Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

V. 12, n. 1

jan-abr 2013

doi:10.5329/RESI.2013.1201

Sumário

ISSN: 1677-3071

Revista hospedada em: http://revistas.facecla.com.br/index.php/reinfo
Forma de avaliação: *double blind review*

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente, mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

MODELO DE AVALIAÇÃO DA MATURIDADE DA SEGURANÇA DA INFORMAÇÃO

INFORMATION SECURITY MATURITY ASSESSMENT MODEL

(artigo submetido em agosto de 2011)

Evandro Alencar Rigon
Graduado em Sistemas de Informação pela Universidade Federal de Santa Catarina (UFSC)
rigon@inf.ufsc.br

Carla Merkle Westphall
Doutora em Engenharia Elétrica pela Universidade Federal de Santa Catarina (UFSC)
e Professora do Mestrado em Ciências da Computação da Universidade Federal de Santa Catarina (UFSC)
carlamw@inf.ufsc.br

ABSTRACT

Business processes are supported by information technologies, although many processes and information systems were not designed to be secure. The lack of a security evaluation method might expose organizations to several risky situations. This work presents an information security maturity management process which uses a measurement method and a set of controls which treat information security on a comprehensive way. The results indicate that the method is efficient for evaluating the current state of information security, to support information security management, risks identification, the improvement of business processes and internal control processes.

Key-words: security; maturity; risks.

RESUMO

Os processos de negócio das organizações são suportados por tecnologias da informação, apesar de muitos processos e sistemas não terem sido projetados para serem seguros. A falta de um método para avaliar a segurança pode expor a organização a riscos em diversas situações. Este artigo apresenta um processo para a gestão da maturidade da segurança da informação por meio de um método de medição e um conjunto de controles que tratam a segurança da informação de forma abrangente. Os resultados indicam que o método é eficiente para avaliar o estado atual da segurança, auxiliar no processo de gestão da segurança da informação e identificação de riscos, e apoiar a melhoria dos processos e controles internos da organização.

Palavras-chave: segurança; maturidade; riscos.

1 INTRODUÇÃO

O gerenciamento da segurança da informação exige uma visão bastante abrangente e integrada de vários domínios de conhecimento, englobando aspectos de gestão de riscos, de tecnologias da informação, de processos de negócios, de recursos humanos, da segurança física e patrimonial, de auditoria, de controle interno e também de requisitos legais e jurídicos. Uma abordagem gerencial que considera a segurança como um assunto somente de tecnologia, comum nas organizações, pode ser a raiz de muitos problemas, pois gerencia a segurança da informação dentro das estruturas de operações de Tecnologia da Informação (TI), com menos visão e controle gerencial.

A avaliação crítica e metódica dos controles relacionados à segurança da informação torna-se necessária já que tecnologias, processos de negócio e pessoas mudam, alterando constantemente o nível de risco atual e gerando novos riscos à organização (PINHEIRO e SLEIMAN, 2009).

O desafio está em definir objetivos de segurança da informação, alcançá-los, mantê-los e melhorar os controles que os suportam, para assegurar a competitividade, a lucratividade, o atendimento a requisitos legais e a manutenção da imagem da organização junto à sociedade e ao mercado financeiro. Modelos de maturidade podem ajudar a enfrentar este desafio (ACEITUNO, 2007; MARANHÃO, 2011).

Normas internacionais importantes relacionadas à segurança da informação, como ABNT (2006) e ABNT (2005), apresentam controles aplicáveis para a gestão da segurança da informação, mas não definem um método para avaliar se os controles sugeridos são adequados para a realidade da organização, levando-se em conta o nível de risco associado e o seu custo/benefício (CHAPIN e AKRIDGE, 2005; WALKER *et al.*, 2012).

A falta de um método para avaliar a adequação dos controles pode levar uma organização a adotar controles fracos, expondo-a ao risco em diversas situações. De modo inverso, pode ocorrer o desperdício de recursos em controles superdimensionados. A falta de método para avaliar a adequação dos controles pode ainda fazer com que uma organização trate os riscos e controles de segurança de acordo com iniciativas individuais que não correspondam às necessidades ou aos objetivos estratégicos da organização.

Os modelos de maturidade são baseados na melhoria de processos e na existência de fundamentos para guiar e medir a implementação e a melhoria dos processos (CHAPIN e AKRIDGE, 2005). Atualmente existem pesquisas relacionadas ao uso de modelos para medir a maturidade de Sistemas de Gestão de Segurança da Informação (CHAPIN e AKRIDGE, 2005; ACEITUNO, 2007; WOODHOUSE, 2008; PARK *et al.*, 2008; JANSSEN, 2008; CUNHA, 2008). Um modelo de governança importante como o CobiT, embora defina um modelo de maturidade, não define um modelo rigoroso de avaliação da maturidade. Os usuários do modelo de maturi-

dade CobiT precisam construir seu próprio modelo de avaliação (BREIER e HUDEC, 2012; WALKER *et al.*, 2012).

Este artigo propõe um método para a gestão da segurança da informação por meio de um processo de avaliação periódica de maturidade e da melhoria contínua dos controles. O modelo proposto é genérico e aplicável a todos os tipos de organização, independente de tamanho ou área de atuação, pelo uso dos 133 objetivos de controle de segurança da informação constantes da norma ABNT NBR ISO/IEC 27002 (ABNT, 2005). O modelo proposto faz uso de controles adequados, dependentes da análise do risco e da evolução do ambiente geral.

O texto do artigo está organizado em sete seções. A seção 2 apresenta os principais trabalhos relacionados. A seção 3 apresenta as principais normas técnicas relacionadas à segurança da informação e à gestão de riscos. A seção 4 descreve conceitos básicos sobre modelos de maturidade. A seção 5 é dedicada à especificação do modelo de avaliação da segurança da informação por meio da medição de níveis de maturidade. A seção 6 apresenta a aplicação do modelo a uma organização para verificação da sua eficácia. A última seção apresenta a conclusão.

