jsp?id=1862714>. Acesso em: 16 jun. 2012.

GARTNER. Gartner Identifies the Top 10 Strategic Technology Trends for 2013. **Gartner Newsroom**, 23 Outubro 2012. Disponivel em: <http://www.gartner.com/it/page.jsp?id=2209615>. Acesso em: 05 jan. 2013.

GARTNER. Top Security Trends and Take-Aways for 2013. **Gartner Insight**, 03 Janeiro 2013. Disponivel em: <http://www.gartner.com>. Acesso em: 05 Janeiro 2013.

GERBER, M.; VON SOLMS, R. Management of risk in the information age. **Computers & Security**, 2005. 16-30.

GILLIES, A. Improving the quality of information security management systems with ISO27001. **The TQM Journal**, 2011. 367-376.

GOODE, A. Managing mobile security: How are we doing?, p. 12-15, 2010.

HERLEY, C. **So Long, And No Thanks for the Externalities:** The Rational Rejection of Security Advice by Users. NSPW. [S.l.]: [s.n.]. 2009.

IDC. IDC Top10 Predictions. **IDC Predictions 2012:** Competing for 2020, Dezembro 2011. Disponivel em: <http://cdn.idc.com/research/Predictions12/Main/downloads/IDCTOP10Predictions2012.pdf>. Acesso em: 05 jan. 2013.

IDC. IDC Top10 Predictions. **IDC Predictions 2013:** Competing on the 3rd Platform, November 2012. Disponivel em: <http://www.idc.com/research/Predictions13/downloadable/238044.pdf>. Acesso em: 05 jan. 2013.

IRIC. Certificate Register. **International Register of ISMS Certificates**, 04 fev. 2013. Disponivel em: <http://www.iso27001certificates.com>. Acesso em: 04 fev. 2013.

ISO/IEC 27001. **ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements**. [S.l.]: [s.n.], 2005.

ISO/IEC 27002. **ISO/IEC 27002 - Information technology - Security techniques - Code of practice for the information security management**. [S.l.]: [s.n.], 2005.

ISO/IEC 27005. ISO/IEC 27005 - Information Technology - Security Techniques - Information Security Risk Management, 2011.

ISO/IEC TR 13335-3. **ISO/IEC TR 13335-3 - Information Technology - Guidelines for the management of IT Security - Part 3 - Techniques for the management of IT Security**. [S.l.]: [s.n.], 1998.

JAKOUBI, S. et al. **A Formal Approach Towards Risk-Aware Service Level Analysis and Planning**. 2010 International Conference on Availability, Reliability and Security. [S.l.]: [s.n.]. 2010. p. 180-187.

JENNEX, M.; ZYNGLER, S. Security as a contributor to knowledge management sucess, 2007.

KHANMOHAMMADI, K. **Business Process-based Information Security Risk Assessment**. 2010 Fourth International Conference on Network and System Security. [S.l.]: [s.n.]. 2010. p. 199-206.

KHIDZIR, N. Z.; MOHAMED, A.; ARSHAD, N. H. H. **Information Security Risk Management - An Empirical Study on the Difficulties and Practices in ICT Outsourcing**. 2010 Second International Conference on Network Applications, Protocols and Services. [S.l.]: [s.n.]. 2010. p. 234-239.

KNAPP, K. J. et al. Information security: management's effect on culture and policy. **Information Management & Computer Security**, p. 24-36, 2006.

LACEY, D. Understanding and transforming organizational security culture. **Information Management & Computer Security**, 2010. 4-13.

LEAVITT, N. Mobile Security: Finally a Serious Problem. **IEEE Computer Society**, p. 11-14, 2011.

MA, W.-M. **Study on Architecture-Oriented Information Security Risk Assessment Model**. ICCCI 2010. [S.l.]: [s.n.]. 2010. p. 218-226.

MILICEVIC, D.; GOEKEN, M. **Application of Models in Information Security Management**. 2011 Fifth International Conference on Research Challenges in Information Science (RCIS). Gosier, France: [s.n.]. 2011. p. 1-6.

MITNICK, K. **The art of deception - Controlling the Human Element of Security**. [S.l.]: Wiley Publishing, 2002.

