

UNIVERSIDADE FEDERAL DE SANTA CATARINA

**MODELO DE AVALIAÇÃO DA MATURIDADE DA
SEGURANÇA DA INFORMAÇÃO**

EVANDRO ALENCAR RIGON

Florianópolis – SC

2010/2

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO**

**MODELO DE AVALIAÇÃO DA MATURIDADE DA
SEGURANÇA DA INFORMAÇÃO**

EVANDRO ALENCAR RIGON

Orientadora:

Professora Dra. CARLA MERKLE WESTPHALL

**Trabalho de conclusão de curso apresentado
como parte dos requisitos para obtenção do
grau de Bacharel em Sistemas de Informação.**

Florianópolis – SC

2010/2

EVANDRO ALENCAR RIGON

**MODELO DE AVALIAÇÃO DA MATURIDADE DA
SEGURANÇA DA INFORMAÇÃO**

**Trabalho de conclusão de curso apresentado
como parte dos requisitos para obtenção do
grau de Bacharel em Sistemas de Informação.**

Orientadora:

Professora Dra. Carla Merkle Westphall

Banca Examinadora:

Professora Dra. Aline França de Abreu

Professor Dr. Ricardo Felipe Custódio

Florianópolis, __ de novembro de 2010.

AGRADECIMENTOS

Agradeço à minha esposa Jacqueline e aos meus filhos Julia e Bernardo pela compreensão durante os anos de estudo na Universidade.

Aos meus pais, por terem proporcionado condição de estudo e aprendizado que me permitiram iniciar e concluir esta etapa.

À professora Carla Merkle Westphall por ter prontamente aceitado orientar este trabalho e ter positivamente contribuído para a sua execução.

Aos professores Ricardo Felipe Custódio e Aline França de Abreu, por aceitarem participar da banca examinadora.

“A leitura traz ao homem plenitude, o discurso segurança e a escrita exatidão”.

Francis Bacon

SUMÁRIO

1.	INTRODUÇÃO	12
1.1.	Motivação	13
1.2.	Objetivo Geral.....	14
1.3.	Objetivos Específicos.....	14
1.4.	Justificativa	14
1.5.	Delimitação de Escopo	15
1.6.	Organização do Trabalho	15
2.	A SEGURANÇA DA INFORMAÇÃO	17
2.1.	Características	18
2.1.1.	Os principais componentes da segurança da informação.....	19
2.1.2.	Benefícios da segurança da informação para o negócio	21
2.1.3.	Cuidados na implementação da gestão da segurança da informação....	24
2.2.	Principais normas técnicas relacionadas à segurança da informação	26
2.2.1.	ABNT NBR ISO/IEC 27001:2006	27
2.2.2.	ABNT NBR ISO/IEC 27002:2005	29
2.2.3.	ABNT NBR ISO/IEC 27004:2010	31
2.3.	Gerenciamento do Risco	31
2.3.1.	ABNT ISO GUIA 73:2009	32
2.3.2.	ABNT NBR ISO 31000:2009	33
2.3.3.	ABNT NBR ISO/IEC 27005:2008	35
2.4.	Frameworks e melhores práticas relacionadas à segurança da informação	37
2.4.1.	CobiT	37
2.4.2.	ITIL	40
3.	O MODELO DE AVALIAÇÃO POR NÍVEIS DE MATURIDADE	41
3.1.	Avaliação e melhoria contínua.....	42
3.1.1.	Abordagem de processo	42
3.2.	Controles de segurança da informação	43
3.3.	Medição e Acompanhamento	43
3.3.1.	<i>Capability Maturity Model</i> - CMM	44
3.4.	Fases do ciclo de avaliação e melhoria contínua da segurança da informação	47
3.4.1.	Definição do escopo de avaliação	48

3.4.2.	Análise dos riscos relacionados à segurança da informação.....	48
3.4.3.	Seleção dos controles de segurança da informação	50
3.4.4.	Planejamento da análise dos controles de segurança da informação	51
3.4.5.	Análise e avaliação da maturidade dos controles de segurança da informação.....	51
3.4.6.	Consolidação dos planos de ação de segurança da informação	53
3.4.7.	Acompanhamento dos planos de ação de segurança da informação.....	55
3.4.8.	Fechamento, documentação e emissão de relatórios.....	55
3.5.	Trabalhos Relacionados	55
4.	ESTUDO DE CASO DE AVALIAÇÃO DA MATURIDADE DA SEGURANÇA DA INFORMAÇÃO	58
4.1.	A organização	58
4.2.	O escopo de avaliação.....	58
4.3.	Análise global dos riscos à segurança da informação.....	59
4.4.	Seleção dos controles de segurança da informação	59
4.5.	Planejamento da análise dos controles de segurança da informação.....	60
4.6.	Análise e avaliação da maturidade dos controles de segurança da informação	60
4.6.1.	Exemplo de avaliação de controles de segurança da informação	60
4.7.	Consolidação dos planos de ação de segurança da informação	64
4.7.1.	Exemplo de consolidação de um plano de ação.....	64
4.8.	Acompanhamento dos planos de ação de segurança da informação	65
4.9.	Fechamento, documentação e emissão de relatórios	65
4.9.1.	Avaliação dos resultados.....	66
4.10.	Percepção da organização sobre o método de avaliação	67
5.	CONSIDERAÇÕES FINAIS	68
5.1.	Conclusões	68
5.2.	Sugestões para pesquisas e trabalhos futuros.....	69
6.	REFERÊNCIAS	71
	APÊNDICE.....	74
	ANEXO A - Formulário para avaliação do nível de maturidade da segurança da informação.....	90

LISTA DE FIGURAS

Figura 1.	Pirâmide ou tríade da Segurança da Informação	19
Figura 2.	Interação entre os componentes da segurança da informação	21
Figura 3.	Posicionamento da gestão da segurança da informação de acordo com os resultados das organizações	26
Figura 4.	Modelo PDCA aplicado aos processos do SGSI	28
Figura 5.	Processo de gestão de riscos	34
Figura 6.	Processo de gestão de riscos de segurança da informação	35
Figura 7.	Atividades de tratamento dos riscos de segurança da informação	36
Figura 8.	Representação gráfica do modelo de maturidade	45
Figura 9.	Fases do ciclo de avaliação e melhoria da segurança da informação	47
Figura 10.	Escala para análise e classificação de riscos.....	49
Figura 11.	Etapas de análise e avaliação dos controles de segurança da informação	52
Figura 12.	Interação das etapas de análise dos controles com a escala de maturidade e as normas utilizadas	53
Figura 13.	Etapas da consolidação dos planos de ação de segurança da informação	54

LISTA DE GRÁFICOS E TABELAS

Tabela 1.	Principais componentes da segurança da informação.	20
Tabela 2.	Comparativo de indicadores de segurança da informação e financeiros das organizações de acordo com seu resultado financeiro.....	22
Tabela 3.	Comparativo de características de gestão da segurança da informação nas organizações de acordo com seu resultado financeiro.....	23
Gráfico 1.	Percentual dos cargos dos responsáveis pela segurança da informação.....	24
Gráfico 2.	Resultados das organizações por cargo do responsável pela segurança da informação	24
Tabela 4.	Descritivo das fases do modelo PDCA aplicado ao SGSI.....	29
Tabela 5.	Níveis de maturidade do processo de gestão da segurança dos sistemas - CobiT.	39
Tabela 6.	Principais características do modelo de avaliação e seu relacionamento com as normas e modelos apresentados.....	41
Tabela 7.	Escala de níveis de maturidade.....	46
Tabela 8.	Exemplo de aplicação e interpretação da escala de maturidade para avaliação do controle sobre vírus.....	46
Tabela 9.	Níveis de maturidade médios apurados	66
Gráfico 3.	Visualização dos níveis de maturidade médios apurados no estudo de caso	66

LISTA DE ACRÔNIMOS

Acrônimo	Descrição
ABNT	Associação Brasileira de Normas Técnicas
BSI	<i>British Standards Institution</i>
CFO	<i>Chief Financial Officer</i>
CIO	<i>Chief Information Officer</i>
CISO	<i>Chief Information Security Officer</i>
CobiT	<i>Control Objectives for Information and related Technology</i>
CRO	<i>Chief Risk Officer</i>
CSO	<i>Chief Security Officer</i>
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization for Standardization</i>
IT	<i>Information Technology</i>
ITGI	<i>IT Governance Institute</i>
ITIL	<i>IT Infrastructure Library</i>
ITPCG	<i>IT Policy Compliance Group</i>
NIST	<i>National Institute of Standards and Technology</i>
OECD	<i>Organisation for Economic Co-operation and Development</i>
PDCA	<i>Plan - Do - Check - Act</i>
SEI	<i>Software Engineering Institute</i>
SGSI	Sistema de Gestão da Segurança da Informação
TI	Tecnologia da Informação

RESUMO

Os processos de negócio das organizações são, cada vez mais, suportados por tecnologias da informação. Apesar disso, muitos processos de negócio e sistemas de informação não foram projetados para serem seguros, deixando as organizações expostas a um crescente número de ameaças e vulnerabilidades. O desconhecimento das ameaças e vulnerabilidades existentes nos processos de negócio e nas tecnologias da informação, cada vez mais interdependentes, expõe as organizações a um nível de risco muito alto à continuidade das suas atividades e, conseqüentemente, à sua própria existência. A falta de um método para avaliar os controles de segurança poderá levar uma organização a adotar controles fracos, expondo-a ao risco em diversas situações. A avaliação crítica e metódica dos controles relacionados à segurança da informação é necessária pelo fato de que tecnologias, processos de negócio e pessoas mudam, alterando constantemente o nível de risco atual ou gerando novos riscos à organização. Este trabalho apresenta um método para a gestão da segurança da informação através da avaliação periódica da maturidade dos controles da organização e da melhoria contínua, com base nos riscos envolvidos. Foi realizada uma revisão na literatura para apresentar as principais normas e fontes de referência para a segurança da informação e gestão de riscos, e modelos de maturidade para medição e geração de indicadores. O modelo de avaliação é estruturado na forma de um processo de gestão e utiliza um conjunto de controles internacionalmente reconhecidos que tratam a segurança da informação de forma abrangente. Ao mesmo tempo, o modelo proporciona uma forma de medir o nível atual de segurança e a sua evolução ao longo do tempo, facilitando a identificação de necessidades de melhoria. Um estudo de caso foi realizado sobre a utilização do modelo para exemplificar a avaliação dos controles de segurança da informação de acordo com escala de níveis de maturidade. O trabalho realizado foi considerado suficiente para concluir que o método de avaliação por níveis de maturidade pode ser considerado eficiente para, além de avaliar o estado atual da segurança da informação da organização, auxiliar no processo de gestão da segurança da informação, na identificação de riscos, e no apoio à melhoria dos processos e dos controles internos da organização.

Palavras chave: sistema de gestão da segurança da informação, maturidade de processos, gestão de riscos, ISO 27001, ISO 27002.

ABSTRACT

Business processes are more often supported by information technologies. Nevertheless, many business processes and information systems were not designed to be safe, leading organizations to be exposed to a wide number of threats and vulnerabilities. Poor awareness on business and information technology threats and vulnerabilities exposes organizations to a very high risk level to their activities continuity and, consequently, to their own existence. The lack of a security control evaluation method might lead the organization to adopt weak controls, exposing it to several risky situations. Critical and methodical evaluations over information security related controls are necessary because technologies, business processes and human resources change over the time. Thus, the risk level changes constantly. This work presents an information security management method based on the periodic maturity level assessment, continuous improvement and on related risks. A literature review was made to present main information security and risk management norms and references, and maturity models for measurement and indicators generation. The evaluation model is structured as a management process based on an internationally recognized set of controls in which information security is treated on a comprehensive way. At the same time, the model provides a way to measure the current security level and its evolution over the time, for identifying improvement needs. A case study was carried out on model utilization to exemplify the information security controls evaluation using the maturity levels scale. The work was considered enough and adequate to conclude that the maturity levels assessment method can be considered efficient for the current state of information security evaluation, and to support the information security management, risk identification, and to improve business and internal control processes.

Key words: information security management system, process maturity, risk management, ISO 27001, ISO 27002.

1. INTRODUÇÃO

A informação existe e é armazenada em diversas formas. Está escrita ou impressa em papel, armazenada eletronicamente, em fitas de áudio e vídeo, ou mesmo falada em conversas (ABNT NBR ISO/IEC 27002, 2005, p. X).

Viver na era da informação, na era da sociedade digital, significa estar mais acessível e, conseqüentemente, mais exposto. As comunicações são mais rápidas e dinâmicas, passando do âmbito local para o alcance global. Os relacionamentos entre pessoas se tornou *online*, gerando mudanças de hábitos e promovendo a comunicação através de troca de mensagens eletrônicas (PINHEIRO; SLEIMAN, 2009).

A troca de informações entre as organizações, de qualquer tipo ou finalidade, também passou a ser feita através do meio eletrônico, principalmente com a chegada do comércio eletrônico e da disponibilização de serviços bancários *online*. A Internet passou a ser mais transacional e, cada vez mais, os bens das organizações passaram a ser representados de maneira intangível, ou seja, informações armazenadas em meios eletrônicos. O modelo de riqueza deixou de ser o de bens de produção e passou a ser o do conhecimento (PINHEIRO; SLEIMAN, 2009).

Os processos de negócio¹ das organizações são, cada vez mais, suportados por tecnologias da informação. Alguns processos somente são viáveis economicamente se forem executados através do uso de sistemas informatizados. Como consequência, a natureza das informações organizacionais trocadas por meios eletrônicos é cada vez mais diversa, e a quantidade e a criticidade das informações em trânsito aumentam substancialmente.