2 TRABALHOS RELACIONADOS

No trabalho de JANSSEN (2008), o objetivo principal é propor um instrumento de avaliação da maturidade dos processos de segurança da informação para instituições hospitalares. É um estudo exploratório, de natureza qualitativa, com aplicação de questionários semiestruturados para estudo de caso em três instituições hospitalares. Como conclusão do trabalho foi destacada a aprovação do instrumento com relação à sua utilidade para avaliar a maturidade dos processos de segurança da informação naquele tipo de instituição. O trabalho desenvolvido por Janssen (2008) se assemelha a este trabalho na utilização da norma ABNT NBR ISO/IEC 27002 e no uso de um modelo de maturidade. A principal diferença é que agora é apresentado um processo de gestão para melhoria contínua da segurança, na forma de um modelo genérico aplicável a todos os tipos de organização, independentemente de tamanho ou área de atuação, por meio do uso dos 133 objetivos de controle de segurança da informação constantes da norma ABNT NBR ISO/IEC 27002. Outra diferença é que o modelo proposto por Janssen (2008) apresenta proposições específicas, estáticas, e que podem não possibilitar ao avaliador a adequada análise dos riscos, na medida em que haja evolução das tecnologias, processos de negócio e/ou requisitos externos aplicáveis.

O trabalho de Cunha (2008) teve como objetivo criar um modelo para que a alta administração da organização incorporasse requisitos de segurança da informação como parte de seu processo de governança computacional, de forma a evidenciar de maneira objetiva os riscos relacionados à informação no momento da definição do planejamento estratégico da organização. As semelhanças com o presente trabalho

estão na utilização da norma ABNT NBR ISO/IEC 27002, o modelo de governança de TI - CobiT, e avaliações de riscos. A principal diferença está no objetivo do estudo, uma vez que o foco do modelo proposto por Cunha (2008) é o alinhamento entre o planejamento estratégico da segurança da informação e o planejamento estratégico da organização, não apresentando um método para medição da situação atual da segurança e do acompanhamento e evolução da segurança e de seus processos relacionados.

Em Woodhouse (2008) existe uma proposta teórica de um modelo de maturidade de um sistema de gestão da segurança da informação (SGSI), composto por nove níveis: -3 (Subversivo), -2 (Arrogante), -1 (Obstrutivo), 0 (Negligente), 1 (Funcional), 2 (Técnico), 3 (Operacional), 4 (Gerenciado) e 5 (Estratégico). Os níveis com números negativos demonstram uma postura de desinteresse e falta de responsabilidade com a segurança da informação, considerando riscos da própria empresa e das empresas com as quais existem interações. O trabalho de Woodhouse (2008) se assemelha a este trabalho por não utilizar uma metodologia baseada em *checklists* genéricos criados com base em controles técnicos. No entanto, Woodhouse (2008) não apresenta um método para efetivamente realizar medições e apurar o nível de maturidade da segurança da informação. O artigo se limita a definir nove níveis para avaliar a maturidade de um sistema de gestão da segurança da informação com base na cultura de uma organização, e não na maturidade dos processos relacionados à segurança da informação e riscos ao negócio da organização.

Park *et al.* (2008) apresentam uma maneira de medir a maturidade de gerenciamento de serviços de tecnologia da informação e usam as práticas definidas no IT Infrastructure Library (ITIL) como fundamento. O artigo demonstra a fase de entrevista com os responsáveis, a fase de cálculos da maturidade e ainda os resultados obtidos com os cálculos. O modelo de Park *et al.* (2008), baseado nas práticas do ITIL, apresenta a limitação de avaliar a segurança sob a ótica dos processos de *suporte e entrega de serviços*, essencialmente vinculados à Tecnologia da Informação, não permitindo uma análise dos riscos à segurança da informação gerados em processos do negócio não essencialmente relacionados à TI.

3 PRINCIPAIS NORMAS TÉCNICAS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO

As principais referências normativas são as normas da “família 27000” da *International Organization for Standardization* (ISO), específicas para gestão da segurança da informação, adotadas pela Associação Brasileira de Normas Técnicas (ABNT).

ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos: é uma tradução da ISO/IEC 27001:2005 e tem como objetivo “prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI)” (ABNT, 2006).

ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: versão atualizada da ABNT NBR ISO/IEC 17799 de 2005, é o fundamento normativo da segurança da informação. O objetivo da norma é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação, por meio da definição de controles que podem ser utilizados para atender aos requisitos identificados por meio da análise/avaliação de riscos (ABNT, 2005). A norma está estruturada em 11 seções de controles de segurança da informação, divididas em 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos. São definidos 133 controles aplicáveis à segurança da informação. A norma ABNT NBR ISO/IEC 27002:2005 prevê que as organizações possam vir a utilizar controles adicionais àqueles que ela recomenda. Por esse motivo o documento deve ser utilizado com cautela, avaliando-se o que é adequado ao negócio (RAMOS, 2006). Todas as atividades de uma organização envolvem riscos, que precisam ser identificados, analisados e avaliados para estabelecer se será necessário tratamento. É justamente esta análise crítica que determina a necessidade de mudanças e a priorização destas mudanças de acordo com os requisitos a serem cumpridos pela organização.

A ABNT NBR ISO/IEC 27005, adoção idêntica à ISO/IEC 27005:2008, fornece as diretrizes para a avaliação de riscos da segurança da informação, de acordo com os conceitos definidos na ABNT NBR ISO/IEC 27001, para implementação da segurança da informação baseada na gestão de riscos (ABNT, 2008). A Figura 1 apresenta uma visão esquemática do processo de gestão de riscos da segurança da informação de acordo com a ABNT NBR ISO/IEC 27005, 2008.

4 MODELOS DE MATURIDADE DE SEGURANÇA

Um modelo de maturidade de segurança fornece um guia para um programa de segurança completo. Define, também, a ordem na qual os elementos de segurança devem ser implementados, incentiva o uso de padrões de melhores práticas e fornece um meio para comparar programas de segurança (CHAPIN e AKRIDGE, 2005).