MÜLLER, I. et al. **Tackling the Loss of Control:** Standards-based Conjoint Management of Security Requirements for Cloud Services. 2011 IEEE 4th International Conference on Cloud Computing. [S.l.]: [s.n.]. 2011. p. 573-581.

NIST. **Guidelines on Security and Privacy in Public Cloud Computing**. [S.l.]. 2011.

NIST. **The NIST Definition of Cloud Computing**. National Institute for Standards and Technology. [S.l.]. 2011.

NONAKA, I. A Dynamic Theory of Organizational Knowledge Creation. **Organization Science**, 1994.

NONAKA, I.; TOYAMA, R. The knowledge-creating theory revisited: knowledge creation as a sysnthesizing process. **Knowledge Management Research & Practice**, 2003.

RANDEREE, E. Knowledge management: securing the future. **Journal of Knowledge Management**, 10, n. 4, 2008. 145-156.

RAO, H. R.; HERATH, T. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. **Decision Support Systems**, 2009.

SCHNJAKIN, M.; ALNEMR, R.; MEINEL, C. **Contract-based Cloud Architecture**. CloudDB'10. [S.l.]: [s.n.]. 2010. p. 33-40.

SHARIATI, M.; BAHMANI, F.; SHAMS, F. **Enterprise information security, a review of architectures and frameworks from interoperability perspective**. WCIT 2010. [S.l.]: [s.n.]. 2010. p. 53-543.

SIPONEN, M. T.; OINAS-KUKKONEN, H. A Review of Information Security Issues and Respective Research Contributions. **ACM SIGMIS Database**, 2007.

SIPONEN, M.; WILLISON, R. Information security management standards: Problems and solutions. **Information & Management**, 2009. 267-270.

SPARROW, B.; LIU, J.; WEGNER, D. M. Google Effects on Memory: Cognitive Consequences of Having Information ar Our Fingertips. **Science Magazine**, p. 776-778, 2011.

STANTON, J. M. et al. Analysis of end user security behaviors. **Computers & Security**, 2005.

THORNGREN, B. et al. **Seamless mobility:** more than it seems. 2003 Mobility Roundtable. [S.l.]: [s.n.]. 2004.

TSOHOU, A. et al. A security standards` framework to facilitate best practice` awareness and conformity. **Information Management & Computer Security**, 2010. 350-365.

VAN CLEEFF, A. **A Risk Management Process for Consumers:** The Next Step in Information Security. NSPW'10. [S.l.]: [s.n.]. 2010. p. 107-114.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. **Computers & Security**, 2004. 371-376.

ZAVARSKY, S. O. et al. **Managing Risk of IT Security Outsourcing in the Decision-Making Stage**. 2009 International Conference on Computational Science and Engineering. [S.l.]: [s.n.]. 2009. p. 456-461.

ZHANG, X. et al. **Information Security Risk Management Framework for the Cloud Computing Environments**. 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010). [S.l.]: [s.n.]. 2010. p. 1328-1334.

11. ANEXOS

11.1. ANEXO A – RISCOS – TERCEIRIZAÇÃO DE INFRAESTRUTURA DE TIC

ID	DESCRIÇÃO DO RISCO	REFERÊNCIA	CLASSIFICAÇÃO	TEMA VINCULADO
RT.1	Risco de não conformidade com legislação aplicável	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.6]**
RT.2	Risco de não conformidade com requisitos de segurança internos e controles internos	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.6]**
RT.3	Risco de não compatibilização com políticas de segurança internas	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.6]**
RT.4	Risco de não atendimento aos níveis de criticidade do serviço contratado para a empresa	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.1]**
RT.5	Risco de níveis diferentes de tolerância ao risco e de avaliação de riscos	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.4]**
RT.6	Risco de não mapeamento do impacto da terceirização de um serviço em processos das várias equipes da empresa	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.4]**
RT.7	Risco de não aprendizado com situações passadas ou incorporação de melhorias no dia a dia	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.4]**
RT.8	Risco de depósito demasiado de confiança no terceiro para a execução dos serviços	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.5]**
RT.9	Risco de falhas no cumprimento de níveis de serviço acordados	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.1]**
RT.10	Risco de entendimento incorreto de benefícios e oportunidades existentes na terceirização	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.5]**
RT.11	Risco de não entendimento adequado da entrega a ser realizada pelo terceiro	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.1]**