Apesar disso, muitos sistemas de informação não foram projetados para serem seguros, deixando as informações e as próprias organizações expostas a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISO/IEC 27002, 2005, p. X), tais como acesso não autorizado, roubo, alteração indevida, perda e destruição.

O desconhecimento das ameaças e das vulnerabilidades existentes nas tecnologias da informação e nos processos de negócio, cada vez mais complexos e interdependentes, expõe as organizações a um nível de risco muito alto à continuidade das suas atividades e, conseqüentemente, à sua própria existência.

¹ As referências a “negócio” neste trabalho devem, de um modo geral, ser consideradas como relacionadas às atividades que são essenciais aos objetivos de existência de uma organização.

O mau uso da informação ou a sua divulgação indevida “pode gerar danos e envolver ilícitos que vão desde a quebra de sigilo profissional a vazamento de informação confidencial de uma instituição, ou exposição de uma vida íntima ou privacidade de uma pessoa” (PINHEIRO; SLEIMAN, 2009, p.27.).

Em virtude disso, muitas leis e regulamentações têm surgido para tentar obrigar as organizações a dar a devida atenção à segurança da informação (RAMOS, 2006, p. 36), para que estas protejam os seus interesses, de seus empregados, clientes, parceiros de negócio, acionistas e a sociedade com que se relacionem.

Ao serem consideradas o principal patrimônio das pessoas e das organizações, as informações passaram a sofrer constante risco, como nunca sofreram antes, e a sua segurança passou a ser crucial (FERREIRA, 2003).

Este trabalho apresenta um modelo para que as organizações possam avaliar se o ambiente de segurança das suas informações está adequadamente definido e dimensionado para a proteção dos seus ativos.

1.1. Motivação

Definir objetivos de segurança da informação, alcançá-los, mantê-los e melhorar os controles que os suportam podem ser atividades essenciais 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 (ABNT NBR ISO/IEC 27002, 2005, p. X).

A avaliação crítica e metódica dos controles relacionados à segurança da informação é necessária pelo simples fato de que tecnologias, processos de negócio e pessoas mudam, em um ritmo muito rápido, alterando constantemente o nível de risco atual e gerando novos riscos à organização.

A motivação para a execução deste trabalho é descrever um método para a avaliação da segurança da informação que possa ser utilizado por diversas organizações, independente de porte e natureza das atividades realizadas, e que apresente um meio para avaliar, documentar e promover a melhoria contínua da segurança das suas informações, de maneira gradual e adequada à realidade na qual estiver inserida.

1.2. Objetivo Geral

Apresentar um método para a gestão da segurança da informação de uma organização através da avaliação periódica da maturidade e melhoria contínua dos seus controles, com base nos riscos a que estiver submetida.

1.3. Objetivos Específicos

Os objetivos específicos para a realização deste trabalho são:

- Realizar pesquisa bibliográfica sobre as principais fontes de referência para a segurança da informação, mostrando as suas características e requisitos para a sua gestão;
- Apresentar um modelo de avaliação da maturidade dos controles de segurança da informação para a geração de indicadores de segurança;
- Estabelecer um comparativo entre o modelo apresentado e trabalhos relacionados;
- Aplicar o modelo em uma organização para avaliação da sua pertinência através de um estudo de caso.

1.4. Justificativa

As principais normas internacionais relacionadas à segurança da informação, apresentadas neste trabalho no item 2.2 *Principais normas técnicas relacionadas*, apresentam controles aplicáveis para a gestão da segurança da informação, sem, contudo, definirem 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.

A falta de um método para avaliar a adequação dos controles poderá levar uma organização a adotar controles fracos, expondo-a ao risco em diversas situações. De modo inverso, poderá ocorrer o desperdício de recursos em controles superdimensionados. A falta de método para avaliar a adequação dos controles poderá levar, também, uma organização a tratar os riscos e controles de segurança de acordo com iniciativas individuais que não correspondam às necessidades ou aos objetivos estratégicos da organização, ou que não recebam o devido apoio para as ações necessárias.

O presente trabalho se justifica por apresentar um método para a avaliação da segurança da informação por meio do uso de normas internacionais que tratam o assunto de maneira abrangente e consistente, promovendo a análise crítica dos riscos e da adequação dos seus controles dentro do considerado adequado para a organização.

Esta análise crítica poderá ser utilizada para suportar a tomada de decisão relacionada às ações e investimentos necessários para a manutenção da segurança da informação de uma organização nas áreas de tecnologia, processos de negócios e de recursos humanos.

1.5. Delimitação de Escopo

O escopo deste trabalho consiste na apresentação de um modelo para avaliação da segurança da informação e a sua aplicação através de um estudo de caso em uma organização que, por questões de segurança, não será identificada. Não fazem parte do escopo deste trabalho:

- O desenvolvimento de recursos e sistemas de informação que auxiliem no processo de avaliação e acompanhamento da evolução do nível de segurança da organização;
- A definição de processos, atividades ou controles que suportem os requisitos de segurança da informação das normas utilizadas.

1.6. Organização do Trabalho

O presente trabalho está dividido em cinco capítulos, nos quais são abordados diversos aspectos relacionados à segurança da informação e dos métodos utilizados para definição do modelo de avaliação. O primeiro capítulo apresenta a introdução ao trabalho, os seus objetivos, motivação, a justificativa para sua realização e a sua estrutura de organização.

O segundo capítulo apresenta a segurança da informação e a gestão de riscos, com seus principais conceitos, características e normas técnicas relacionadas.

O terceiro capítulo é dedicado à especificação do modelo de avaliação da segurança da informação através da medição de níveis de maturidade, com a integração dos conceitos e normas apresentados nos capítulos anteriores.

O quarto capítulo apresenta um estudo de caso realizado em uma organização onde o modelo foi aplicado para verificação da sua eficácia. O quinto capítulo apresenta as conclusões e considerações finais do trabalho.

2. A SEGURANÇA DA INFORMAÇÃO

A informação é um recurso crítico não apenas para a realização de tarefas e concretização de negócios, mas também para a tomada de decisões. Pelo fato de estarem armazenadas em meios eletrônicos e até mesmo conectadas a redes externas, as informações poderiam ser divulgadas a concorrentes, corrompidas, apagadas ou mesmo não estar disponíveis quando necessário para as atividades do negócio (FERREIRA, 2003, p. 2).

Com uma importância cada vez maior para as organizações, as informações são consideradas um ativo de elevado valor que deve ser adequadamente mantido e protegido, para que se mantenha a continuidade das atividades de negócio e até mesmo a existência da organização.

Segundo Ramos (2006, p.16), “segurança é estar livre de perigos e incertezas”. Sêmola (2003, p. 40) define que “segurança é implementar controles que reduzam o risco a níveis adequados, viáveis e administráveis”.

Ferreira (2003, p. 1) define que “a segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades”.

Sêmola (2003, p. 43) define a segurança da informação como sendo “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua disponibilidade”.

A norma ABNT NBR ISO/IEC 27002 (2005, p. X) define:

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

O *National Institute of Standards and Technology* (NIST) define o propósito da segurança computacional (NIST *Handbook*, 1995, p. 9 - tradução livre do autor):

O propósito da segurança computacional é proteger os valiosos recursos de uma organização, tais como informação, hardware e software. Através da seleção e aplicação de medidas de controle apropriadas, a segurança auxilia na missão da organização protegendo os seus recursos físicos e financeiros, reputação, posição legal, empregados e outros recursos tangíveis e intangíveis.

A segurança da informação pode ser considerada como uma forma de “blindagem” para a proteção do patrimônio intangível de uma organização, e “engloba um conjunto de

ações que devem ser planejadas e programadas de forma a abranger as questões técnicas, comportamentais e, também, jurídicas” (PINHEIRO; SLEIMAN, 2009, p.27.).

A expressão “segurança da informação”, por si só, é um termo ambíguo, podendo significar tanto uma prática interdisciplinar adotada para tornar um ambiente seguro (segurança como um meio), como a característica que a informação adquire ao ser alvo de uma prática da segurança (segurança como fim) (SÊMOLA, 2003, p. 44).

A partir das diversas definições dadas para a segurança da informação, pode-se concluir que o seu gerenciamento 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, de segurança física e patrimonial, de auditoria, de controle interno e também de requisitos legais e jurídicos.

Uma visão lógica sobre a segurança da informação é que ela compreende todo esse universo. Entretanto, a maioria das organizações possui diferentes áreas para controlar os diferentes aspectos relacionados segurança da informação (RAMOS, 2006, p. 26).

Uma definição mais abrangente para a segurança da informação é dada por Sêmola (2003, p.44):

[...] uma prática adotada para tornar um ambiente seguro [...], de caráter interdisciplinar, composta de um conjunto de metodologias e aplicações que visam estabelecer: controles de segurança [...] dos elementos constituintes de uma rede de comunicação e/ou que manipulem a informação; e procedimentos para garantir a continuidade de negócios na ocorrência de incidentes.

2.1. Características

A premissa fundamental da segurança da informação é que não existe segurança absoluta. Jamais serão tratadas todas as possíveis situações de prejuízo. Praticamente não se tem como gerenciar, muitas vezes, um número razoável de situações inesperadas (RAMOS, 2006, p. 22).

A segurança da informação considera, basicamente, três aspectos fundamentais para evitar que ocorram danos aos ativos ou situações prejudiciais inesperadas: a integridade, a confidencialidade, e a disponibilidade da informação (FERREIRA, 2003, p. 2).

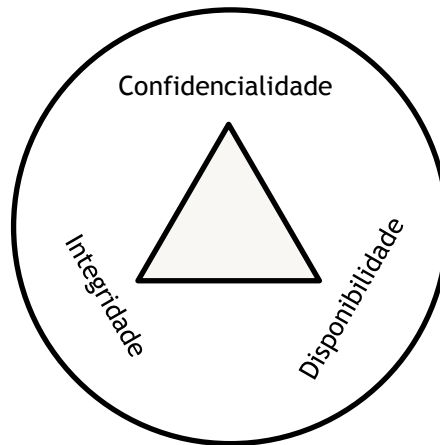


Figura 1. Pirâmide ou tríade da Segurança da Informação (adaptada de RAMOS, 2006, p. 21)

Ferreira (2003, p. 2) conceitua cada um dos aspectos:

Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas.

Integridade: salvaguarda da exatidão da informação e dos métodos de processamento.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Outro aspecto considerado por Ferreira (2003, p.2) é a segurança física e ambiental, para que haja garantia de que o ambiente de processamento esteja livre de acessos não autorizados que pudessem promover sabotagens, fraudes, ou de outras ações nocivas como desastres naturais e falhas estruturais.

2.1.1. Os principais componentes da segurança da informação

Para que a segurança da informação seja adequada para uma organização, sem se descuidar do bom senso financeiro, devem ser levadas em conta as interações entre alguns agentes principais e certos fatores. Ramos (2006, p.23) relaciona os principais agentes e fatores: valor, ameaça, vulnerabilidade, impacto e risco.

O valor pode ser avaliado através de propriedades mensuráveis como valores financeiros, ou de propriedades abstratas como a imagem da organização. Ativo é tudo aquilo que tenha valor e que necessita de algum tipo de proteção. Proteções são práticas, procedimentos ou mecanismos para proteger os ativos contra ameaças, reduzir ou eliminar as vulnerabilidades, ou mesmo limitar o impacto de um incidente. A ameaça é tudo o que tem potencial para comprometer os objetivos da organização e causar algum tipo de dano aos ativos, e está associada à ausência de mecanismos de proteção ou a falhas em mecanismos de

proteção existentes. O impacto é o tamanho do prejuízo que a concretização de uma determinada ameaça poderá causar. O risco é uma medida que indica a probabilidade de uma determinada ameaça se concretizar, combinada com os seus impactos. (RAMOS, 2006, p. 23 a 48).

A tabela 1 apresenta os principais componentes da segurança da informação e respectivos conceitos:

Tabela 1. Principais componentes da segurança da informação.

Componente	Conceito
Agente Ameaçador	Entidade (pessoa, sistema ou outras formas) que têm a intenção e/ou condição de criar ameaças e causar danos aos ativos.
Ameaça	Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT NBR ISO/IEC 27002:2005, p.3).
Ativo	Qualquer coisa que tenha valor para a organização (ABNT NBR ISO/IEC 27002:2005, p.1).
Proprietário	Pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos ² (ABNT NBR ISO/IEC 27002:2005, p.22).
Proteção	É a forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal ³ (ABNT NBR ISO/IEC 27002:2005, p.1).
Risco	Efeito da incerteza nos objetivos ⁴ (ABNT ISO GUIA 73, 2009, p. 1).
Valor	Importância do ativo para a organização (RAMOS, 2006, p. 24 e 25).
Vulnerabilidade	Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (ABNT NBR ISO/IEC 27002:2005, p.3).

A figura 2 apresenta um diagrama do relacionamento entre os principais componentes da segurança da informação.

² O termo “proprietário” não significa que uma pessoa realmente tenha qualquer direito de propriedade ao ativo (ABNT NBR ISO/IEC 27002:2005, p.22).

³ O termo “proteção” também é usado como sinônimo para controle ou contramedida (ABNT NBR ISO/IEC 27002:2005, p.1).

⁴ Um efeito é um desvio em relação ao esperado – positivo e/ou negativo. [...] A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade (ABNT ISO GUIA 73, 2009, p. 1).