Os níveis de maturidade são utilizados para classificar o estágio atual da organização, apresentando os objetivos de controle e os processos necessários para se atingir cada um deles (GARCIA, 2012).

Após identificar processos e controles críticos, o uso de um modelo de maturidade permite a identificação de lacunas que representem risco e sua demonstração à administração. Com base nessa análise podem ser avaliados e desenvolvidos planos de ação para melhoria dos processos e controles considerados deficientes até o nível de desenvolvimento desejado (ITGI, 2007).

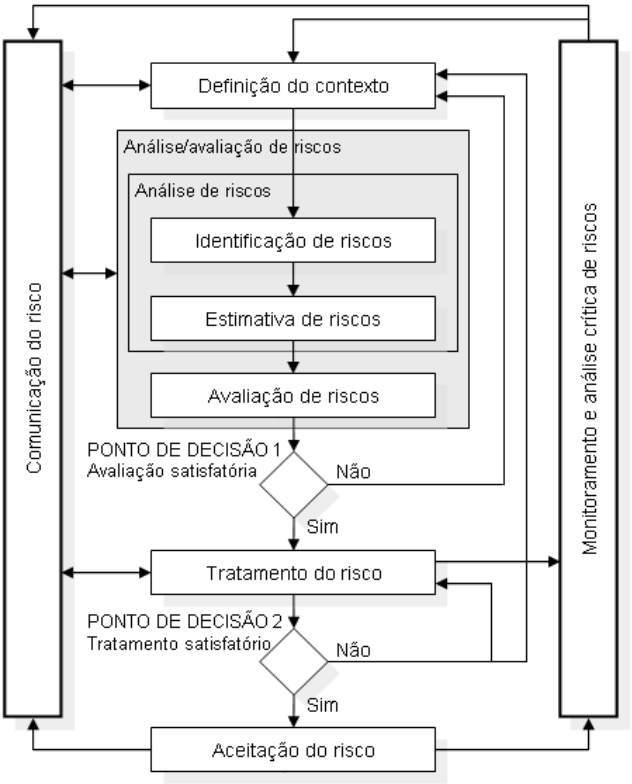

Figura 1. Processo de gestão de riscos de segurança da informação
Fonte: adaptado de ABNT (2008).

Algumas abordagens de padrões para gerenciamento da segurança da informação podem ser classificadas da seguinte forma: orientadas a processos como CobiT e ITIL; orientadas a controles como ISO 27001; orientadas a produtos como os Critérios Comuns (ISO 15408); orientadas ao gerenciamento de riscos como OCTAVE e ISO 27005 e orientadas a boas práticas como a ISO 27002. O trabalho de Aceituno (2007) define um modelo de maturidade para o gerenciamento da segurança da informação, chamado atualmente O-ISM3, compatível com a norma ISO 27001.

Os dois modelos de maturidade considerados mais importantes neste trabalho são CobiT e O-ISM3. O modelo de maturidade do CobiT é amplamente usado para governança de TI. Já o modelo O-ISM3 é um modelo recente específico para gerenciamento da segurança da informação. Karokola *et al.* (2011) descrevem outros modelos de maturidade, entretanto, como não possuem aspectos de medidas dos níveis de maturidade, não fizeram, aqui, parte de um estudo mais detalhado.

4.1 MODELO DE MATURIDADE DO COBIT

O CobiT (*Control Objectives for Information and Related Technology*) (ITGI, 2007) apresenta um conjunto de indicadores obtidos por meio do consenso de especialistas, mais focados no controle das atividades do que na sua execução, que auxiliam na otimização de investimentos em TI, garantem a entrega de serviço e providenciam uma medida para emitir julgamento e permitir a comparação.

A escala de maturidade do CobiT está representada na Figura 2. A escala de seis níveis consiste em uma escala simples de maturidade que demonstra como um processo evolui de uma capacidade não existente para uma capacidade otimizada. A escala inclui o nível 0 (zero) porque é possível que nenhum processo ou controle exista para o controle ou processo que estiver sendo avaliado.

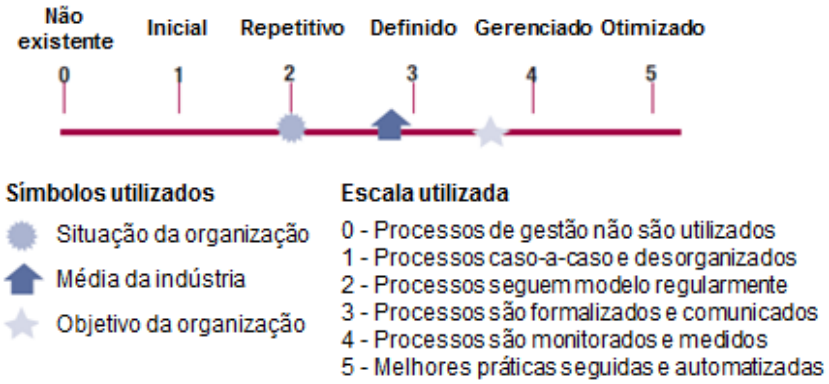

Figura 2. Representação gráfica do modelo de maturidade utilizado no CobiT
Fonte: adaptado de ITGI (2007)

O Quadro 1 apresenta a descrição da escala de maturidade da Figura 2.

Nível	Características
0 Não-existente	Completa falta de qualquer processo reconhecível. A organização ainda não reconheceu que há um risco a ser tratado.
1 Inicial	Existe uma evidência de que a organização reconheceu que riscos existem e precisam ser tratados. No entanto, não há qualquer processo padronizado; existem alguns processos aplicados caso-a-caso por iniciativas individuais.
2 Repetitivo	Processos foram desenvolvidos até o estágio em que procedimentos similares são seguidos por diferentes pessoas que realizam a mesma tarefa. Não há treinamento formal ou comunicação dos procedimentos e a responsabilidade é individual. Existe uma alta confiança no conhecimento das pessoas, sendo os erros comuns.
3 Definido	Procedimentos foram documentados, formalizados e comunicados em treinamento. É obrigatório que os procedimentos sejam seguidos; entretanto, é improvável que desvios sejam detectados. Os procedimentos não são sofisticados. Representam apenas a formalização das práticas existentes.
4 Gerenciado	A gerência monitora e mensura a conformidade com os procedimentos e toma ações quando os processos parecem não funcionar efetivamente. Processos estão sob constante melhoria e utilizam boas práticas. Ferramentas e automação são utilizadas em uma maneira limitada e fragmentada.
5 Otimizado	Os processos foram refinados ao nível de melhores práticas, baseados no resultado de melhorias contínuas e de comparação com outras organizações. A TI é utilizada de maneira integrada para automatizar fluxos de trabalho.