RT.12	Risco de falhas de visão durante a escolha do provedor do serviço	(ZAVARSKY, RUHL, *et al.*, 2009)	Processos	**[T.5]**
RT.13	Risco de não existência de respeito adequado a leis de propriedade intelectual e privacidade pelo terceiro	(DOOMUM, 2008)	Processos	**[T.6]**
RT.14	Risco de não utilização de padrões adequados de segurança, benchmarks globais, auditorias regulares e revisões do nível de segurança	(DOOMUM, 2008)	Processos	**[T.6]**
RT.15	Risco de diferenças de objetivos entre provedores de serviços e organização	(KHIDZIR, MOHAMED e ARSHAD, 2010)	Processos	**[T.4]**
RT.16	Risco de falhas de comunicação sobre o status do plano de ação definido entre provedores de serviços e organização	(KHIDZIR, MOHAMED e ARSHAD, 2010)	Processos	**[T.4]**
RT.17	Risco de número limitado de profissionais para analisar os dados sobre o plano de ação e tomar ações, de acordo com as diretrizes organizacionais	(KHIDZIR, MOHAMED e ARSHAD, 2010)	Processos	**[T.2]**
RT.18	Risco de dificuldade de implementação devido a falta de conhecimento sobre análise de riscos do provedor e da organização	(KHIDZIR, MOHAMED e ARSHAD, 2010)	Processos	**[T.4]**
RT.19	Risco de baixo nível de monitoração da infraestrutura, resposta a incidentes e planos de recuperação de desastres	(DOOMUM, 2008)	Processos	**[T.4]**
RT.20	Risco de ameaças internas como o acesso indevido a dados, divulgação de dados confidenciais e pouco treinamento em conscientização e segurança	(DOOMUM, 2008)	Pessoas	**[T.8]**
RT.21	Risco de não utilização ou utilização inadequada de soluções de segurança na infraestrutura disponibilizada para os clientes	(DOOMUM, 2008)	Tecnologia	**[T.3]**
RT.22	Risco de não existência de recursos de segurança física como câmeras, sistemas de controle de incêndio e acordos de nível de serviço e segurança	(DOOMUM, 2008)	Tecnologia	**[T.5]**

11.2. ANEXO B – RISCOS – COMPUTAÇÃO EM NUVEM

ID	DESCRIÇÃO DO RISCO	REFERÊNCIA	CLASSIFICAÇÃO	TEMA VINCULADO
RC.1	Risco de incompatibilidade das aplicações utilizadas na nuvem, dificultando a recuperação ou replicação de dados armazenados para outros locais	(CPNI, 2010)	Processos	**[T.7]**
RC.2	Risco de proibição da execução de testes no ambiente devido a potenciais impactos na operação de outros clientes devido ao ambiente compartilhado	(CPNI, 2010)	Processos	**[T.4]**
RC.3	Risco de falta de controle sobre o planejamento de capacidade do provedor, causando sobrecarga em infraestruturas devido aos diversos clientes	(CPNI, 2010)	Processos	**[T.1]**
RC.4	Risco de falta de visibilidade sobre o processo de remoção, resultando em dados deletados ainda armazenados em servidores do provedor	(CPNI, 2010)	Processos	**[T.8]**
RC.5	Risco de não seguimento das melhores práticas de segurança sobre autenticação uma vez que as credenciais são mantidas por terceiros	(CPNI, 2010)	Processos	**[T.6]**
RC.6	Risco de não conformidades devido a impossibilidade de execução de auditorias nos provedores de nuvem.	(CPNI, 2010)	Processos	**[T.4]**
RC.7	Risco de não conformidade devido a complexidade regulatória introduzida pela utilização de serviços de nuvem	(CPNI, 2010)	Processos	**[T.6]**
RC.8	Risco de não conformidades em certificações já existentes devido ao fato de que elas precisariam ser revisadas para inclusão do ambiente na nuvem	(CPNI, 2010)	Processos	**[T.6]**
RC.9	Risco de corrupção de dados devido a inabilidade de execução de testes periódicos nos ambientes compartilhados	(CPNI, 2010)	Processos	**[T.2]**
RC.10	Risco de corrupção de dados devido a falta de monitoração dos dados armazenados na nuvem para modificações indevidas	(CPNI, 2010)	Processos	**[T.8]**
RC.11	Risco de complexidade regulatória causada pela utilização de ambientes com múltiplicas jurisdições, típicas dos provedores de nuvem	(CPNI, 2010)	Processos	**[T.6]**