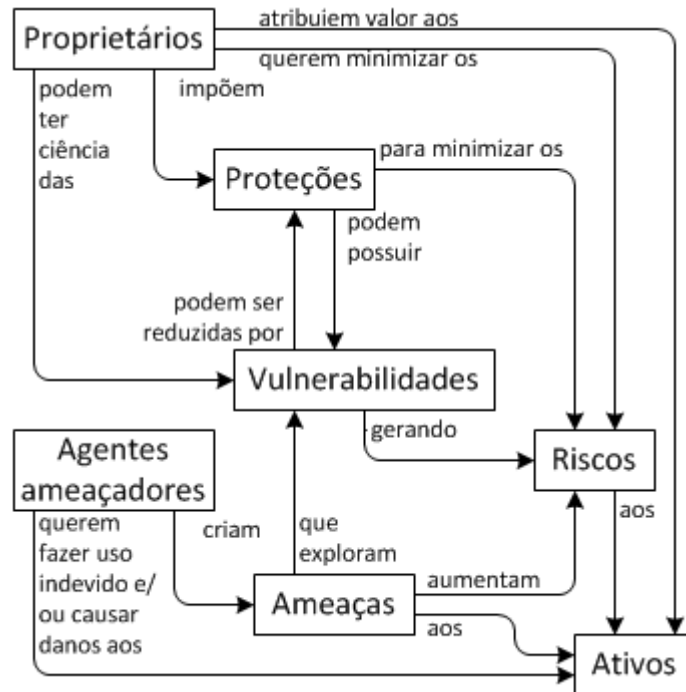


Figura 2. Interação entre os componentes da segurança da informação (adaptada de RAMOS, 2006 p. 26)

2.1.2. Benefícios da segurança da informação para o negócio

Segundo Sêmola (2003, p. 36 a 38) a gestão integrada da segurança da informação, sob a ótica do executivo e seu negócio, traz diversos benefícios ao negócio, tais como valoriza as ações da empresa, consolida a imagem de modernidade, consolida a imagem de saúde administrativa, aumenta os níveis de disponibilidade operacional, reduz os custos provocados por ameaças ou pelo mau uso dos recursos tecnológicos, reduz os riscos operacionais, preserva a imagem da empresa junto à sociedade e integra a segurança ao negócio.

O *IT Policy Compliance Group*⁵ (ITPCG), em sua publicação *Best Practices for Managing Information Security* (melhores práticas para gerenciar a segurança da informação) (2010), apresenta os resultados de uma pesquisa em tópicos relevantes à gestão da segurança da informação, incluindo: estrutura organizacional, estratégias operacionais, normas administrativas e operações de TI, entre outras. Os resultados são de comparações (*benchmarks*) realizados de dezembro de 2008 a outubro de 2009, entre empresas localizadas na América do Norte, de diversos setores da indústria, tais como aeroespacial, serviços

⁵ O ITPCG (*IT Policy Compliance Group*) é uma entidade dedicada à promoção e desenvolvimento de informações úteis que auxiliem as organizações a definir suas políticas de TI e alcançar seus objetivos de conformidade.

contábeis, financeiro e bancário, automotivo, químico, de informática, engenharia, saúde, médico e telecomunicações (ITPCG, 2010, p. 3 e 20).

Dentre as principais conclusões, destaca-se que as organizações com melhores resultados possuem características comuns relacionadas à segurança da informação.

Segundo ITPCG (2010, p.3), das organizações avaliadas, 10% apresentam os melhores resultados, 70% apresentam resultados normais e 20% apresentam os piores resultados. Essas organizações possuem estruturas e estratégias operacionais bem diferentes para a gestão da segurança da informação, de acordo com o seu resultado financeiro.

Das organizações que participaram da pesquisa, 30% possuem receita anual menor ou igual a \$50 milhões, 28% possuem receita anual de \$50 milhões a \$999 milhões, e 42% possuem receita anual igual ou maior que \$1 bilhão (ITPCG, 2010, p. 20).

O estudo apresenta indicadores de fatores relacionados à segurança da informação e ao desempenho financeiro, para comparação entre as organizações que responderam à pesquisa. Os indicadores estão consolidados na tabela 2:

Tabela 2. Comparativo de indicadores de segurança da informação e financeiros das organizações de acordo com seu resultado financeiro (adaptado de ITPCG, 2010, p. 3 e 4. Tradução livre do autor).

Indicador	Organizações com melhores resultados (10%)	Organizações com resultados normais (70%)	Organizações com piores resultados (20%)
Exposição anual de dados	0,4% da receita	6,4% da receita	9,6% da receita
Indisponibilidade de atividades do negócio	menos de 4 horas	4 a 59 horas	mais de 60 horas
Gastos com auditorias regulatórias	\$1,30 relacionadas à segurança	\$4,20 relacionadas à segurança	\$1,50 relacionadas à segurança
Receita	8,5% maior que a média da indústria	média da indústria	8,5% menor que a média da indústria
Lucro	6,4% maior que a média da indústria	média da indústria	6,9% menor que a média da indústria

A pesquisa demonstra que as organizações participantes com melhor resultado financeiro possuem menor exposição dos dados e maior disponibilidade das atividades de negócio.

A tabela 3 apresenta um comparativo entre características da gestão da segurança da informação entre as organizações que responderam à pesquisa, de acordo com o seu perfil de resultado.

Tabela 3. Comparativo de características de gestão da segurança da informação nas organizações de acordo com seu resultado financeiro (adaptado de ITPCG, 2010, p. 3 e 4. Tradução livre do autor).

organizações com melhores resultados (10%)	organizações com resultados normais (70%)	organizações com piores resultados (20%)
a segurança da informação se reporta ao <i>Chief Risk Officer</i> (CRO) ou gestor de controle interno	a segurança da informação se reporta ao <i>Chief Information Officer</i> (CIO), ou ao vice presidente de operações de TI	a segurança da informação se reporta ao vice presidente de operações de TI, ou ao <i>Chief Financial Officer</i> (CFO)
o gestor da segurança da informação é um <i>Chief Information Security Officer</i> (CISO) ou gerente sênior de TI	o gestor da segurança da informação é um <i>Chief Security Officer</i> (CSO), um gerente ou um diretor de TI	o gestor da segurança da informação é uma pessoa de administração de sistemas ou redes
a equipe de TI gerencia normas de integridade, disponibilidade e confidencialidade das informações	um conselho legal gerencia normas de integridade, disponibilidade e confidencialidade das informações	áreas de negócio gerenciam normas de integridade, disponibilidade e confidencialidade das informações
produtividade e segurança são gerenciadas por políticas e metas para uma indisponibilidade mínima e máximo de riscos aceitáveis	políticas e metas para uma indisponibilidade mínima e máximo de riscos aceitáveis não são implementadas	políticas e metas para uma indisponibilidade mínima e máximo de riscos aceitáveis não são implementadas
procedimentos e controle normatizados estão implementados	uma mistura de controles e procedimentos especialmente selecionados e criados caso a caso é implementada	procedimentos e controle normatizados não são implementados
políticas, procedimentos e controles estão perto de serem totalmente automatizados	uma mistura de controles e procedimentos manuais e automatizados é utilizada	basicamente procedimentos e controles manuais são utilizados
verificações e reportes de riscos e controles ocorrem diariamente, semanalmente e mensalmente	verificações e reportes ocorrem trimestral ou semestralmente	verificações e reportes ocorrem a cada nove meses ou anualmente

O estudo apresenta duas importantes constatações sobre a estrutura relacionada à função de gestão da segurança da informação (ITPCG, 2010, p. 7. Tradução livre do autor):

- a) Os piores resultados ocorrem entre organizações que gerenciam a segurança da informação em níveis mais baixos, dentro das operações de TI;
- b) Os melhores resultados ocorrem entre organizações que gerenciam a segurança da informação fora da área de TI, por um CISO ou um gerente sênior do controle da qualidade da informação de TI.

O gráfico 1 apresenta a distribuição percentual dos cargos do responsável pela gestão da segurança da informação nas organizações participantes. O gráfico 2 apresenta a distribuição das organizações participantes por resultado de acordo com o cargo do responsável pela gestão da segurança da informação.

Gráfico 1. Percentual dos cargos dos responsáveis pela segurança da informação (adaptado de ITPCG, 2010 p. 7. Tradução livre do autor)

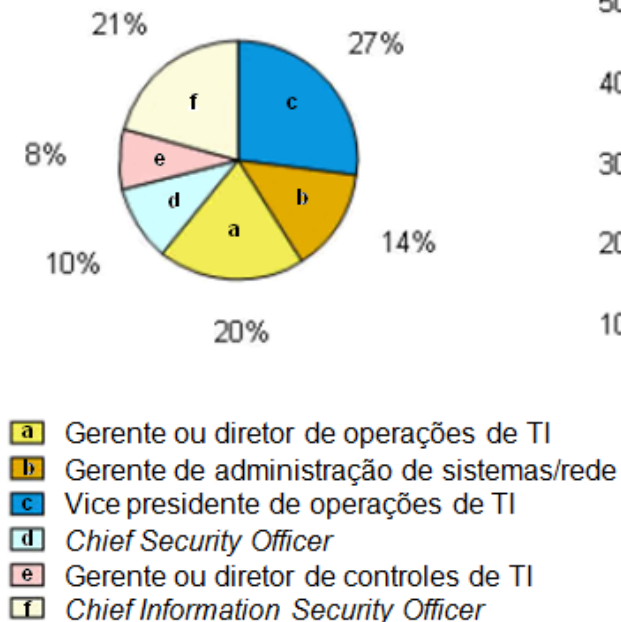
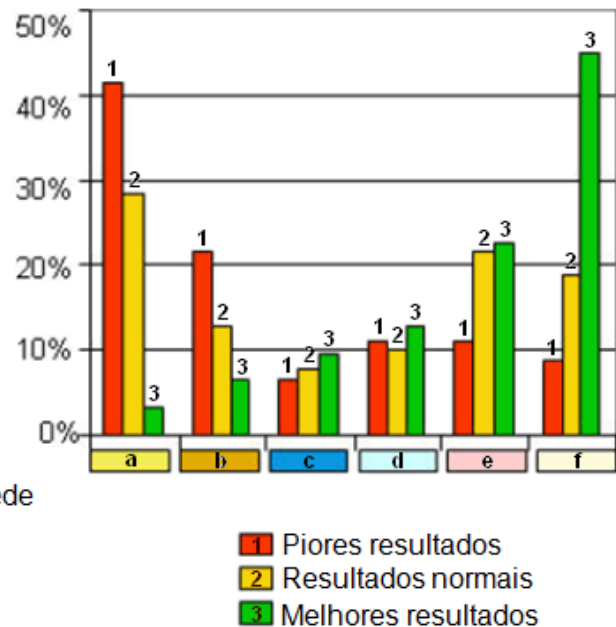


Gráfico 2. Resultados das organizações por cargo do responsável pela segurança da informação (adaptado de ITPCG, 2010 p. 7. Tradução livre do autor)



2.1.3. Cuidados na implementação da gestão da segurança da informação

Muitos erros são praticados quando se pensa em segurança da informação. Muitas pessoas percebem os aspectos da segurança considerando e enxergando apenas os riscos e problemas associados à tecnologia - internet, redes, computadores, vírus e hackers (SÊMOLA, 2003, p. 20).

Em função desse entendimento míope, Sêmola (2003, p. 20) relaciona alguns “pecados” cometidos que refletem negativamente nos negócios:

- Atribuir exclusivamente à área tecnológica a segurança da informação.
- Posicionar hierarquicamente essa equipe debaixo da diretoria de TI.
- Definir investimentos subestimados e limitados à abrangência dessa diretoria.
- Elaborar planos de ação orientados à reatividade.
[...]
- Não cultivar corporativamente a mentalidade de segurança.
- Tratar a segurança como um projeto e não como um processo.

Para que sejam efetivos, os controles de segurança frequentemente dependem do adequado funcionamento de outros controles. Se apropriadamente escolhidos, controles gerenciais, operacionais e técnicos podem trabalhar juntos, em sinergia. Caso não haja uma clara compreensão da interdependência dos controles de segurança, eles poderão, na verdade, prejudicar uns aos outros (NIST *Handbook*, 2005, p. 13).

Acrescenta-se a este fato a constatação dada pelo ITPCG (2010, p. 7. Tradução do autor):

Uma abordagem gerencial comum para segurança da informação - que segurança é somente um assunto de tecnologia - pode ser a raiz do problema das organizações que apresentam as maiores taxas de perda e roubo de informação. Estas organizações gerenciam a função profundamente dentro das estruturas de operações de TI, com menos visão e controle gerencial. As constatações mostram que as organizações com mais sucesso estão gerenciando a segurança da informação em níveis mais altos, tal como uma função de controle qualificada que inclui e vai além das tecnologias envolvidas.

Quando as atividades de segurança da informação são avaliadas contra os resultados das organizações, surge uma imagem bastante expressiva do impacto da estrutura organizacional nos seus resultados.

A figura 3 mostra uma clara distinção nos resultados - por diferentes atividades de gerenciamento - para a subordinação das equipes às áreas de operações de TI, ao gerente de segurança de TI ou ao CISO (ITPCG, 2010, p. 12). Os resultados da pesquisa demonstram que:

- Entre as organizações com piores resultados financeiros a maioria das atividades de gerência ligadas à segurança da informação são realizadas por uma equipe que se reporta à estrutura operacional de TI;
- Entre as organizações com resultados financeiros normais, ou medianos, maioria das atividades de gerência ligadas à segurança da informação são realizadas por uma equipe que se reporta ao gerente de segurança de TI; e
- Entre as organizações com os melhores resultados financeiros a maioria das atividades de gerência ligadas à segurança da informação são realizadas por uma equipe que se reporta ao gerente de segurança da informação.