Quadro 1. Escala utilizada para os níveis de maturidade
Fonte: adaptado de ITGI (2007)

O CobiT não define um modelo de avaliação da maturidade rigoroso. O conteúdo descritivo se limita a definir os níveis de maturidade do processo, juntamente com características comportamentais associadas ao conjunto dos seis níveis de maturidade possíveis. Os usuários do modelo de maturidade CobiT precisam construir seu próprio modelo de avaliação conforme a granularidade dos processos que desejem avaliar (BREIER e HUDEC, 2012; WALKER *et al.*, 2012).

4.2 MODELO DE MATURIDADE DO O-ISM3

O O-ISM3 (*The Open Group Information Security Management Maturity Model*) é um modelo de maturidade para o gerenciamento da segurança da informação que tem cinco níveis: indefinido, definido, gerenciado, controlado e otimizado (THE OPEN GROUP, 2011). Este modelo é uma evolução do trabalho inicial de Aceituno (2007).

O modelo oferece aos gerentes e auditores uma abordagem para avaliar, especificar, implementar e melhorar sistemas de gerenciamento da segurança da informação. O O-ISM3 é fundamentado nas boas práticas de vários padrões como CMMI, ITIL, ISO 9000 e ISO 27001.

Entretanto, O-ISM3 não tem medidas para risco ou para a segurança de forma direta (KAROKOLA *et al.*, 2011). As métricas são baseadas em processos e devem medir atividades, escopo, eficácia, eficiência e qualidade.

5 O MODELO DE AVALIAÇÃO POR NÍVEIS DE MATURIDADE

O modelo apresentado neste artigo almeja avaliar a segurança da informação de maneira abrangente, fazendo com que o foco da segurança da informação esteja de acordo com os objetivos organizacionais. O modelo tem como principais características:

a) ser estruturado na forma de um processo de gestão que possibilite avaliação e melhoria contínuas, por meio do uso da norma ABNT NBR ISO/IEC 27001;

b) ser baseado em controles apropriados para a segurança da informação, por meio do uso da norma ABNT NBR ISO/IEC 27002;

c) fornecer meio para medir a situação atual da gestão da segurança da informação e sua evolução ao longo do tempo, por meio do uso de um modelo de maturidade; e,

d) fornecer subsídio para levar a ações de melhoria oportunas e viáveis, baseadas nos riscos, suportado pelo uso da ABNT NBR ISO/IEC 27005.

5.1 AVALIAÇÃO E MELHORIA CONTÍNUA

Como os riscos são dinâmicos, os requisitos de segurança da informação são alterados constantemente. A norma ABNT NBR ISO/IEC 27001 adota o modelo *Plan-Do-Check-Act* (PDCA) para estruturar os processos do SGSI e garantir a melhoria contínua. O uso do PDCA encoraja os usuários

administradores do SGSI a enfatizarem a importância de melhoria contínua, baseada em medições objetivas (ABNT, 2006).

Neste trabalho a abordagem de processo para a gestão da segurança da informação é baseada no ciclo PDCA de melhoria contínua e utiliza um modelo de maturidade para a mensuração do desenvolvimento dos processos e controles considerados aplicáveis à segurança da informação da organização.

5.2 CONTROLES DE SEGURANÇA DA INFORMAÇÃO

O modelo de avaliação deste artigo utiliza a estrutura de objetivos de controle da norma ABNT NBR ISO/IEC 27002. A norma define 133 controles que podem ser avaliados.

5.3 MEDIÇÃO E ACOMPANHAMENTO

O modelo de gestão da segurança da informação apresentado neste artigo tem a sua base de medição suportada na escala de maturidade do CobiT (Figura 2). A escala de maturidade utilizada neste artigo é apresentada no Quadro 1. Entretanto, neste artigo é proposto um conjunto de fases para a realização do ciclo de avaliação da maturidade.

5.4 FASES DO CICLO DE AVALIAÇÃO DA MATURIDADE E MELHORIA CONTÍNUA

Como o CobiT não define um modelo de avaliação da maturidade rigoroso e os usuários do modelo de maturidade CobiT precisam construir seu próprio modelo de avaliação (BREIER e HUDEC, 2012; WALKER *et al.*, 2012), este artigo propõe as fases do ciclo de avaliação da maturidade e melhoria da segurança da informação (Figura 3).

Uma métrica, ou indicador, por si só, não é a resposta para gerenciar os problemas de segurança da informação de uma organização. Além de se medir, deve existir ação sobre os problemas encontrados e acompanhamento da evolução ao longo do tempo. A Figura 3 apresenta as oito fases que compõem o ciclo de avaliação da maturidade proposto.

Figura 3. Proposta de ciclo de avaliação da maturidade e melhoria da segurança da informação
Fonte: elaborada pelos autores

5.4.1 Definição do escopo de avaliação

Nesta fase é definido o escopo para a avaliação do nível de maturidade da segurança da informação. Uma organização pode possuir, simultaneamente, atividades administrativas, industriais e de prestação de serviços, ou pode estar distribuída geograficamente, e considerar conveniente dividir a avaliação da maturidade da segurança em partes, respeitando as características específicas de cada uma de suas atividades, unidades ou núcleos de especialização.

A definição do escopo consiste em identificar as áreas, tecnologias e processos da organização a serem incluídos na avaliação (ABNT, 2006).