RC.12	Risco de falhas gerais de segurança devido ao uso de esquemas de controle de ativos utilizados pelos provedores de nuvem serem diferentes dos da empresa	(CPNI, 2010)	Processos	**[T.4]**
RC.13	Risco de problemas ao tentar estabelecer um sistema de gestão de segurança da informação que inclua o provedor de nuvem de maneira adequada	(CPNI, 2010)	Processos	**[T.4]**
RC.14	Risco de falhas típicas do processo de contratação de fornecedores causando problemas de segurança ao contratar serviços na nuvem	(NIST, 2011)	Processos	**[T.5]**
RC.15	Risco de não conformidade devido a não cumprimento de leis e regulamentações públicas existentes pelo provedor de acesso	(NIST, 2011)	Processos	**[T.6]**
RC.16	Risco de falta de visibilidade sobre o local de armazenamento de dados, para garantia de conformidade	(NIST, 2011)	Processos	**[T.6]**
RC.17	Risco de lentidão para resposta quando da necessidades de resposta a solicitações de investigação quando os dados estão disponíveis na nuvem	(NIST, 2011)	Processos	**[T.2]**
RC.18	Risco de uso indevido de dados devido a dificuldade em estabelecer com precisão a propriedade sobre os dados armazenados em serviços de nuvem	(NIST, 2011)	Processos	**[T.4]**
RC.19	Risco de falta de monitoramento constante dos controles existentes na nuvem para suportar as decisões em gestão de segurança	(NIST, 2011)	Processos	**[T.8]**
RC.20	Risco de gerenciamento inapropriado de riscos devido a pouca visibilidade sobre os controles utilizados pelo provedor de serviços	(NIST, 2011)	Processos	**[T.4]**
RC.21	Risco de falhas na metodologia utilizada para resolução de incidentes detectados pelo provedor de nuvem	(NIST, 2011)	Processos	**[T.4]**
RC.22	Risco de remoção incompleta de dados após a solicitação no caso de sistemas de armazenamento compartilhados	(NIST, 2011)	Processos	**[T.8]**
RC.23	Riscos de não existência de granularidade, flexibilidade e adaptabilidade adequadas paras diferentes necessidades de acesso de clientes	(NIST, 2011)	Processos	**[T.7]**
RC.24	Risco de utilização de serviços desprotegidos de terceiros pelo provedor de nuvem para atendimento a demandas de clientes	(NIST, 2011)	Processos	**[T.8]**

RC.25	Risco de maior interesse de atacantes com relação a provedores de serviços de nuvem devido a alta concentração de alvos potenciais	(NIST, 2011)	Processos	**[T.3]**
RC.26	Risco de ingerência sobre as ameaças introduzidos pela computação em nuvem, especialmente com referência aos processos do provedor de serviços	(CSA, 2009)	Processos	**[T.3]**
RC.27	Risco de problemas legais introduzidos durante o uso de computação em nuvem, relacionados a legislações, privacidade, etc.	(CSA, 2009)	Processos	**[T.6]**
RC.28	Risco de manutenção inadequada de conformidade com políticas internas de segurança, e também com requisitos legais	(CSA, 2009)	Processos	**[T.6]**
RC.29	Risco de falta de controle sobre o gerenciamento do ciclo de vida da informação colocada na nuvem	(CSA, 2009)	Processos	**[T.8]**
RC.30	Risco de interferência em processos e procedimentos de segurança atualmente em uso na empresa e na busca por melhores modelos de risco	(CSA, 2009)	Processos	**[T.4]**
RC.31	Risco de desenho de procedimentos inadequados para detecção e resposta a incidentes	(CSA, 2009)	Processos	**[T.4]**
RC.32	Risco de maior dificuldade de controle da segurança para os clientes que utilizam serviços de computação em nuvem	(NIST, 2011)	Pessoas	**[T.3]**
RC.33	Risco inerente de acesso a dados por funcionáros do provedor de nuvem	(NIST, 2011)	Pessoas	**[T.8]**
RC.34	Risco de problemas regulatórios devido a necessidade de consentimentos de responsáveis quanto a manipulação de dados armazenados na nuvem	(CPNI, 2010)	Pessoas	**[T.6]**
RC.35	Risco de falhas devido ao não estabelecimento de responsabilidades e poucas definições sobre as ações para resposta a incidentes	(CPNI, 2010)	Pessoas	**[T.4]**
RC.36	Risco de falhas dos provedores de serviços não alcançarem RTOs e RPOs internos, além do risco de potenciais paradas definitivas de serviços	(CPNI, 2010)	Tecnologia	**[T.1]**
RC.37	Risco de dificuldades de recuperação de sistemas causadas pela grande complexidade existente em ambientes virtualizados	(CPNI, 2010)	Tecnologia	**[T.3]**