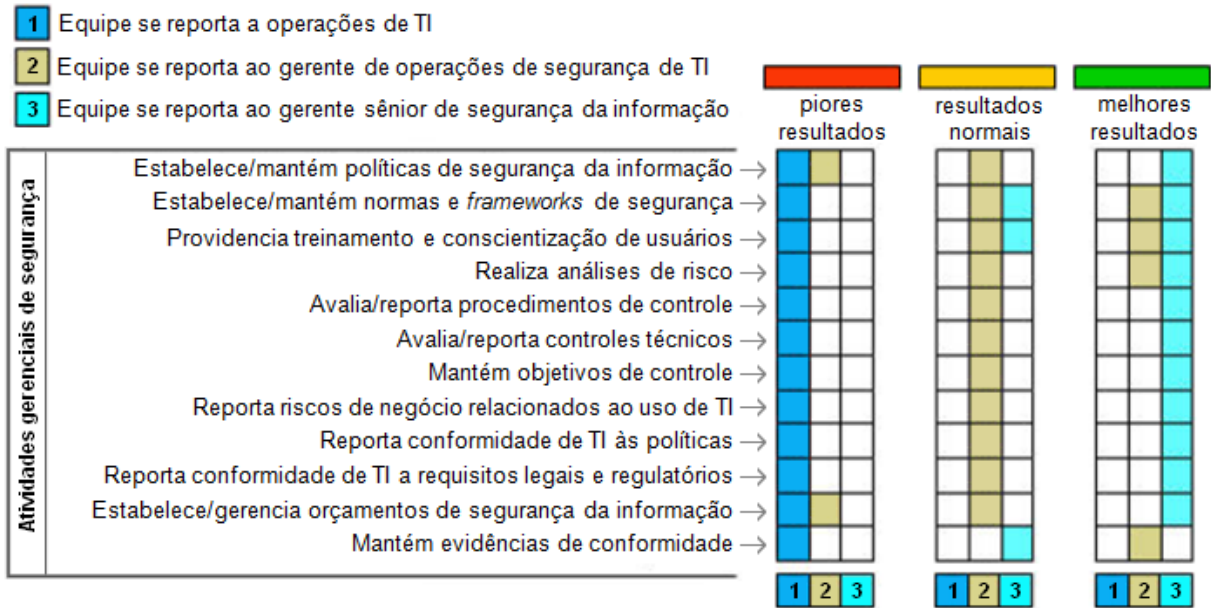


Figura 3. Posicionamento da gestão da segurança da informação de acordo com os resultados das organizações (adaptada de ITPCG, 2010, p. 12).

Pinheiro (2010) afirma que não apenas é necessária a formação de um comitê multidisciplinar de segurança da informação, mas a área de segurança da informação também deve possuir autonomia, desmembrada da área de TI e se reportando diretamente a alta-direção, visto que é uma área de gestão de riscos e controles (inclusive com alçada sobre a TI).

Com base nas colocações de Sêmola (2003, p. 20), NIST (2005), Pinheiro (2010) e nos resultados apresentados pela pesquisa realizada pelo ITPCG (2010), fica claro que dois importantes pontos de cuidado na implantação da gestão da segurança da informação são conferir-lhe alto nível de especialização e posicioná-la na organização de modo que tenha autonomia e uma visão integrada de todos os processos de negócio da organização e que se reporte às estruturas mais altas de decisão.

2.2. Principais normas técnicas relacionadas à segurança da informação

O conceito de segurança é, em essência, bastante abstrato. O fato de uma organização estar segura não impede que sofra incidentes e, por outro lado, a insegurança não é garantia de que haja problemas, apesar de existir uma maior probabilidade de que eles ocorram. A forma que uma organização considera adequada para gerenciar a segurança das suas informações

pode não ser a melhor maneira na opinião de outras pessoas ou organizações (RAMOS, 2006, p. 38).

Com o objetivo de diminuir ou mesmo evitar esta subjetividade, na execução deste trabalho foram utilizadas normas técnicas adotadas internacionalmente por organizações que buscam um direcionamento para as suas iniciativas de segurança.

As principais referências normativas para este trabalho são as normas da “família 27000” da *International Organization for Standardization* (ISO), específicas para gestão da segurança da informação, e traduzidas pela Associação Brasileira de Normas Técnicas⁶ (ABNT).

As organizações brasileiras não são legalmente obrigadas a seguir normas técnicas de segurança da informação. Contudo, uma norma técnica regulamenta boas práticas de forma unificada e consensada internacionalmente. Ao segui-la, caso a organização sofra algum incidente, poderá alegar que fez tudo o que estava ao seu alcance para evitá-lo, visto que pratica recomendações internacionais (PINHEIRO; SLEIMAN, 2009, P. 27).

Ainda, a norma técnica embasa as recomendações de segurança, inclusive aumentando a força da argumentação daqueles que necessitam implementá-las junto aos gestores do negócio (RAMOS, 2006, p. 38).

Deve-se salientar, contudo, que a aplicação de normas técnicas por uma organização deve ser realizada criteriosamente de acordo com o seu tamanho, necessidades, objetivos, riscos e demais requisitos de segurança.

A conformidade com uma norma técnica, por si só, não confere imunidade à organização em relação às suas obrigações legais (ABNT NBR ISO/IEC 27001, 2006, p. 1).

As principais normas da família 27000 utilizadas neste trabalho são apresentadas a seguir. A exata proporção dos controles aplicáveis é específica para cada organização e deveria ser definida através da análise dos riscos aos seus objetivos e atividades de negócios.

2.2.1. ABNT NBR ISO/IEC 27001:2006

A norma 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, elaborada pelo *Join Technical Committee Information Technology*. A

⁶ A ABNT (Associação Brasileira de Normas Técnicas) é o Fórum Nacional de Normalização e participa da elaboração das normas ISO da família 27000, enviando sugestões e traduzindo as normas para a língua portuguesa.

ISO/IEC 27001, por sua vez, tem sua origem ligada ao padrão britânico BS7799, com suas normas publicadas pelo *British Standards Institution* (BSI).

O objetivo da norma é “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, p. v).

Esta norma pode ser utilizada para avaliar a conformidade das partes interessadas internas e externas, e para a certificação e acreditação das práticas de gestão da segurança da informação de uma organização - é a parte “auditável” da família 27000.

Em sintonia com os padrões adotados pela norma de qualidade ISO9000, esta norma adota o modelo *Plan-Do-Check-Act* (PDCA), aplicado para estruturar todos os processos do SGSI. Este alinhamento sustenta a implementação e operação do SGSI de forma consistente e integrada com normas de gestão relacionadas, como a ISO 9001 e ISO 14001, de modo a satisfazer os seus requisitos.

A figura 4 ilustra como um SGSI considera as entradas de requisitos de segurança da informação e as expectativas das partes interessadas.

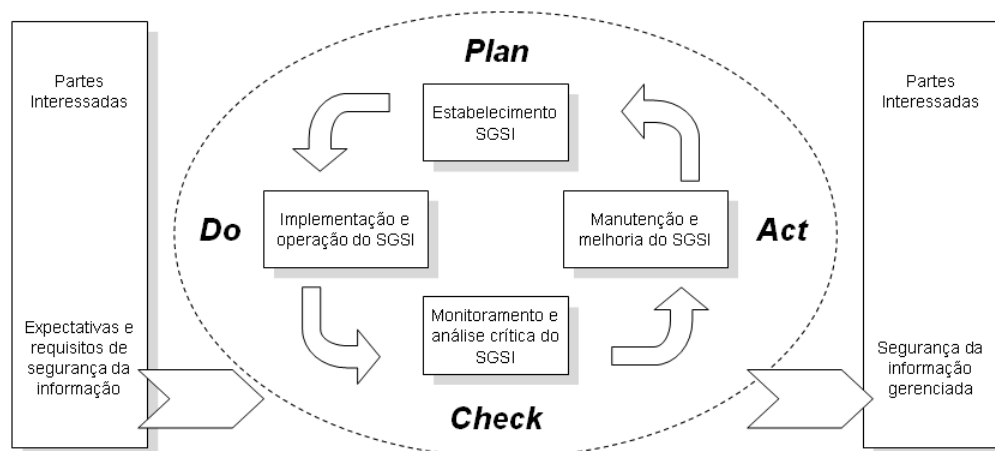


Figura 4. Modelo PDCA aplicado aos processos do SGSI
(adaptado de ABNT NBR ISO/IEC 27001, 2006 p. vi).

A tabela 4 apresenta uma descrição das fases do ciclo aplicado ao SGSI.

Tabela 4. Descritivo das fases do modelo PDCA aplicado ao SGSI
(ABNT NBR ISO/IEC 27001, 2006 p. vi).

Plan (planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

A adoção do modelo PDCA pela norma também reflete os princípios definidos nas diretrizes da *Organization for Economic Co-operation and Development*⁷ (OECD) para governar a segurança de sistemas de informação e redes (ABNT NBR ISO/IEC 27001, 2006 p. v).

Esta norma representa uma trilha que orienta as organizações dispostas a se organizarem para gerir os riscos de segurança da informação. Por esse motivo, limita-se a indicar o que deve ser feito, sem dizer como fazê-lo (SÊMOLA, 2003, p. 142).

Segundo a própria ABNT NBR ISO/IEC 27001 (2006, p. 2), para a sua aplicação é indispensável a utilização da norma ABNT NBR ISO/IEC 27002, na sua versão mais recente. A versão publicada em 2005 é apresentada a seguir.

Este trabalho irá abordar, basicamente, as fases *plan* e *check* do ciclo, pois apresenta um modelo para avaliação e melhoria dos controles de segurança da informação implementados na organização.

2.2.2. ABNT NBR ISO/IEC 27002:2005

A norma 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 (PINHEIRO; SLEIMAN, 2009, P. 27).

⁷ Diretrizes da *Organisation for Economic Co-operation and Development* (OECD) para a Segurança de Sistemas de Informação e Redes - Para uma Cultura de Segurança. Paris: OECD, 2002. <http://www.oecd.org>

A norma é equivalente à ISO/IEC 27002:2005 e apresenta uma abordagem multidisciplinar para a 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 de uma organização, através da definição de controles que podem ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. A norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização (ABNT NBR ISO/IEC 27002:2005, 2007, p.1).

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 pela norma 133 controles específicos relacionados à segurança da informação que podem ser implementados por uma organização.

As categorias principais da norma apresentam um objetivo de controle, que define o que deveria ser alcançado pela organização, e um ou mais controles que podem ser aplicados para que o objetivo de controle seja alcançado. Os controles apresentam uma definição geral, diretrizes com informações detalhadas para apoiar a implementação, e informações adicionais que podem ser consideradas (referências a outras normas e considerações gerais acerca do controle).

Devido a importância desta norma para o modelo de avaliação apresentado neste trabalho, relacionam-se abaixo as 11 seções da norma (ABNT NBR ISO/IEC 27002:2005, 2007, p.4):

- a) Política de Segurança da Informação;
- b) Organização da Segurança da Informação;
- c) Gestão de Ativos;
- d) Segurança em Recursos Humanos;
- e) Segurança Física e do Ambiente;
- f) Gestão das Operações e Comunicações;
- g) Controle de Acesso;
- h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- i) Gestão de Incidentes de Segurança da Informação;
- j) Gestão da Continuidade do Negócio;
- k) Conformidade.

2.2.3. ABNT NBR ISO/IEC 27004:2010

A norma ABNT NBR ISO/IEC 27004:2010 - Tecnologia da informação - Técnicas de Segurança - Gestão da segurança da informação - Medição - apresenta diretrizes para a elaboração e uso de métricas e medições, a fim de avaliar a eficácia do SGSI e dos controles apresentados na ABNT NBR ISO/IEC 27001. A adoção de medições de segurança da informação apoia a gestão na identificação e avaliação de processos e controles do SGSI ineficazes e não conformes, e na priorização de ações associadas com a melhoria ou modificação desses processos e/ou controles. Também pode auxiliar a organização a prover evidências adicionais para os processos de análise crítica e de gestão de riscos com a segurança da informação (ABNT NBR ISO/IEC 27004, 2010, p. vi).

A ABNT NBR ISO/IEC 27001 exige que a organização realize, regularmente, análises críticas da eficácia do SGSI (seção 7 - Análise crítica do SGSI pela direção), e defina como medir a eficácia dos controles implementados, para verificar se os objetivos definidos para a segurança da informação estão sendo alcançados.

Desta forma, organizações que, em virtude de constatações baseadas no risco a que estão submetidas, necessitem medir a eficácia dos controles de segurança da informação aplicáveis ao negócio, poderão encontrar na ABNT NBR ISO/IEC 27004 uma base para documentar as medições e gerar indicadores de conformidade dos controles com os seus objetivos, alcançando níveis mais altos de maturidade nos processos relacionados.

2.3. Gerenciamento do Risco

Os desafios da segurança da informação aumentam diariamente e o grande número de problemas e de vulnerabilidades que precisam ser gerenciados demandam recursos por parte das organizações (RAMOS, 2006, p.9. In: PREFÁCIO).

Muitas leis e regulamentações têm surgido para tentar obrigar as organizações a dar a devida atenção à segurança da informação, o que gerou outro problema: um número excessivo de regulamentações que se sobrepõem criando uma situação desnecessária de sobrecarga de trabalho para as organizações. Esta situação gera o questionamento, por parte das organizações, da efetividade das regulamentações, ou seja, até que ponto elas realmente conseguirão melhorar a segurança da informação e se há uma razoabilidade na relação custo/benefício dos investimentos sugeridos (RAMOS, 2006, p. 36).

A norma ABNT NBR ISO/IEC 27002:2005 não é perfeita e prevê que as organizações possam ter a necessidade de utilizar mais controles, além dos que ela recomenda. Por esse motivo o documento deve ser utilizado com uma postura crítica de modo a validar as suas proposições para o que é adequado ao negócio (RAMOS, 2006, p. 39).