5.4.2 Análise dos riscos relacionados à segurança da informação

Nesta fase a organização realiza a identificação global dos riscos relacionados à segurança das suas informações, para garantir que os controles selecionados estejam relacionados ao tratamento dos riscos (ABNT, 2006).

A metodologia de análise pode ser quantitativa, qualitativa ou uma combinação de ambas. A estimativa qualitativa é frequentemente utilizada em primeiro lugar, para que se obtenha uma indicação geral do nível de risco e se tornem evidentes grandes riscos. Normalmente, é menos complexa e menos onerosa (ABNT, 2008).

Este modelo utiliza o método qualitativo para análise de riscos, adotando uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (impacto) e a probabilidade dessas consequências ocorrerem. Essa abordagem foi considerada suficiente para a identificação dos riscos e para suportar a decisão de escolha dos controles de segurança da informação a serem avaliados.

5.4.3 Seleção dos controles de segurança da informação

Nesta fase são selecionados os controles de segurança da informação, constantes da ABNT NBR ISO/IEC 27002, considerados aplicáveis para a cobertura dos riscos identificados na fase de análise dos riscos relacionados à segurança da informação.

Apesar de o modelo utilizar a estrutura de controles da ABNT NBR ISO/IEC 27002 como base de avaliação, as organizações devem ser capazes de identificar outros controles, considerando, por exemplo, a análise dos riscos corporativos, a gestão da conformidade, outras fontes de requisitos legais ou regulamentares aplicáveis, ou de boas práticas adotadas no setor em que a organização está inserida.

5.4.4 Planejamento da análise dos controles de segurança da informação

Nesta fase é realizado um planejamento para análise e avaliação dos objetivos de controle considerados aplicáveis e suas respectivas atividades de controle. Esta fase tem por finalidade identificar e comprometer as partes envolvidas nas análises, identificar as partes interessadas, definir

um cronograma para as atividades de avaliação do ciclo e criar um plano de comunicação para os resultados obtidos.

5.4.5 Análise e avaliação da maturidade dos controles de segurança da informação

Nesta fase o nível de maturidade de cada controle é comparado com a análise de riscos e, caso necessário, ações são propostas para correção e/ou melhoria das atividades relacionadas. Esta fase propõe cinco etapas (representadas na Figura 4):

a) Identificação dos processos e atividades relacionadas: os controles de segurança da informação são cumpridos nas atividades dos processos de negócio, operacionais (execução da tarefa) ou de controle (verificação ou aprovação da tarefa executada). Esta etapa consiste em identificar e relacionar ao controle de segurança todos os processos, procedimentos e atividades que contribuam para que seja cumprido;

b) Análise do nível de maturidade do controle: com base nos processos e atividades que suportam o controle avaliado, apurar o nível de maturidade do controle de acordo com a escala de maturidade utilizada pelo modelo. Possivelmente há atividades relacionadas ao mesmo controle com níveis de maturidade distintos;

c) Avaliação da maturidade do controle: nesta etapa é avaliado se a maturidade do controle, apurada pelo conjunto das atividades que o suportam, está de acordo com a maturidade necessária para tratar os riscos relacionados ao negócio;

d) Definição de melhorias necessárias: com base nas possíveis deficiências encontradas no cumprimento dos controles, nesta etapa são documentadas as ações e melhorias nas atividades relacionadas ao controle de segurança, ou mesmo as novas atividades criadas, para manter o risco em nível adequado. As alterações devem ser documentadas em conjunto com os responsáveis pelos processos de negócio;

e) Comunicação dos resultados aos responsáveis pelo controle: nesta etapa os resultados da análise do controle de segurança são comunicados aos responsáveis, para que tomem conhecimento e possam avaliar as ações necessárias e possíveis intervenções emergenciais.