RC.38	Risco de existência de pontos únicos de falhas no caminho de acesso da empresa até os provedores de computação em nuvem	(CPNI, 2010)	Tecnologia	**[T.7]**
RC.39	Risco da falta de controles granulares de acesso, permitindo o acesso não autorizado de terceiros a dados confidenciais	(CPNI, 2010)	Tecnologia	**[T.3]**
RC.40	Risco de fraca segregação entre clientes facilitando o o acesso não autorizado a dados armazenados em ambientes compartilhados	(CPNI, 2010)	Tecnologia	**[T.8]**
RC.41	Risco de acessos indesejados causados pela utilização de serviços de autenticação compartilhados configurados incorretamente	(CPNI, 2010)	Tecnologia	**[T.3]**
RC.42	Risco de uso incorreto de criptografia devido a falhas nos processos utilizados para geração, armazenamento, transmissão e uso de chaves	(CPNI, 2010)	Tecnologia	**[T.6]**
RC.43	Risco de acessos indesejados devido ao uso de serviços específicos de autenticaçao entre nuvens	(CPNI, 2010)	Tecnologia	**[T.3]**
RC.44	Risco de modificações não autorizadas devido a utilização de dados não criptografados	(CPNI, 2010)	Tecnologia	**[T.6]**
RC.45	Risco de quebras de sigilo causados pelo uso de múltiplas centrais adicionais para o armazenamento de dados	(CPNI, 2010)	Tecnologia	**[T.8]**
RC.46	Risco de ataques causados pela divulgação de vulnerabilidades em ambientes de nuvens, que podem comprometer vários sistemas ao mesmo tempo	(CPNI, 2010)	Tecnologia	**[T.3]**
RC.47	Risco de problemas na movimentação de dados de um tipo de serviço para o outro, inclusive entre provedores diferentes, devido a incompatibilidade	(CSA, 2009)	Tecnologia	**[T.8]**
RC.48	Risco de provedor de acesso não atender de maneira adequada os requisitos da organização no que diz respeito a arquitetura de data center	(CSA, 2009)	Tecnologia	**[T.5]**
RC.49	Risco de falhas de segurança de aplicações desenvolvidas ou em execução na nuvem	(CSA, 2009)	Tecnologia	**[T.3]**
RC.50	Risco de uso inadequado de criptografia ou do gerenciamento inadequado de chaves no que diz respeito a escalabilidade	(CSA, 2009)	Tecnologia	**[T.6]**

RC.51	Risco do uso inadequado de diretórios para prover acesso aos dados e recursos da nuvem	(CSA, 2009)	Tecnologia	**[T.7]**
RC.52	Risco de relacionados aos ambientes compartilhados (Multi-tenancy), isolação de máquinas virtuais, vulnerabilidades do hypervisor, etc.	(CSA, 2009)	Tecnologia	**[T.3]**
RC.53	Risco da abordagem ineficaz ou inexistente para recuperação de dados e serviços de clientes no caso de interrupção total de serviços	(NIST, 2011)	Tecnologia	**[T.1]**
RC.54	Risco de não disponibilização de dados sobre a monitoração de sistemas para reporte de incidentes	(NIST, 2011)	Tecnologia	**[T.4]**
RC.55	Risco de falhas no hypervisior representando novos pontos de vulnerabilidade para os serviços do provedor de nuvem	(NIST, 2011)	Tecnologia	**[T.3]**
RC.56	Risco de falta de proteção de equipamentos reais de rede devido ao uso de redes virtuais criadas pelos ambientes virtualizados	(NIST, 2011)	Tecnologia	**[T.3]**
RC.57	Risco de utilização indiscrimada das imagens armazenadas de máquinas virtuais, que podem conter informações sensíveis	(NIST, 2011)	Tecnologia	**[T.3]**
RC.58	Risco de utilização de mecanismo de autenticação não conhecidos ou homologados pelos provedors de computação em nuvem	(NIST, 2011)	Tecnologia	**[T.6]**
RC.59	Risco de complexidade de hypervisors utilizados pelo provedor de computação causarem dificuldades na análise de segurança	(NIST, 2011)	Tecnologia	**[T.7]**
RC.60	Risco de funcionalidades específicas existentes em ambientes virtualizados aumentarem o número de vetores de ataque disponíveis	(NIST, 2011)	Tecnologia	**[T.3]**
RC.61	Risco de incapacidade do provedor de nuvem de proteger dados armazenados em diversas situações através de criptografia	(NIST, 2011)	Tecnologia	**[T.6]**
RC.62	Risco de falhas nos serviços disponibilizados impactando a operação da empresa	(NIST, 2011)	Tecnologia	**[T.1]**
RC.63	Risco de ataques de DoS causarem interrupções dos serviços, mesmo com recursos abundantes disponíveis	(NIST, 2011)	Tecnologia	**[T.1]**