Uma das explicações para o fato de que segurança total é inalcançável, é que segurança necessita de investimento, e não se investe mais do que o valor do ativo que está sendo protegido (RAMOS, 2006, p. 22).

Para que os investimentos possam ser focados nas áreas problemáticas mais críticas, princípios de gestão de riscos devem ser aplicados para que sejam priorizados os riscos mais importantes e sejam selecionadas as proteções adequadas (RAMOS, 2006, p.9 In: PREFÁCIO).

Todas as atividades de uma organização envolvem risco. Esses riscos precisam ser identificados, analisados e avaliados para estabelecer se será necessário o seu tratamento, de acordo com os critérios de risco e com o apetite de risco da organização. A ABNT ISO GUIA 73 (2009, p.3 e 6) define “critérios de risco” como sendo os termos de referência contra os quais a significância de um risco é avaliada, e “apetite de risco” a quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir.

É justamente esta análise crítica que irá determinar a necessidade de mudanças e a priorização destas de acordo com requisitos a serem cumpridos, necessidade de investimento e características da organização - tecnológicas, de processos de negócio, normativas, capacitação de recursos humanos e culturais.

De acordo com a norma ABNT NBR ISO 31000 (2009, p. 7):

A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho referente, por exemplo, à segurança e saúde das pessoas, à segurança, à conformidade legal e regulatória, [...], ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação. [...] A gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação. [...] Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.

2.3.1. ABNT ISO GUIA 73:2009

Este guia cancela e substitui a ABNT ISO/IEC GUIA 73:2005, e é uma adoção do ISO GUIDE 73:2009, que foi elaborado pelo ISO *Technical Management Board Working Group on Risk Management* (ABNT ISO GUIA 73, 2009, p. iv).

O ABNT ISO GUIA 73 fornece o vocabulário básico para um entendimento comum sobre os conceitos da gestão de riscos entre organizações e entre funções que gerenciam riscos de maneira integrada, de forma a evitar que os termos relativos à gestão de riscos sejam mal interpretados, deturpados ou mal utilizados (ABNT ISO GUIA 73, 2009, p. v).

2.3.2. ABNT NBR ISO 31000:2009

Esta norma é uma adoção idêntica à ISO 31000:2009, que foi elaborada pelo ISO *Technical Management Board Working Group on Risk Management* (ABNT NBR ISO 31000, 2009, p. iv).

A ABNT NBR ISO 31000 fornece princípios genéricos para a gestão de riscos de uma organização, pública ou privada, podendo ser utilizada nas diversas áreas que tenham a responsabilidade de gerir riscos. A norma pode ser utilizada para harmonizar os processos de gestão de riscos, tanto em normas atuais quanto em futuras, através da adoção de uma abordagem comum entre as normas que tratem de riscos específicos⁸. Não é objetivo desta norma promover uniformização para gerenciamento de riscos entre as organizações, pois os planos e estruturas para gestão de riscos devem levar em consideração as necessidades específicas de cada organização, de acordo com a sua estrutura, objetivos e práticas realizadas (ABNT NBR ISO 31000, 2009, p. 1).

A norma ABNT NBR ISO 31000 (2009, p. 8) determina que, para que uma gestão de riscos seja eficaz, convém que os seguintes princípios sejam atendidos pela organização:

- a) A gestão de riscos cria e protege valor; [...]
- b) A gestão de riscos é parte integrante de todos os processos organizacionais; [...]
- c) A gestão de riscos é parte da tomada de decisões; [...]
- d) A gestão de riscos aborda explicitamente a incerteza; [...]
- e) A gestão de riscos é sistemática, estruturada e oportuna; [...]
- f) A gestão de riscos baseia-se nas melhores informações disponíveis; [...]
- g) A gestão de riscos é feita sob medida; [...]
- h) A gestão de riscos considera fatores humanos e culturais; [...]
- i) A gestão de riscos é transparente e inclusiva; [...]
- j) A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças; [...]
- k) A gestão de riscos facilita a melhoria contínua da organização.

⁸ Um exemplo é a ABNT NBR ISO/IEC 27005, para a gestão de riscos de segurança da informação.

A norma determina, também, algumas opções para o tratamento dos riscos (ABNT NBR ISO 31000, 2009, p. 19):

- a) ação de evitar o risco ao se decidir não iniciar ou descontinuar a atividade que dá origem ao risco;
- b) tomada ou aumento do risco na tentativa de tirar proveito de uma oportunidade;
- c) remoção da fonte de risco;
- d) alteração da probabilidade;
- e) alteração das consequências;
- f) compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e
- g) retenção⁹ do risco por uma decisão consciente e bem embasada.

A figura 5 apresenta uma visão esquemática do processo de gestão de riscos de acordo com a ABNT NBR ISO 31000, 2009.

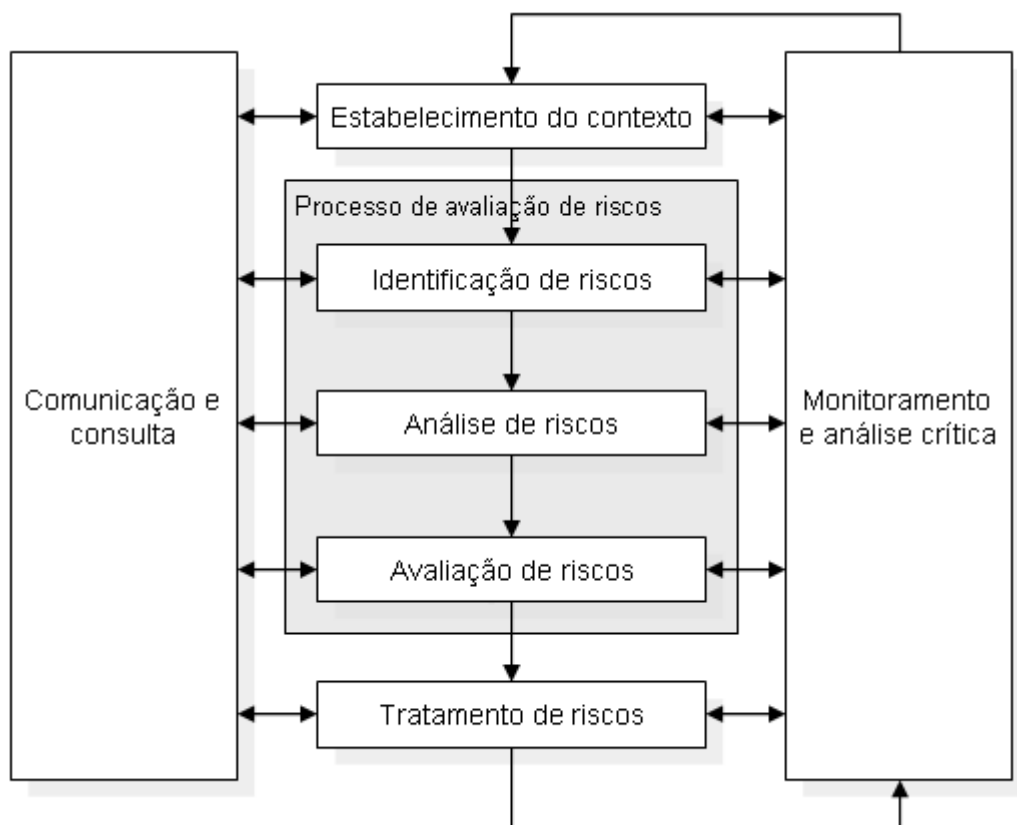


Figura 5. Processo de gestão de riscos (adaptado de ABNT NBR ISO 3100, 2009 p. 14).

⁹ A Norma ABNT NBR ISO/IEC 27001 (2006, p. 5) utiliza o termo “aceitação do risco” em vez de “retenção do risco”.

2.3.3. ABNT NBR ISO/IEC 27005:2008

Esta norma é uma adoção idêntica à ISO/IEC 27005:2008, que foi elaborada pelo ISO *Technical Committee Information Technology* (ABNT NBR ISO/IEC 27005, 2008, p. v).

A ABNT NBR ISO/IEC 27005 fornece as diretrizes para a avaliação de riscos da segurança da informação, de acordo com os conceitos especificados na ABNT NBR ISO/IEC 27001, para uma implementação da segurança da informação baseada na gestão de riscos e suas atividades (ABNT NBR ISO/IEC 27005, 2008, p. 1 a 3).

A ABNT NBR ISO/IEC 27005 (2008, p. 1) conceitua o termo “risco de segurança da informação” como sendo “a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização”.

A figura 6 apresenta uma visão esquemática do processo de gestão de riscos da segurança da informação de acordo com a ABNT NBR ISO/IEC 27005, 2008.

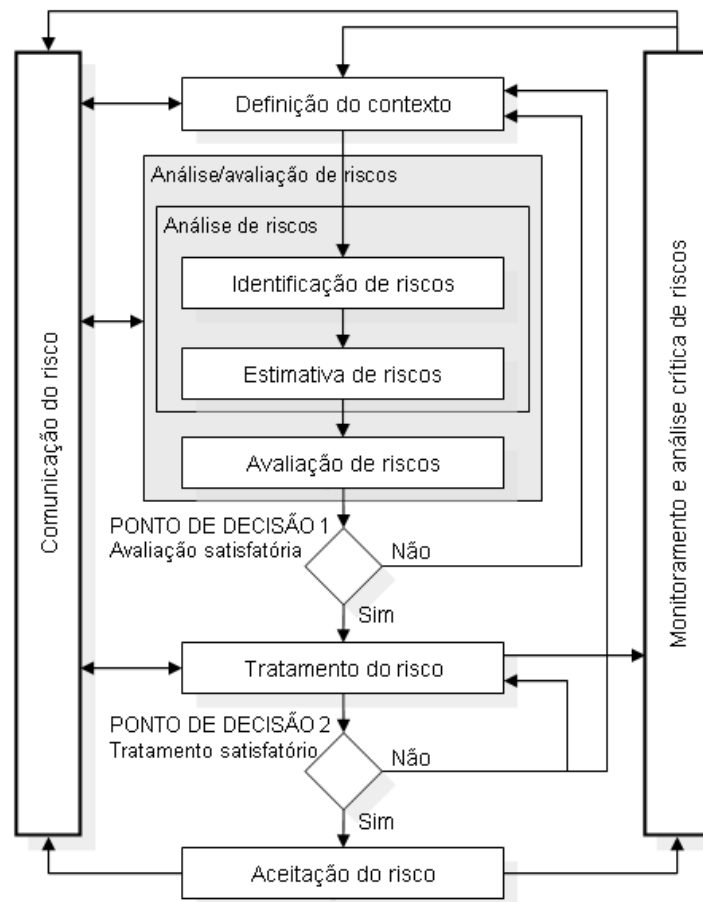


Figura 6. Processo de gestão de riscos de segurança da informação (adaptado de ABNT NBR ISO/IEC 27005, 2008 p. 5).

A norma apresenta as maneiras de tratamento¹⁰ dos riscos, cujas atividades estão ilustradas na figura 7.

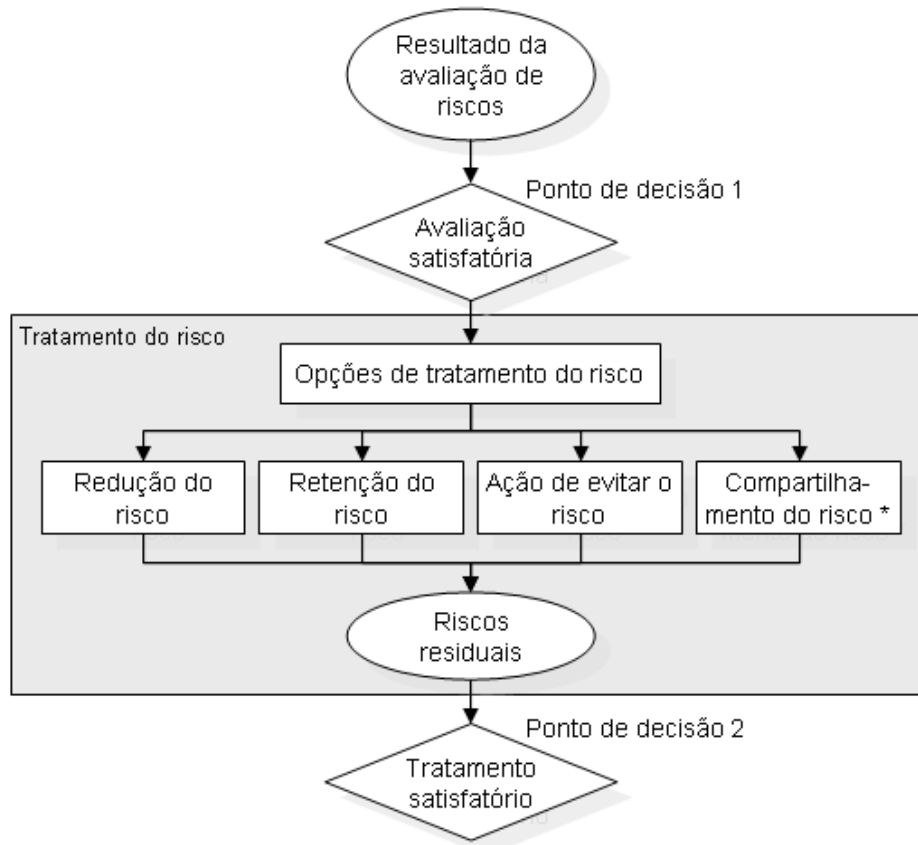


Figura 7. Atividades de tratamento dos riscos de segurança da informação (adaptado de ABNT NBR ISO/IEC 27005, 2008 p. 18 e de ABNT NBR ISO 31000, 2009, p. 19*).

