Modelo de Avaliação da Maturidade da Segurança da Informação

Evandro Alencar Rigon, Carla Merkle Westphall

Departamento de Informática e Estatística (INE)
Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 - 88.040-970 - Florianópolis - SC - Brasil

{rigon@inf.ufsc.br, 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 treats 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 and business and internal control processes.*

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 poderá expor a organização ao risco em diversas situações. Este artigo apresenta um processo para a gestão da maturidade da segurança da informação através 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.*

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 gerenciam 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.

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).

Este artigo propõe um método para a gestão da segurança da informação através 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, através do uso dos 133 objetivos de controle de segurança da informação constantes da norma ABNT NBR ISO/IEC 27002 (ABNT NBR ISO/IEC 27002:2005, 2007). 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 através da medição de níveis de maturidade. A seção 6 apresenta um estudo de caso onde o modelo foi aplicado em uma organização para verificação da sua eficácia. A última seção apresenta as conclusões.

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 3 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 em instituições hospitalares. 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 no nosso trabalho é apresentado um processo de gestão para melhoria contínua da segurança, na forma de um modelo genérico aplicável a todos os tipos de organização, independente de tamanho ou área de atuação, através do uso dos 133 objetivos de controle de segurança da informação constantes da norma ABNT NBR ISO/IEC 27002. A principal diferença é que o modelo proposto por (JANSSEN, 2008) apresenta proposições específicas, estáticas, e que pode 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 incorpore 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 nosso 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 na 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 a maturidade dos processos relacionados à segurança da informação e respectivos riscos ao negócio da organização.

(PARK et al, 2008) apresenta uma maneira de medir a maturidade de gerenciamento de serviços de tecnologia da informação e usa as melhores 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 melhores 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, e 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 NBR ISO/IEC 27001:2006).

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, através da definição de controles que podem ser utilizados para atender aos requisitos identificados por meio da análise/avaliação de riscos (ABNT NBR ISO/IEC

27002:2005, 2007). 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 não é perfeita e prevê que as organizações possam vir a utilizar mais controles além dos que ela recomenda.

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/IEC27001, para implementação da segurança da informação baseada na gestão de riscos (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).

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

Algumas abordagens de padrões para gerenciamento da segurança da informação podem ser classificados da seguinte forma: orientados a processos como CobiT e ITIL; orientados a controles como ISO 27001; orientados a produtos como os Critérios Comuns (ISO 15408); orientados a gerenciamento de riscos como OCTAVE e ISO 27005 e orientados a melhores práticas como a ISO 27002. O trabalho de (ACEITUNO, 2007) define um modelo de maturidade para o gerenciamento da segurança da informação, compatível com a norma ISO 27001.

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, através do uso da norma ABNT NBR ISO/IEC 27001.
b) Ser baseado em controles apropriados para a segurança da informação, através 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, através do uso de um modelo de maturidade;
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.

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 poderão ser avaliados.

5.3. Medição e Acompanhamento

O CobiT (*Control Objectives for Information and Related Technology*) apresnta um conjunto de indicadores obtidos através do consenso de experts, 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.

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 1).

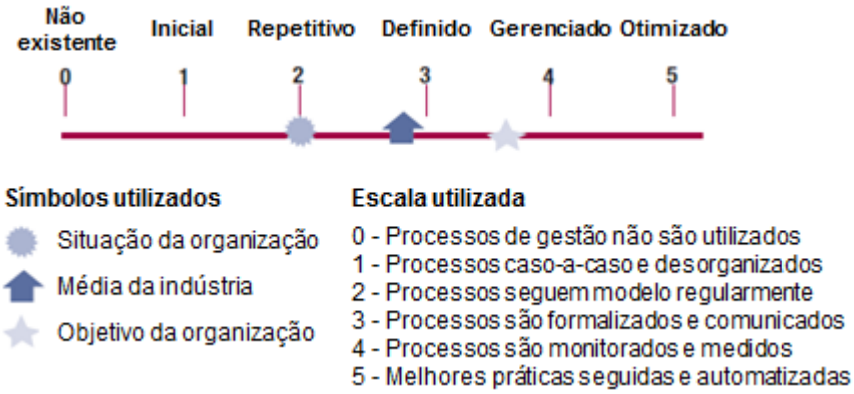

Figura 1. Representação gráfica do modelo de maturidade utilizado no CobiT (adaptado de ITGI, 2007).