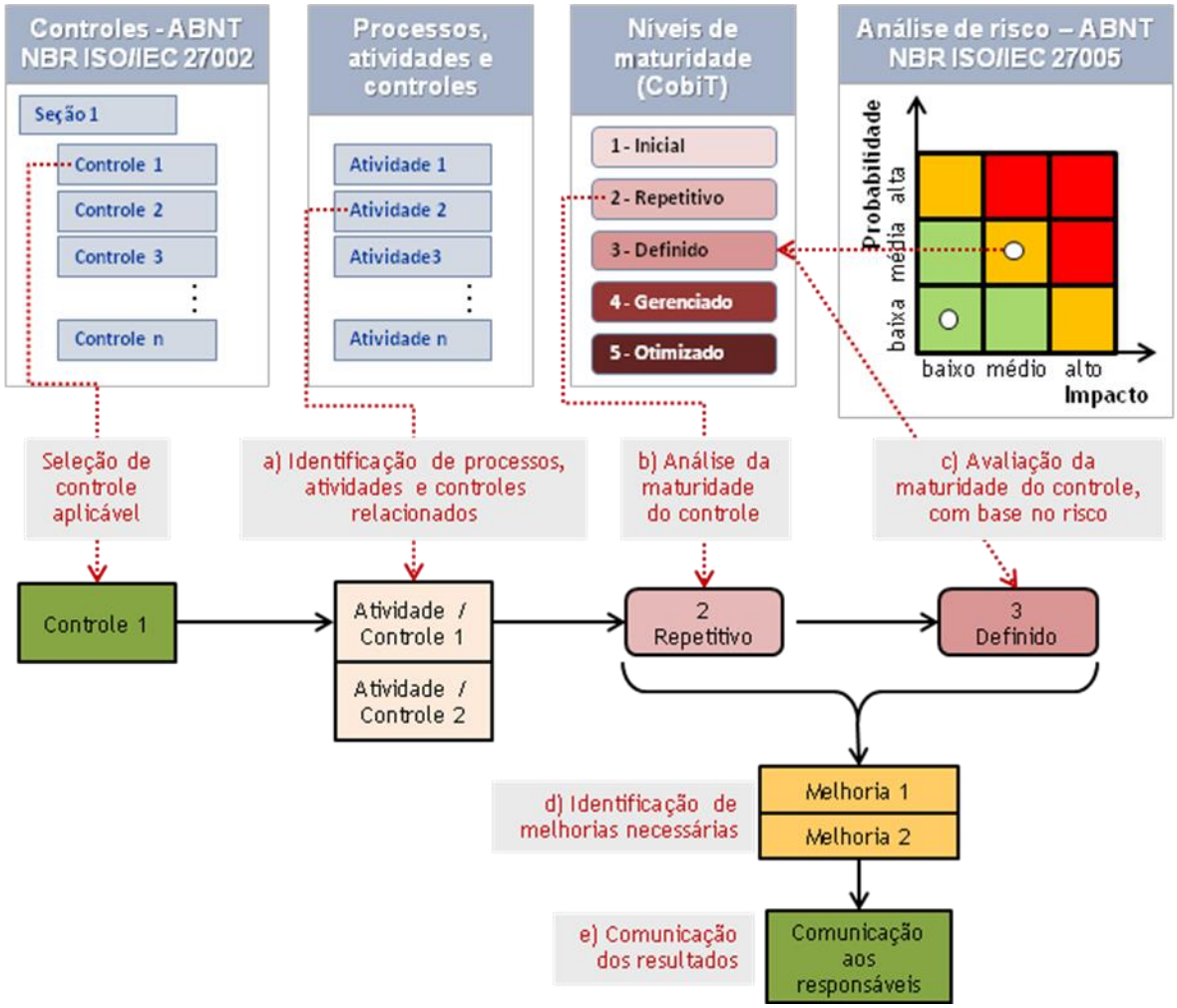

Figura 4. Proposta de etapas da avaliação da maturidade dos controles de segurança da informação
Fonte: elaborada pelos autores

5.4.6 Consolidação dos planos de ação de segurança da informação

É razoável esperar que diversos objetivos de controle possam ter planos de ação em comum, relacionados ou interdependentes. Nesta fase todas as melhorias propostas são consolidadas e organizadas de acordo com os processos e atividades de negócio aos quais estão relacionadas. Esta fase está dividida em quatro etapas:

a) Revisão e organização das melhorias identificadas: nesta etapa todas as melhorias identificadas são analisadas em conjunto, para identificação de pontos em comum e para a convergência das ações de melhoria. Esta etapa visa a criar uma visão integrada de todas as ações de melhoria julgadas necessárias para diminuir o esforço de implementação por meio da colaboração entre as áreas envolvidas, visto que mudanças similares podem ser identificadas e propostas em diferentes controles;

b) Definição do responsável pela execução: esta etapa tem a finalidade de indicar, para cada plano de ação proposto, um responsável pela sua execução e acompanhamento;

c) Aprovação dos planos de ação: nesta etapa os planos de ação devem ser aprovados. Também ocorre a priorização dos planos e a definição da data de início da execução;

d) Comunicação dos planos de ação: nesta etapa os planos de ação são comunicados aos responsáveis, de maneira a torná-los conscientes dos trabalhos a serem realizados.

A organização deve "atualizar os planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica" (ABNT, 2006, p. 7).

5.4.7 Acompanhamento dos planos de ação de segurança da informação

Nesta fase, é realizado um acompanhamento da execução dos planos de ação, juntamente com os responsáveis pela sua execução, para verificar o cumprimento dos prazos e avaliar possíveis desvios de execução que tornem necessária uma nova avaliação.

5.4.8 Fechamento, documentação e emissão de relatórios

Nesta fase são registradas as ações realizadas durante o ciclo de avaliação e confeccionados relatórios operacionais e gerenciais. Nesta fase é documentada a evolução do nível de maturidade dos objetivos de controle.

A documentação de fechamento deve ser completa o suficiente para demonstrar a evolução da segurança da informação, conscientizar a direção para os principais pontos de atenção e riscos remanescentes, justificar a necessidade de recursos para melhorar o nível de segurança e embasar as análises críticas de melhoria do SGSI.

6 ESTUDO DE CASO DE AVALIAÇÃO DA MATURIDADE DA SEGURANÇA DA INFORMAÇÃO

Um estudo de caso foi realizado para aplicação do modelo de avaliação do nível de maturidade da segurança da informação descrito nas seções anteriores. A organização que participou do estudo possui sua sede administrativa em Florianópolis, no Estado de Santa Catarina.

O escopo de avaliação escolhido foi o conjunto de processos e atividades administrativas da organização. A organização já havia realizado, em anos anteriores, avaliações de segurança da informação com método semelhante ao descrito neste artigo, fato que facilitou as tarefas de avaliação e diminuiu o tempo de análise.

A organização avaliada não possuía, no início dos trabalhos, uma avaliação formal dos riscos especificamente relacionados à segurança da informação. Considerou-se que uma análise completa dos controles de

segurança da informação seria adequada para a apuração do atual nível de maturidade e identificação de riscos desconhecidos.

Inicialmente, em virtude da grande extensão dos processos de negócio da organização, decidiu-se por considerar como sendo aplicável a maioria dos controles de segurança da informação propostos na norma ABNT NBR ISO/IEC 27002. O controle 10.9.1 - Comércio Eletrônico - foi o único controle excluído do escopo de análise, pois a organização não apresenta este tipo de atividade.

A avaliação dos controles foi realizada pelo responsável pela segurança da informação, com a possibilidade de consulta aos especialistas em cada área. As análises e avaliações foram registradas em planilha de avaliação. Também foram registradas sugestões para as melhorias consideradas necessárias. Para cada um dos controles de segurança da norma ABN NBR ISO/IEC 27002 existem campos na planilha de avaliação que foram preenchidos com os seguintes dados: o nível de maturidade atual, o nível de maturidade objetivo, o nome do(s) avaliador(es), a data da última avaliação, os processos e atividades relacionados e os planos de ação sugeridos.