Há uma diferença entre as Normas ABNT NBR ISO/IEC 27005 (2008, p. 17), ABNT NBR ISO 27001 (2006, p. 5) e ABNT ISO 31000 (2009) quanto à possibilidade de transferência do risco. A ABNT ISO 31000 (2009, p. 19) adequou o entendimento de que uma organização sempre será responsável pelos riscos ao seu negócio, podendo compartilhá-los com outras organizações, mas não transferi-los por completo (o termo transferência induz à ideia de que uma organização poderia tentar se isentar da responsabilidade da gestão do risco). A figura 7 foi adequada ao novo entendimento dado pela ABNT ISO 31000.

¹⁰ Tratamento de riscos: processo para modificar o risco (ABNT NBR ISO 31000, 2009, p.6).

2.4. Frameworks e melhores práticas relacionadas à segurança da informação

A segurança da informação é objeto de estudo e preocupação em diversos *frameworks* e conjuntos de melhores práticas para a governança corporativa, governança de TI e gestão de serviços de TI.

São relacionados abaixo os principais *frameworks* e conjuntos de melhores práticas relacionados à segurança da informação.

2.4.1. CobiT

A necessidade de garantia do valor da TI, o gerenciamento dos riscos relacionados à TI e a crescente necessidade de controles sobre as informações são compreendidas como aspectos chave da governança corporativa. Valor, risco e controle constituem o núcleo da governança de TI (ITGI, 2007, p. 8).

*Control Objectives for Information and related Technology (CobiT)*¹¹ é um conjunto de boas práticas obtidas através do consenso de experts, mais focadas 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 CobiT disponibiliza boas práticas para governança de TI, através de um ambiente de domínios e processos, e apresenta as atividades em uma estrutura lógica e gerenciável. A orientação a negócios do CobiT consiste em vincular objetivos de negócios aos objetivos de TI, provendo métricas e modelos de maturidade para medir o seu cumprimento e identificar as responsabilidades associadas a proprietários de processos de negócios e de TI. Para fornecer as informações que a organização necessita para alcançar os seus objetivos, os recursos de TI precisam ser gerenciados por um conjunto de processos naturalmente agrupados (ITGI, 2007, p. 8).

Segundo o CobiT, “a governança de TI é de responsabilidade de executivos e diretores, e consiste na liderança, estruturas organizacionais e de processos que garantam que a TI corporativa suporte e estenda as estratégias e objetivos da organização” (ITGI, 2007, p. 8).

¹¹ CobiT é uma marca registrada de ITGI – IT Governance Institute.

Para responder aos requisitos de governança de TI, e determinar e monitorar o nível apropriado de controle e desempenho de TI, o CobiT utiliza-se da medição da capacidade através de modelo de maturidade, derivado do CMM (*Software Engineering Institute's Capability Maturity Model*), o qual pode ser utilizado, também, para comparações entre organizações - *benchmark* (ITGI, 2007, p. 9).

O CobiT define um processo para a segurança dos sistemas de informação - *DS5 - Ensure Systems Security*. Este processo inclui a definição e manutenção de papéis, responsabilidades, políticas, normas e procedimentos de segurança de TI, com o objetivo de proteger todos os ativos de TI de maneira a minimizar o impacto ao negócio gerado por vulnerabilidades e incidentes de segurança (ITGI, 2009, p. 124).

O modelo de gestão da segurança da informação apresentado neste trabalho tem a sua base de medição suportada, assim como o CobiT, em modelos de maturidade. Utilizando-se de uma analogia entre a segurança de TI e a segurança da informação como um todo, o modelo de avaliação apresentado pretende dar subsídio para que o processo de gestão da segurança de informação possa atingir níveis mais altos de maturidade: 3 (Definido), ou 4 (Gerenciado).

A tabela 5 apresenta a descrição dos níveis de maturidade para o processo de gestão da segurança dos sistemas, de acordo com o CobiT.

Apesar de a TI estar diretamente ligada à segurança da informação, e constituir uma das maiores áreas de conhecimento a ser considerada na análise, a gestão da segurança da informação envolve muitas outras disciplinas, e não poderia ser suportada apenas na análise de controles e processos de TI.

O CobiT está focado em processos e indicadores para a governança de TI. Mesmo contendo indicadores relacionados à segurança de sistemas, o CobiT foi utilizado no presente trabalho como uma fonte de referência e não como fonte primária para construção sistemática do modelo de avaliação da segurança da informação. Esta abordagem poderia levar a uma visão subdimensionada dos riscos, objetivos de controle e controles específicos para a segurança da informação, mais apropriadamente especificados na ABNT NBR ISO/IEC 27002.

Tabela 5. Níveis de maturidade do processo de gestão da segurança dos sistemas - CobiT (adaptado de ITGI, 2007, p. 127. Tradução do autor).

Nível de Maturidade	Alcançado quando ...
0 – Inexistente	A organização não reconhece a necessidade de segurança de TI. Não foram designadas responsabilidades para garantia de segurança. Medidas de suporte e gerenciamento da segurança não foram implementadas. Existe uma completa falta de processos para a administração da segurança de sistemas.
1 – Inicial	A organização reconhece a necessidade de segurança de TI. As responsabilidades relacionadas à segurança não são claras. A conscientização da necessidade de segurança depende de uma iniciativa individual. A segurança de TI é tratada de maneira reativa. A segurança não é mensurada.
2 – Repetitivo	A responsabilidade pela segurança de TI é designada a um coordenador de segurança de TI, embora a autoridade gerencial do coordenador seja limitada. A conscientização da necessidade de segurança é fragmentada e limitada. Embora informações relacionadas à segurança de sistemas sejam produzidas, elas não são analisadas. Serviços de terceiros podem não levar em conta os requisitos de segurança da organização. Políticas de segurança estão sendo criadas, mas as competências e ferramentas são inadequadas. O reporte de segurança de TI é incompleto, equivocado ou não pertinente. Treinamentos de segurança estão disponíveis, mas sob iniciativa individual. A visão da segurança é primária e o negócio não a considera como um dos seus domínios.
3 – Definido	A conscientização de segurança existe e é promovida pela direção. Procedimentos de segurança de TI são definidos e alinhados à política de segurança de TI. Responsabilidades para a segurança de TI são definidas e compreendidas, mas não aplicadas consistentemente. Um plano de segurança de TI e soluções de segurança existem como resultado de uma análise de riscos. Relatórios de segurança não possuem um foco claro de negócios. Testes de segurança (ex. testes de penetração) são realizados individualmente, caso a caso. Treinamento de segurança está disponível para TI e para o negócio, mas é planejado e gerenciado informalmente.
4 – Gerenciado	As responsabilidades para a segurança de TI são claramente atribuídas, gerenciadas e reforçadas. A análise de risco e impacto da segurança de TI é realizada consistentemente. Políticas e procedimentos são complementados com linhas de base de segurança. A conscientização para a segurança é obrigatória. A identificação, autenticação e autorização de usuários são normatizadas. Certificação de segurança é perseguida por membros da equipe responsável pela gestão e auditoria de segurança. Testes de segurança são executados com o uso de normas e procedimentos formalizados. Os processos de segurança de TI são coordenados por uma função de segurança de nível organizacional. Os relatórios de segurança são vinculados aos objetivos de negócio. Treinamento de segurança é aplicado tanto para TI quanto para o negócio. Objetivos e métricas para a gestão da segurança foram definidos, mas ainda não são medidos.
5 – Otimizado	A segurança de TI é uma responsabilidade compartilhada entre os gestores do negócio e da TI, e integrada aos objetivos de segurança do negócio. Os requisitos de segurança de TI são claramente definidos, otimizados e incluídos em um plano de segurança aprovado. Incidentes de segurança são prontamente tratados por meio de procedimentos formais de resposta a incidentes suportados por ferramentas automatizadas. Avaliações de segurança são realizadas periodicamente para evidenciar a efetividade da implementação do plano de segurança. Informações sobre ameaças e vulnerabilidades são sistematicamente coletadas e analisadas. Os processos e tecnologias de segurança são integrados através da organização. Indicadores para a gestão da segurança são medidos, coletados e comunicados, e a gerência utiliza esses indicadores para ajustar continuamente o plano de segurança.

2.4.2. ITIL

A *IT Infrastructure Library* (ITIL) é uma série de livros considerada como sendo uma biblioteca consistente e abrangente de melhores práticas para o gerenciamento de serviços de TI, focada na entrega de serviços de TI de alta qualidade. O objetivo principal da biblioteca é o desenvolvimento de abordagens independentes de fabricantes para a gestão de serviços de TI. Embora seja produzida e publicada por uma única entidade governamental, a ITIL não é uma norma (ITGI, 2006. p. 21).

ITIL foi inicialmente publicada entre 1989 e 1995, pela HMSO (Her Majesty's Stationery Office), no Reino Unido, sob responsabilidade da CCTA (*Central Communications and Telecommunications Agency*), hoje submetida ao OGC (*Office of Government Commerce*). A segunda versão foi publicada entre 2000 e 2004, e a terceira em 2007 (ITSMF, 2007, p. 2 e 8).

Os principais processos de TI apresentados pelo ITIL relacionados à segurança da informação são os processos de suporte aos serviços (gestão de incidentes, gestão de problemas, gestão da configuração, gestão de mudanças e gestão de liberação) e de entrega de serviços (gestão da capacidade, gestão da disponibilidade e gestão da continuidade dos serviços de TI) (ITGI, 2006. p. 25).

Apesar de a gestão de serviços de TI estar diretamente ligada à segurança da informação, a gestão da segurança da informação envolve muitas outras disciplinas, e não poderia ser suportada apenas na análise de controles e processos de TI.

O ITIL está focado em melhores práticas para a entrega de serviços de TI. Mesmo contendo processos relacionados à segurança de TI, o ITIL não foi utilizado no presente trabalho como fonte de referência (a sugestão de como implementar os controles de segurança da informação não faz parte do escopo deste trabalho).

Organizações que necessitem alcançar níveis mais altos de maturidade para controles de segurança da informação relacionados ou suportados por processos e serviços de TI poderão encontrar na biblioteca ITIL uma importante fonte de referências e melhores práticas para basear a tomada de decisão e a estrutura dos seus processos.

3. O MODELO DE AVALIAÇÃO POR NÍVEIS DE MATURIDADE

Com base nas características da segurança da informação e nas principais normas técnicas relacionadas, procurou-se reunir no modelo de avaliação apresentado neste trabalho as seguintes características principais:

- a) Utilizar uma estrutura de processo de gestão que possibilite a avaliação e a melhoria contínuas da segurança da informação;
- b) Utilizar como base um conjunto específico e adequado de controles reconhecidos internacionalmente que tratem a segurança da informação de forma abrangente;
- c) Fornecer um meio para medir a situação atual da segurança da informação e a sua evolução ao longo do tempo;
- d) Fornecer subsídio para identificar ações de melhoria oportunas e viáveis, baseadas nos riscos e nas condições dos processos de negócio da organização.

A tabela 6 apresenta as principais características do modelo de avaliação e a forma como cada característica é suportada pelas normas apresentadas neste trabalho.

Tabela 6. Principais características do modelo de avaliação e seu relacionamento com as normas e modelos apresentados

Característica	Relacionamento
Avaliação e melhoria contínua	Utilização da ABNT NBR ISO/IEC 27001 para criação de um processo de avaliação e melhoria contínua da gestão da segurança da informação - ciclo PDCA.
Estrutura de controles apropriados	Utilização da ABNT NBR ISO/IEC 27002 como base para a especificação de controles de segurança da informação.
Medição e acompanhamento	Utilização do modelo de níveis de maturidade (CMM / CobiT) para medição e acompanhamento da evolução da segurança da informação.
Avaliação de riscos	Utilização das ABNT NBR ISO/IEC 27005 e ABNT NBR ISO 31000 para análise e avaliação de riscos, de acordo com as características e estratégias da organização.

O modelo apresentado neste trabalho tem como principais propósitos:

- a) Avaliar a segurança da informação de maneira abrangente, integrando as diversas áreas de controle da organização; e
- b) Fazer com que o foco da segurança da informação seja convenientemente convergido para um ponto em comum de acordo com os objetivos organizacionais.

3.1. Avaliação e melhoria contínua

Computadores e o ambiente no qual eles operam são dinâmicos. Os sistemas tecnológicos, usuários, dados nos sistemas, e os riscos associados a um sistema estão em constante mudança. Como consequência, os requisitos de segurança da informação são alterados constante e indefinidamente. Muitos tipos de mudanças alteram a segurança dos sistemas: desenvolvimento tecnológico, conexão a redes externas, alterações no valor da informação, ou mesmo o surgimento de uma nova ameaça. Em adição, a segurança nunca é perfeita quando um novo sistema é desenvolvido, e as mudanças nos ambientes e nos sistemas podem criar novas vulnerabilidades. Usuários do sistema e operadores descobrem novas maneiras de, intencionalmente ou não, driblar ou subverter os controles de segurança. A aderência aos procedimentos instituídos pela organização raramente é conseguida e os procedimentos se tornam desatualizados com o tempo (NIST – *NIST Handbook*, 2005, p. 13 e 14).

Esses fatores demonstram que se torna necessária a reavaliação periódica da segurança da informação, através de um processo cíclico de gestão que possa ser repetido e reavaliado de tempos em tempos.

O ciclo *Plan-Do-Check-Act* (PDCA), além de ser considerado o método mais geral para trabalhar com qualidade, pode condicionar a gestão das organizações a um ciclo lógico de melhorias contínuas para alcançar os resultados esperados. Um resultado é alcançado mais eficientemente quando as atividades e os recursos relacionados são gerenciados como processos que, quando identificados, compreendidos e gerenciados de forma inter-relacionada como um sistema, contribuem para a eficácia e eficiência da organização para alcançar os seus objetivos (MARANHÃO, 2001, p.11, 52 e 53).