A escala de maturidade utilizada neste artigo é apresentada na tabela 1.

Tabela 1. Escala utilizada para os níveis de maturidade (adaptado de ITGI, 2007)

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 através de treinamento. É obrigatório que os procedimentos sejam seguidos; entretanto, é improvável que desvios sejam detectados. Os procedimentos não são, por si só, sofisticados, mas são 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.

Nível	Características
5 Otimizado	Os processos foram refinados ao nível de melhores práticas, baseado no resultado de melhorias contínuas e de comparação com outras organizações. TI é utilizada de maneira integrada para automatizar fluxos de trabalho.

5.4. Fases do ciclo de avaliação e melhoria contínua

Uma métrica, ou indicador, por si só, não é a resposta para gerenciar os problemas de segurança da informação de uma organização. Além de medir, deve existir ação sobre os problemas encontrados e o acompanhamento da evolução ao longo do tempo. A figura 2 apresenta as oito fases que compõem o ciclo de avaliação da maturidade da segurança da informação (SI) proposto.

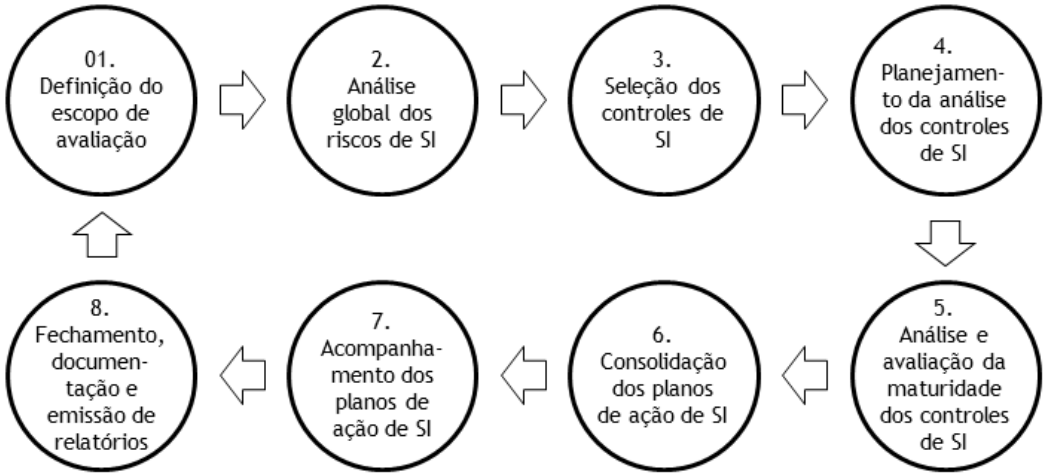

Figura 2. Fases do ciclo de avaliação e melhoria da segurança da informação (SI)

5.4.1. Definição do escopo de avaliação

Nesta fase será definido o escopo para a avaliação do nível de maturidade da segurança. Uma organização pode possuir atividades administrativas, industriais e de prestação de serviços, e considerar conveniente dividir a avaliação da maturidade em partes.

A definição do escopo consiste em identificar as áreas, tecnologias e processos da organização que serão incluídos na avaliação (ABNT NBR ISO/IEC 27001, 2006).

5.4.2. Análise dos riscos relacionados à segurança da informação

Nesta fase a organização realizará a identificação global dos riscos relacionados à segurança das suas informações, para garantir que os controles selecionados estejam relacionados ao tratamento dos riscos (ABNT NBR ISO/IEC 27001, 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 tornar evidentes grandes riscos, e normalmente é menos complexa e menos onerosa (ABNT NBR ISO/IEC 27005, 2008).

Este modelo utiliza o método qualitativo para análise de riscos, através do uso de 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 melhores práticas adotadas no setor ao qual a organização estiver inserida.

5.4.4. Planejamento da análise dos controles de segurança da informação

Nesta fase será 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 será comparado com a análise de riscos e, caso necessário, ações devem ser propostas para correção e/ou melhoria das atividades relacionadas. Esta fase é dividida em cinco etapas:

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 haverá atividades relacionadas ao mesmo controle com níveis de maturidade distintos;
c) Avaliação da maturidade do controle: nesta etapa será 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 serão documentadas as ações e melhorias nas atividades relacionadas ao controle de segurança, ou mesmo a criação de novas atividades, 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.