Foi selecionado para exemplo o controle 11.2.4 - *Análise crítica dos direitos de acesso de usuário*, objetivo de controle 11.2 - *Gerenciamento de acesso do usuário*. De acordo com a ABNT (2005, p. 68), “convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal”, a fim de manter um efetivo controle sobre os acessos. As atividades realizadas nos cinco passos de avaliação foram:

a) Identificação dos processos e atividades relacionadas: a organização possuía um processo semestral de revisão dos direitos de acesso ao ambiente computacional. Todo o processo de revisão estava formalizado em um procedimento de gestão, e a Política de Segurança de Informações atribuía as responsabilidades pelo processo de revisão aos usuários chave de cada sistema, módulo ou ambiente computacional. Houve treinamento dos responsáveis pela revisão e há material de apoio disponível. A coordenação do processo era realizada pelo responsável pela segurança da informação. Entretanto, a solicitação da revisão de acessos e a resposta de conclusão eram realizadas por e-mail, com pouco controle sobre a execução do processo;

b) Análise do nível de maturidade do controle: de acordo com a escala de maturidade utilizada neste trabalho, a existência de um processo formalmente definido e aprovado, com responsabilidades identificadas, e com treinamento dos envolvidos caracteriza o nível de maturidade 3 – Definido;

c) Avaliação da maturidade do controle: a organização, por estar submetida a exigências de controles nos processos de TI, necessitava demonstrar que possuía controle sobre o processo de revisão de direitos de acesso. Neste caso não bastava para a organização ter um processo

definido para realizar a atividade, mas um processo para controlar a atividade de modo a garantir que fosse executada de acordo com o definido. Como consequência a organização considerou necessário melhorar o processo de revisão de direitos de acesso, de modo a atingir o nível 4 – Gerenciado;

d) Definição de melhorias necessárias: para alcançar o nível 4 de maturidade (gerenciado) as seguintes ações foram sugeridas:

   I. Fazer um sistema para registrar todos os ciclos de revisão de direitos de acesso, contendo todos os sistemas, módulos e ambientes que participaram do ciclo, os respectivos responsáveis pela revisão e data de conclusão do processo de revisão;

   II. Modificar o processo de revisão de direitos de acesso para que houvesse controle documentado sobre a realização das revisões e sobre a tomada de ação no caso de haver algum sistema, módulo ou ambiente que não tivesse a revisão concluída no prazo estipulado;

   III. Realizar comunicação formal ao responsável pelo sistema, módulo ou ambiente que não tivesse seu processo de revisão concluído no prazo estipulado; e

   IV. Realizar comunicação formal sobre o acompanhamento do processo ao gerente da área de TI e auditoria interna sobre a finalização do ciclo de revisão.

e) Comunicação dos resultados aos responsáveis pelo controle: as ações propostas foram documentadas e encaminhadas ao gerente de TI e à auditoria interna.

Após a finalização das avaliações do nível de maturidade de todos os controles selecionados, as ações propostas deram origem a planos de ação. Os planos de ação que não necessitavam de recursos financeiros foram selecionados para serem executados primeiro. Os planos de ação que necessitavam de investimento ou exigiam mudanças maiores em processos serão acompanhados pela organização. A cada novo ciclo de avaliação os controles aplicáveis serão reavaliados e os planos de ação revisados.

A Tabela 1 foi obtida a partir da planilha de avaliação preenchida com dados do nível de maturidade atual para cada seção da norma ABNT NBR ISO/IEC 27002, apresentando os resultados dos níveis de maturidade médios.

Pela análise dos resultados obtidos, considera-se que a organização possui um nível de maturidade médio geral de 2,54. Isso indica que, em média, seus processos relacionados à segurança da informação estão sendo estruturados para serem definidos formalmente. A organização considera que a maioria dos seus processos possui nível de maturidade adequado à sua realidade, sendo que os principais controles relacionados à conformidade com requisitos externos estão classificados nos níveis entre 3 e 4. Diversos planos de ação criados objetivaram pequenas melhorias em processos, não estando necessariamente relacionados a incrementos do nível de maturidade.

Tabela 1. Níveis de maturidade médios calculados

Seção	Descrição – ABNT NBR ISO/IEC 27002	Maturidade média
5	Política de segurança da informação	3,17
6	Organização da segurança da informação	2,78
7	Gestão de ativos	2,55
8	Segurança em recursos humanos	2,35
9	Segurança física e do ambiente	3,24
10	Gerenciamento das operações e comunicações	2,61
11	Controle de acessos	2,59
12	Aquisição, desenvolvimento e manutenção de sistemas de informação	2,80
13	Gestão de incidentes de segurança da informação	1,55
14	Gestão da continuidade do negócio	2,02
15	Conformidade	2,24

Fonte: elaborada pelos autores.

A Figura 5 apresenta a visualização dos níveis de maturidade médios calculados.

Figura 5. Níveis de maturidade médios obtidos no estudo de caso
Fonte: elaborada pelos autores.

A partir das análises realizadas durante o estudo de caso observou-se que a organização participante do estudo delegou a responsabilidade pela realização das análises e avaliações a apenas uma pessoa. O fato de o responsável pela avaliação estar subordinado ao departamento de TI poderia caracterizar falta de independência para avaliação. Considera-se, contudo, que tal situação tem pouca influência na avaliação do método em si e dos benefícios gerados pela sua utilização.

De acordo com a percepção da organização, o método de avaliação dos controles da norma ABNT NBR ISO/IEC 27002 por meio de níveis de maturidade proporcionou algumas vantagens, conforme relato do responsável pela área de TI: “Este método não será utilizado apenas como uma forma de avaliação isolada, e sim como um instrumento de gestão para a segurança das nossas informações. Além de fornecer uma ‘foto’ do cenário atual dos nossos controles, o método proporciona a criação de documentação para avaliação e direcionamento dos esforços para a melhoria da segurança. Muitas ações de melhoria foram identificadas com a avaliação individual de cada item de controle, e o modelo de maturidade auxilia na sua priorização”.

7 CONCLUSÃO

O detalhamento de um método para a gestão da segurança da informação por meio da avaliação periódica da maturidade e melhoria contínua dos controles foi mostrado. O uso da escala de maturidade aliado ao processo cíclico de avaliação proporcionou a geração de indicadores instantâneos e temporais para a gestão da segurança da informação.