3.1.1. Abordagem de processo

Sêmola (2003, p. 20) cita que tratar a segurança da informação como um projeto, e não como um processo, é uma das principais causas para o seu fracasso.

De acordo com a norma ABNT NBR ISO/IEC 27001 (2006, p. v), a abordagem de processo¹² para a gestão da segurança da informação encoraja que os usuários administradores do SGSI enfatizem a importância de:

- a) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;
- b) implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
- c) monitoração e análise crítica do desempenho e eficácia do SGSI; e
- d) melhoria contínua baseada em medições objetivas.

Segundo Hintz (2010), um processo é institucionalizado quando está “impregnado” na maneira como o trabalho é realizado, e existem comprometimento e consistência na sua realização. Um processo com essas características é mais provável de ser seguido e cumprido durante um período de *stress* na organização.

3.2. Controles de segurança da informação

O modelo de avaliação apresentado neste trabalho utiliza a estrutura de objetivos de controle e controles da norma ABNT NBR ISO/IEC 27002, internacionalmente reconhecidos por serem adequados à gestão da segurança da informação. A versão utilizada, de 2005, define 133 controles que poderão ser avaliados através do modelo apresentado.

Para cada controle sugerido pela norma que for considerado aplicável à organização será realizada uma avaliação de conformidade com as necessidades do negócio, fazendo-se uso de um método de medição para o registro da avaliação.

Cabe salientar que a estrutura da norma, apesar de ser abrangente, pode não conter todos os controles necessários aos diversos tipos de organizações, e poderá ser necessária a avaliação de controles adicionais que suportem os riscos, objetivos ou requisitos específicos aos quais a organização estiver submetida e necessite estar em conformidade.

3.3. Medição e Acompanhamento

A grande quantidade e variedade de objetivos de controle e controles aplicáveis à segurança da informação tornam a sua gestão um processo complexo. Os níveis de

¹² A aplicação de um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos e sua gestão podem ser consideradas como “abordagem de processo” (ABNT ISO/IEC 27001, 2006, p. v).

desenvolvimento dos processos, das tecnologias e dos recursos humanos de uma organização são diferentes entre si, principalmente se consideradas as diversas áreas de conhecimento envolvidas e as diferentes velocidades com que se desenvolvem em função dos objetivos específicos de cada área. Dentro da organização os processos e controles relacionados à segurança da informação estão mais ou menos desenvolvidos com relação aos demais processos e controles do negócio. Torna-se necessário, então, identificar as lacunas, analisar as diferenças e avaliar a necessidade de medidas corretivas.

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

3.3.1. *Capability Maturity Model - CMM*

A avaliação dos processos de acordo com um modelo de maturidade é atividade chave para implementação de governança. Após identificar processos e controles críticos, o uso de um modelo de maturidade permite a análise para identificação de lacunas que representam risco e a sua demonstração à administração. Com base nessa análise poderão ser avaliados e desenvolvidos planos para melhoria dos processos e controles considerados deficientes até o nível de desenvolvimento desejado. A medição por níveis de maturidade, além de dar transparência ao processo de gestão, permite realizar comparações entre ciclos de avaliação e mesmo entre organizações - *benchmark* (ITGI, 2007, p. 9). Esta abordagem insere o fator temporal no processo de gestão da segurança da informação.

A abordagem por níveis de maturidade adotada neste trabalho deriva do modelo de níveis de maturidade criado pela SEI (*Software Engineering Institute*), para medição da maturidade do processo de desenvolvimento de *softwares*.

Embora os conceitos definidos pela SEI tenham sido seguidos, os níveis de maturidade utilizados seguiram os conceitos definidos pelo CobiT (*Control Objectives for Information and Related Technology*), apresentado neste trabalho, e que diferem consideravelmente do modelo original. A escala do modelo original criado pela SEI era orientada a princípios de engenharia de produtos de *software*, enquanto a escala de maturidade do modelo CobiT apresenta definições genéricas para a gestão de processos.

Outra importante diferença é que as escalas do CobiT não foram criadas para servir como um modelo de barreiras, onde não se poderia mover ao próximo nível de maturidade sem que fossem cumpridas todas as exigências do nível anterior (ITGI, 2007, p. 17), permitindo maior flexibilidade à gestão do sistema de avaliação e à gestão dos controles e processos avaliados. Esta diferença pode ser considerada expressiva, principalmente nos casos em que seja necessário ter que se alcançar rapidamente um determinado nível de maturidade (por determinação legal, por exemplo).

A utilização do modelo de maturidade tem a vantagem de tornar relativamente fácil para a administração posicionar-se em uma escala e avaliar o que deveria ser feito no caso em que uma melhoria fosse considerada necessária. A escala de seis níveis é baseada 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. (ITGI, 2007, p. 18).

A figura 8 é uma representação gráfica para o modelo de níveis de maturidade utilizado pelo CobiT.

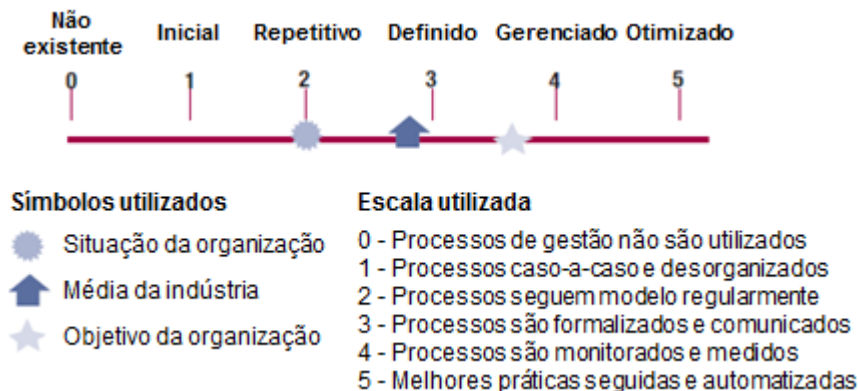


Figura 8. Representação gráfica do modelo de maturidade (adaptado de ITGI, 2007 p. 18).

Este trabalho foi baseado na escala do CobiT, com seis níveis de maturidade. A tabela 7 apresenta a escala utilizada e as respectivas características definidas para cada nível de maturidade.

Tabela 7. Escala de níveis de maturidade
(adaptado de ITGI, 2007, p. 19. Tradução livre do autor).

Nível	Características
Nível 0 Não-Existente	Completa falta de qualquer processo reconhecível. A organização ainda não reconheceu que há um risco a ser tratado.
Nível 1 Inicial	Existe uma evidência de que a organização reconheceu que o risco existe e precisa ser tratado. No entanto, não há qualquer processo padronizado; existem alguns processos aplicados caso-a-caso por iniciativas individuais.
Nível 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.
Nível 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.
Nível 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 de automação são utilizadas de maneira limitada e fragmentada.
Nível 5 Otimizado	Os processos foram refinados ao nível de melhores práticas, baseado no resultado de melhorias contínuas e de comparação da maturidade com outras organizações. A TI é utilizada de maneira integrada para automatizar os fluxos de trabalho, fornecendo ferramentas para melhorar a qualidade e efetividade, e tornando fácil para a organização se adaptar a mudanças.

A tabela 8 apresenta um exemplo de aplicação e interpretação da escala de maturidade para avaliação de controle sobre vírus de computador (código malicioso).

Tabela 8. Exemplo de aplicação e interpretação da escala de maturidade para avaliação do controle sobre vírus.

Nível	Características Encontradas
Nível 0 Não-Existente	A organização ainda não reconheceu que vírus existem e que há risco envolvido em decorrência da infecção dos seus equipamentos.
Nível 1 Inicial	As pessoas reconheceram que vírus existem e precisam ser evitados. Não há um processo padronizado, mas algumas pessoas utilizam antivírus individualmente.
Nível 2 Repetitivo	A organização sugere informalmente que as pessoas instalem antivírus nos equipamentos, mas deixa a instalação sob responsabilidade individual. Muitos equipamentos poderão permanecer desprotegidos indefinidamente.
Nível 3 Definido	É obrigatório por política formal da organização que procedimentos de instalação de antivírus sejam seguidos. Existe contrato para fornecimento do software e de atualizações de definições de vírus. Entretanto, não há verificação periódica da aplicação da política e da atualização dos antivírus nos equipamentos.
Nível 4 Gerenciado	Existem relatórios mensais de infecções por vírus e listas de equipamentos sem antivírus ou com antivírus desatualizado. Desvios detectados são documentados e levam à tomada de ações corretivas.
Nível 5 Otimizado	São utilizadas ferramentas de software que identificam periodicamente os equipamentos da organização sem antivírus e realizam a instalação ou atualização automaticamente, sem interferência ou dependência dos usuários.

3.4. Fases do ciclo de avaliação e melhoria contínua da segurança da informação

Uma métrica, ou indicador, por si só, não é a resposta para os problemas de segurança da informação de uma organização, pois não levam em conta o tempo, fator considerado relevante para o tipo de análise proposto. Além de medir a situação atual, deve existir ação sobre os problemas encontrados e o acompanhamento da evolução ao longo do tempo.

A figura 9 apresenta as oito fases que compõem o ciclo de avaliação da maturidade da segurança da informação.

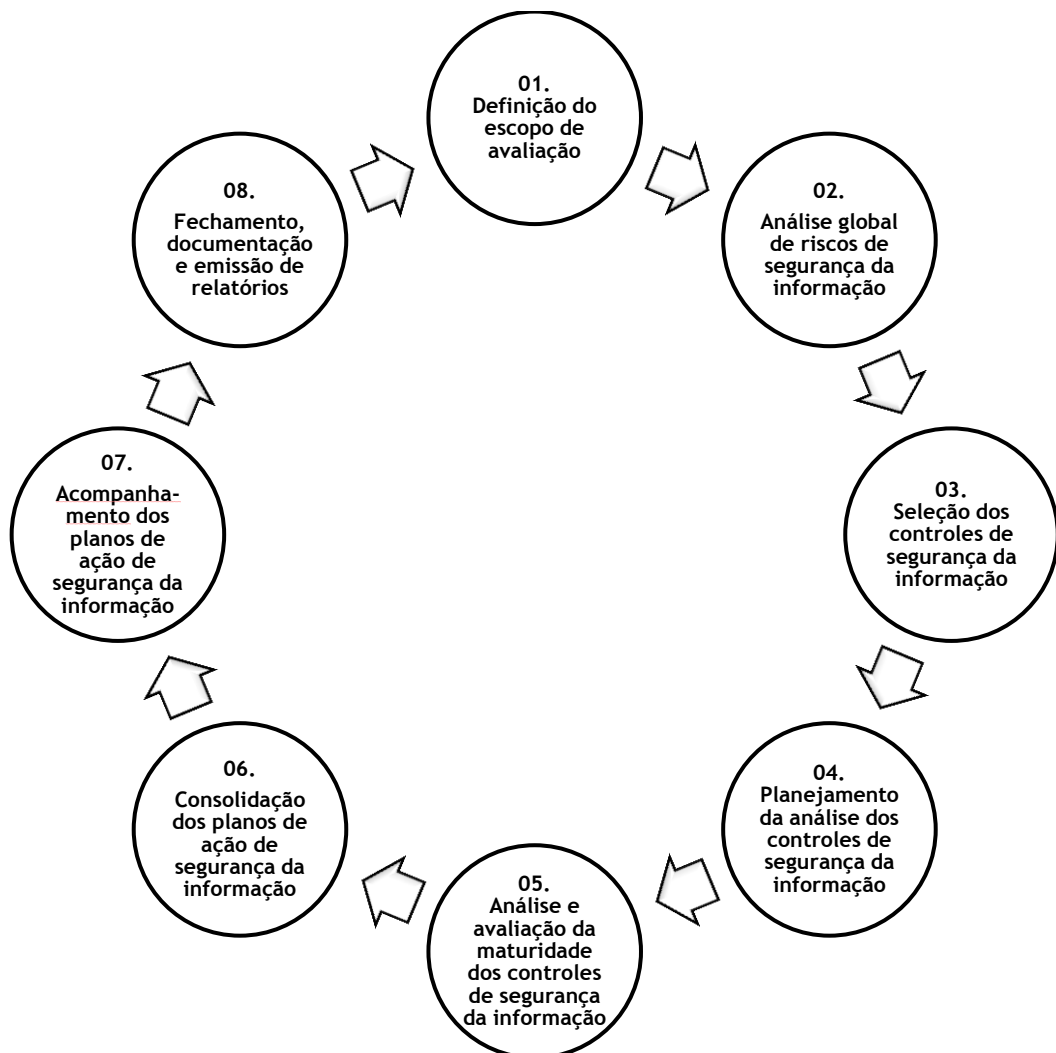


Figura 9. Fases do ciclo de avaliação e melhoria da segurança da informação

As principais atividades realizadas em cada fase do ciclo de avaliação e melhoria da segurança da informação são apresentadas a seguir.

3.4.1. Definição do escopo de avaliação

Nesta fase deve ser 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 mesmo estar geograficamente distribuída. Pode ser considerado conveniente dividir a avaliação da maturidade em partes, de acordo com as características específicas das atividades, unidades ou núcleos de especialização da organização.

A definição do escopo consiste em identificar as áreas, tecnologias e processos de negócio da organização que serão incluídos no processo de avaliação do nível de maturidade da segurança da informação. Esta fase do modelo pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 4), que orienta que o escopo e os limites do SGSI devem ser definidos “nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo”.