11.3. ANEXO C – RISCOS – MOBILIDADE

ID	DESCRIÇÃO DO RISCO	REFERÊNCIA	CLASSIFICAÇÃO	TEMA VINCULADO
RM.1	Risco de não conhecimento e não cumprimento das políticas de segurança para dispositivos móveis	(GOODE, 2010)	Processos	**[T.6]**
RM.2	Risco de não integração entre a estratégia de segurança móvel e estratégia geral de segurança de uma empresa	(GOODE, 2010)	Processos	**[T.9]**
RM.3	Risco de inabilidade de proteger as informações existentes nos dispositivos que são propriedade de um funcionário	(GOODE, 2010)	Processos	**[T.8]**
RM.4	Risco de acesso a sites perigosos sem restrições, devido a maior confiança depositada nos dispositivos móveis	(LEAVITT, 2011)	Pessoas	**[T.9]**
RM.5	Risco de controle de dispositivos móveis para a formação de botnets	(LEAVITT, 2011)	Tecnologia	**[T.3]**
RM.6	Risco de aplicações maliciosas serem instaladas em dispositivos móveis	(LEAVITT, 2011)	Tecnologia	**[T.3]**
RM.7	Risco de utilização de links maliciosos publicados em redes sociais, levando a contaminação do dispositivo móvel com malware	(LEAVITT, 2011)	Tecnologia	**[T.3]**
RM.8	Risco de instalação de spyware com captura de conteúdo inadequado para o usuário final	(LEAVITT, 2011)	Tecnologia	**[T.9]**
RM.9	Risco de compartilhamento de informações não autorizados através de conexões Bluetooth	(LEAVITT, 2011)	Tecnologia	**[T.8]**
RM.10	Risco de interceptação de comunicação Wi-Fi devido ao uso de pontos de acesso não protegidos	(LEAVITT, 2011)	Tecnologia	**[T.8]**
RM.11	Risco de desenvolvimento inseguro de aplicações, com a criação de exploits para as vulnerabilidades introduzidas	(GOODE, 2010)	Tecnologia	**[T.3]**
RM.12	Risco de acesso indevido a informações disponíveis na rede local devido ao uso de dispositivos móveis para a conexão	(GOODE, 2010)	Tecnologia	**[T.9]**

RM.13	Risco de acesso indevido a informações disponíveis na rede local devido ao uso de dispositivos móveis para a conexão remota	(GOODE, 2010)	Tecnologia	**[T.9]**
RM.14	Risco de implementação incorreta de mecanismos de autenticação ao utilizar o dispositivo móvel para tal	(GOODE, 2010)	Tecnologia	**[T.9]**
RM.15	Risco de contaminação de dispositivos móveis com virus	(GOODE, 2010)	Tecnologia	**[T.9]**
RM.16	Risco de não utilização de criptografia nos dados armazenados em dispositivos móveis	(GOODE, 2010)	Tecnologia	**[T.6]**
RM.17	Risco de perda de dados devido a falta de soluções de backup para o conteúdo armazenado em dispositivos móveis	(GOODE, 2010)	Tecnologia	**[T.8]**