A semelhança entre este trabalho e os trabalhos relacionados apresentados está no uso da norma ABNT NBR ISO/IEC 27002 e de um modelo de maturidade. A principal diferença reside no fato de que os modelos propostos que apresentam proposições específicas, estáticas, podem não possibilitar ao avaliador a adequada análise dos riscos inerentes ao negócio, na medida em que haja evolução do ambiente. Outra importante diferença é que este trabalho procura definir um modelo genérico de avaliação, aplicável a todos os tipos de organização, utilizando todos os objetivos de controle constantes da norma ABNT NBR ISO/IEC 27002.

Consideramos que o uso de modelos com proposições estáticas e específicas para um determinado setor é útil para avaliadores iniciantes ou inexperientes, pois pode conter exemplos do que poderia ser feito para melhorar os seus processos de segurança. Contudo, limita a avaliação às questões propostas, à visão do elaborador e ao tempo em que foram criadas as questões incluídas no modelo adotado. Já o uso de um modelo genérico pode não ser o mais adequado para avaliadores iniciantes, que devem primeiro compreender e interpretar as normas. No entanto, propiciam ao avaliador experiente espaço para adequações e expansões do escopo de avaliação de acordo com mudanças dos níveis de risco ao longo do tempo, sendo mais condizente com o ciclo de melhoria contínua.

A percepção da organização que participou do estudo de caso indica que o método de avaliação apresentado pode ser eficaz para avaliar o estado atual da segurança da informação da organização, para auxiliar nos processos de gestão, identificação de riscos, e para apoiar a melhoria dos processos e controles internos.

Alguns trabalhos futuros podem ser sugeridos: (a) projetar ferramenta para automatizar a vinculação dos resultados das avaliações de riscos dos objetivos de controle a níveis de maturidade mínimos a serem atingidos; (b) aplicar o instrumento de avaliação proposto em outras organizações para possibilitar comparações entre organizações do mesmo setor; (c) criar modelos que possam ser utilizados em todas as fases e etapas de avaliação; e (d) inserir no ciclo de avaliação uma fase para auditoria independente dos resultados, para as organizações que optarem pela autoavaliação.

REFERÊNCIAS

ACEITUNO, Vicente. ISM3 - Information Security Managemente Maturity Model v. 2.1. ISM3 Consortium, 2007. Disponível em: http://www.ism3.com. Acesso em: 20 dez 2012.

ABNT. *NBR ISO/IEC 27001:2006: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos*. Rio de Janeiro: ABNT, 2006.

ABNT. *NBR ISO/IEC 27002:2005: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT, 2005.

ABNT. *NBR ISO/IEC 27005:2008: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança de informação*. Rio de Janeiro: ABNT, 2008.

BREIER, J.; HUDEC, L. New approach in information system security evaluation. In: IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), 1., Rome, Italy, *Proceedings*..., p. 1-6, IEEE, 2012.

CHAPIN, D. A.; AKRIDGE, S. How can security be measured. *Information Systems Control Journal*, v. 2, p. 43-47, 2005.

CUNHA, Renato Menezes da. Modelo de governança da segurança da informação no escopo da governança computacional. Dissertação – Mestrado em Engenharia de Produção, Universidade Federal de Pernambuco, Recife, 2008.

GARCIA, Carlos Kleber da Silva. Avaliação do serviço de perícia criminal baseada em confiança institucional. 2012. xiv, 109 f., il. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, 2012.

ITGI – IT GOVERNANCE INSTITUTE. CobiT 4.1 - Control Objectives for Information and related Technology - Framework. Rolling Meadows - USA: [s.n.], 2007. Disponível em: http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx. Acesso em: 12 dez 2012.

JANSSEN, Luis Antonio. Instrumento de avaliação de maturidade em processos de segurança da informação: estudo de caso em instituições hospitalares. Dissertação – Curso de Mestrado em Administração e Negó-

cios, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: http://tede.pucrs.br/tde_arquivos/2/TDE-2008-04-22T140541Z-1200/Publico/400421.pdf. Acesso em: 12 dez 2012.

KAROKOLA, G.; KOWALSKI, S; YNGSTRÖM, L. Towards an information security maturity model for secure e-government services: a stakeholders view. In: International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011), 5., London, UK. *Proceedings*..., p. 58-73, HAISA, 2011. Disponível em: http://su.diva-portal.org/smash/record.jsf?pid=diva2:469623. Acesso em: 15 dez 2012.

MARANHÃO, Mauriti. *ISO Série 9000: manual de implementação: versão ISO 2008*. Rio de Janeiro: Qualitymark, 2011.

PARK, Jung-Oh; KIM, Sang-Geun; CHOI, Byeong-Hun; JUN, Moon-Seog. The study on the maturity measurement method of security management for ITSM. In: International Conference on Convergence and Hybrid Information Technology, Daejeon, Korea. *Proceedings...* SERC: IEEE Press, 2008. p. 826-830.

PINHEIRO, Patrícia Peck; SLEIMAN, Cristina Moraes. *Tudo o que você precisa saber sobre direito digital no dia-a-dia*. São Paulo: Saraiva, 2009.

RAMOS, Anderson. *Security officer - 1: guia oficial para formação de gestores em segurança da informação*. Porto Alegre: Zouk, 2006.

THE OPEN GROUP. *Open information security management maturity model (O-ISM3)*. Netherlands: Van Haren Publishing, 2011.

WALKER, Alastair; McBRIDE, Tom; BASSON, Gerhard; OAKLEY, Robert. ISO/IEC 15504 measurement applied to COBIT process maturity. *Benchmarking: an International Journal*, v. 19, n. 2, p. 159-176, 2012.

WOODHOUSE, Steven. An ISMS (Im)-Maturity Capability Model. In: IEEE International Conference on Computer and Information Technology, 8., Washington, DC, USA, *Proceedings...* IEEE: Computer Society Press, 2008, p. 242-247.