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 mesmo interdependentes. Nesta fase todas as melhorias

propostas serão 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;
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.

5.4.7. Acompanhamento dos planos de ação de segurança da informação

Nesta fase será realizado um acompanhamento da execução dos planos de ação para verificar o cumprimento dos prazos e avaliar possíveis desvios de execução.

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 deverá 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. A organização que participou do estudo possui sua sede administrativa situada 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.

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 NBR ISO/IEC 27002, "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 do nível de 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 ambientes que participaram do ciclo, responsáveis e data de conclusão;
   ii. Modificar o processo de revisão de direitos de acesso para que houvesse controle documentado sobre a realização das revisões;
   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 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 processo serão acompanhados pela organização. A cada novo ciclo de avaliação os controles aplicáveis serão reavaliados e os planos de ação revisados.

A tabela 2 apresenta os resultados dos níveis de maturidade médios apurados para cada seção da norma ABNT NBR ISO/IEC 27002 na avaliação.

Tabela 2. Níveis de maturidade médios apurados

Seção	Descrição – ABNT NBR ISO/IEC 27002	Maturidade média
5	Política de segurança da informação	3,17
6	Organizando a 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

A figura 3 apresenta a visualização dos níveis de maturidade médios apurados.

Figura 3. Visualização dos níveis de maturidade médios apurados no estudo de caso

Através da 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.

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 nos 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. Conclusões e Trabalhos Futuros

O detalhamento de um método para a gestão da segurança da informação através 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 (RIGON, 2010).

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, através do uso de 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, limitam a avaliação às questões propostas, à visão do elaborador e ao tempo em que foram criadas. 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 auto avaliação.

8. Referências

ACEITUNO, Vicente. ISM3 - Information Security Managemente Maturity Model – v. 2.1. ISM3 Consortium. 2007. Disponível em <http://www.ism3.com/page1.php>. Acesso em: 20 janeiro 2011.

ABNT. NBR ISO/IEC 27001:2006: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro, 2006. 34 p.

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, 2005. 120 p.

ABNT. NBR ISO/IEC 27005:2008: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança de informação. Rio de Janeiro, 2008. 55 p.

CHAPIN, D. A. e AKRIDGE, S. "How can security be measured," Information Systems Control Journal, vol. 2, pp. 43-47, 2005.

CUNHA, Renato Menezes da. Modelo de Governança da Segurança da Informação no Escopo da Governança Computacional. UFPE. 2008. Disponível em < http://www.bdtd.ufpe.br/tedeSimplificado/tde_arquivos/26/TDE-2009-03-09T123252Z-5469/Publico/rmc.pdf >. Acesso em: 29 abril 2010.

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 setembro 2010.

JANSSEN, Luis Antonio. Instrumento de avaliação de maturidade em processos de segurança da informação: estudo de caso em instituições hospitalares. PUC-RS. 2008. Disponível em <http://tede.pucrs.br/tde_arquivos/2/TDE-2008-04-22T140541Z-1200/Publico/400421.pdf >. Acesso em: 29 abril 2010.

MARANHÃO, Mauriti; ISO Série 9000: manual de implementação: versão ISO 2000. 6ª ed. Rio de Janeiro: Qualitymark, 2001. 220p.

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: Proc. of the International Conference on Convergence and Hybrid Information Technology, pp.826-830, 2008. IEEE Press.

PINHEIRO, Patrícia Peck; SLEIMAN, Cristina Moraes. Tudo o que você precisa saber sobre direito digital no dia-a-dia. São Paulo: Saraiva, 2009. 58p.

RAMOS, Anderson (org.). Security Officer - 1: guia oficial para formação de gestores em segurança da informação. Porto Alegre: Zouk, 2006. 460p.

RIGON, Evandro Alencar. Modelo de Avaliação da Maturidade da Segurança da Informação. UFSC. 2010. Disponível em <http://projetos.inf.ufsc.br/arquivos_projetos/projeto_1055/Modelo_Avaliacao_Maturidade_Seguranca_Informacao_Rigon.pdf>. Acesso em: 08 abril 2011.

WOODHOUSE, Steven. 2008. An ISMS (Im)-Maturity Capability Model. In: Proceedings of the 2008 IEEE 8th International Conference on Computer and Information Technology Workshops (CITWORKSHOPS '08). IEEE Computer Society, Washington, DC, USA, pp. 242-247.