Na medida em que os ciclos de avaliação forem sendo executados, dentro dos intervalos de tempo definidos pela organização, esta fase também poderá ser utilizada para uma revisão crítica das etapas de avaliação da maturidade da segurança da informação. É razoável esperar que, com o tempo, possa haver alterações no escopo de avaliação em virtude de mudanças na legislação, estratégia, processos de negócios, tecnologia e quadro de pessoal da organização, que levem a mudanças do processo de avaliação. Esta avaliação crítica pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 11), que orienta:

A direção deve analisar criticamente o SGSI da organização a intervalos planejados (pelo menos uma vez por ano) para assegurar a sua contínua pertinência, adequação e eficácia. Esta análise crítica deve incluir a avaliação de oportunidades para melhoria e necessidade de mudanças no SGSI.

Caso haja alteração no escopo de avaliação ou no método de avaliação, as mudanças introduzidas e possíveis ações corretivas devem ser justificadas e documentadas.

3.4.2. Análise dos riscos relacionados à segurança da informação

Nesta fase a organização deve realizar a identificação global dos riscos relacionados à segurança das suas informações.

Esta fase é importante para garantir que os controles selecionados para análise estejam relacionados ao tratamento dos riscos aos quais a organização estiver submetida. Esta fase pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 8), que orienta que a documentação do SGSI deva conter “uma descrição da metodologia de análise/avaliação de riscos”.

A análise de riscos pode ser realizada em diferentes graus de detalhamento, dependendo da criticidade dos ativos e da extensão das vulnerabilidades. A metodologia de análise pode ser quantitativa, qualitativa ou uma combinação de ambas, dependendo das circunstâncias de avaliação e informações disponíveis para análise. A estimativa qualitativa é frequentemente utilizada em primeiro lugar, para que se obtenha uma indicação geral do nível de risco e para evidenciar grandes riscos. Normalmente é menos complexo e menos oneroso realizar análises qualitativas, que possuem a vantagem de serem mais facilmente compreendidas pelas pessoas envolvidas. As análises quantitativas poderão ser realizadas de maneira mais específica, para os grandes riscos, desde que se tenham disponíveis indicadores adequados que suportem a análise (ABNT NBR ISO/IEC 27005, 2008, p.14).

Este modelo utiliza um 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. Esta abordagem pode ser considerada suficiente para a identificação dos riscos e para suportar a decisão de escolha dos controles de segurança da informação a serem avaliados.

A figura 10 apresenta a escala utilizada para análise e classificação dos riscos relacionados à segurança da informação.

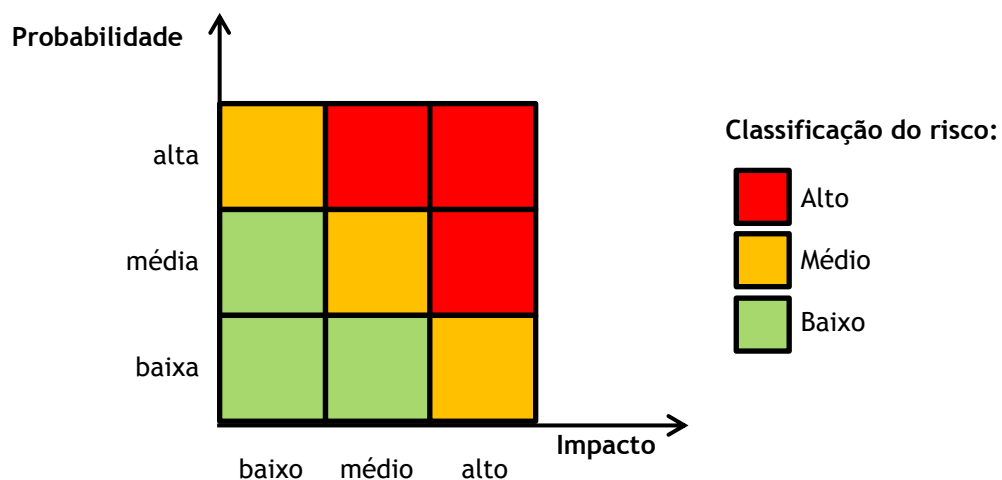


Figura 10. Escala para análise e classificação de riscos

Segundo a ABNT ISO GUIA 73 (2009, p.5 e 6) a análise do risco consiste no “processo de compreender a natureza do risco e determinar o nível de risco”. Nível de risco é a “magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades (*likelihood*)”. A avaliação do risco é o “processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou a sua magnitude é aceitável e tolerável”.

Cabe salientar que, de acordo com as normas ABNT NBR ISO/IEC 27005 (2008) e ABN NBR ISO 31000 (2009), esta fase representa a análise dos riscos, na qual os riscos são identificados e é realizada uma estimativa do impacto e probabilidade, levando a identificação do nível de risco inerente (risco sem considerar os controles envolvidos).

Nesta fase ainda não é possível concluir a avaliação do risco, pois os controles utilizados para o tratamento dos riscos identificados serão analisados na fase 5 do ciclo de avaliação - análise e avaliação da maturidade dos controles de segurança da informação.

3.4.3. Seleção dos controles de segurança da informação

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

Esta fase do modelo pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 6), que orienta que os “objetivos de controle e controles devem ser selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos [...]”, e que a organização deva preparar uma declaração de aplicabilidade, onde serão apresentados os objetivos de controle e controles selecionados a partir do anexo A da norma.

Apesar de o modelo apresentado utilizar a estrutura de controles da norma ABNT NBR ISO/IEC 27002 como base de avaliação, as organizações devem ser capazes de identificar outros controles pertinentes que devam ser avaliados, considerando, por exemplo, a análise dos riscos relacionados à segurança da informação, a análise dos riscos corporativos, a gestão da conformidade (*compliance*), outras fontes de requisitos legais ou regulamentares aplicáveis ao negócio, e melhores práticas adotadas no setor ao qual a organização estiver inserida.

3.4.4. Planejamento da análise dos controles de segurança da informação

Nesta fase deverá ser criado um projeto para o ciclo de análise e avaliação dos objetivos de controle considerados aplicáveis e suas respectivas atividades de controle. Esta fase tem por principais finalidades identificar e comprometer as partes envolvidas nas análises, identificar as partes interessadas, definir um cronograma para as atividades de avaliação, e criar um plano de comunicação para os resultados obtidos.

Esta fase do modelo pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 6), que orienta que a organização deve “obter autorização da direção para implementar e operar o SGSI”.

Esta fase não deve ser considerada como sendo um único projeto para avaliação da maturidade da segurança da informação, uma vez que está inserida no processo cíclico de avaliação e deve ser atualizada a cada ciclo.

3.4.5. Análise e avaliação da maturidade dos controles de segurança da informação

Nesta fase cada controle de segurança da informação selecionado deve ser avaliado, juntamente com os processos, atividades e controles relacionados, para determinar o nível de maturidade do controle de acordo com a escala de maturidade definida no modelo. O nível de maturidade de cada controle será comparado com a análise de riscos e, caso necessário, um plano de ação deve ser documentado para correção e/ou melhoria das atividades relacionadas.

Esta fase é dividida em cinco etapas que devem ser executadas para cada controle selecionado:

- 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 de segurança avaliado, apurar o nível de maturidade do controle de acordo com a escala de maturidade definida no modelo. Possivelmente

haverá diferentes atividades com níveis de maturidade distintos relacionados ao mesmo controle;

- c) **Avaliação da maturidade do controle:** nesta etapa será avaliado se a maturidade do controle de segurança, apurada pelo conjunto das atividades que o suportam, está de acordo com a maturidade necessária para tratar os riscos relacionados. São documentadas possíveis falhas no cumprimento dos controles, relacionando os problemas observados e, quando possível, relacionando sugestões de possíveis melhorias que poderiam ser implementadas;
- d) **Identificação de melhorias necessárias:** com base nas possíveis deficiências encontradas no cumprimento dos controles de segurança, nesta etapa serão documentadas as alterações e melhorias necessárias para as atividades relacionadas ao controle, ou mesmo a criação de novas atividades, para manter o nível de risco adequado de acordo com o apetite de risco da organização. As alterações devem ser propostas e documentadas em conjunto com os responsáveis pelos processos de negócio envolvidos;
- e) **Comunicação dos resultados aos responsáveis pelo controle:** nesta etapa os resultados da análise do controle de segurança avaliado são comunicados aos seus responsáveis, para que tomem conhecimento dos resultados e possam avaliar as ações necessárias e possíveis intervenções emergenciais.

Esta fase pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 7), que orienta que a organização deve “realizar análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica dos controles de segurança), [...]”.

A figura 11 apresenta um esquema com as etapas da análise e avaliação dos controles de segurança da informação e respectivas atividades de controle.



Figura 11. Etapas de análise e avaliação dos controles de segurança da informação

A figura 12 apresenta um esquema que ilustra a interação das etapas da análise do controle da segurança da informação com a escala de maturidade e as principais normas utilizadas.

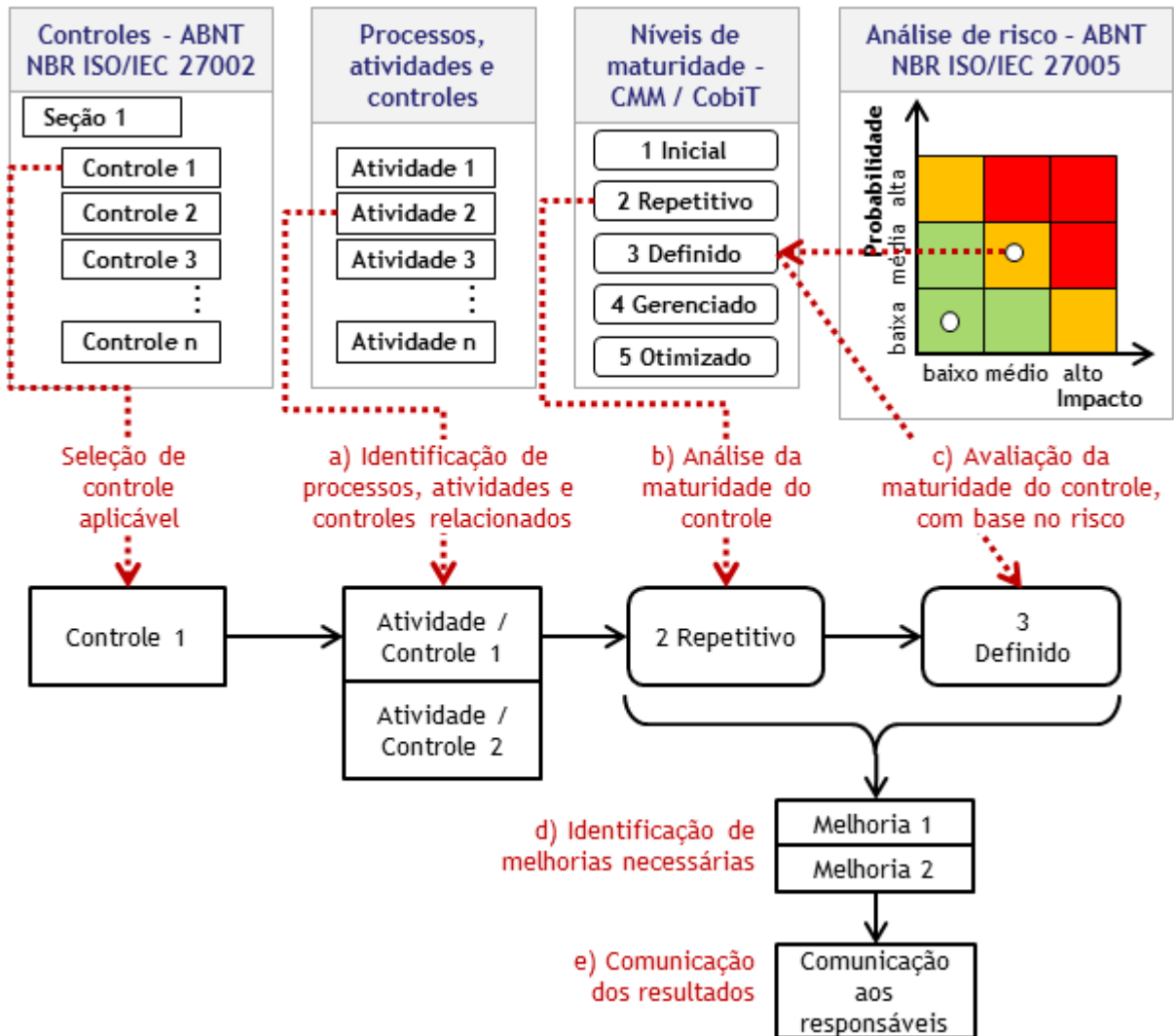


Figura 12. Interação das etapas de análise dos controles com a escala de maturidade e as normas utilizadas

3.4.6. Consolidação dos planos de ação de segurança da informação

É razoável esperar que diversos controles de segurança avaliados possam ter propostas de melhoria em comum, relacionadas ou mesmo interdependentes. Nesta fase todas as propostas de melhoria 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 propostas:** nesta etapa todas as melhorias propostas são analisadas em conjunto, para identificação de pontos em comum, dependências, possíveis sobreposições de atividades, e para a convergência das ações de melhoria. Esta etapa tem como objetivo criar uma visão integrada de todas as ações de melhoria julgadas necessárias para diminuir o esforço de implementação através 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 pelos gestores responsáveis pelas atividades que serão desenvolvidas. Nesta etapa ocorre, também, a priorização dos planos de ação e a definição de uma data para o provável início da execução;
- d) **Comunicação dos planos de ação:** nesta etapa os planos de ação são comunicados aos responsáveis pela gestão da organização e demais partes interessadas, de maneira a torná-los conscientes dos trabalhos que serão realizados.

A figura 13 apresenta um esquema com as etapas da consolidação dos planos de ação de segurança da informação.

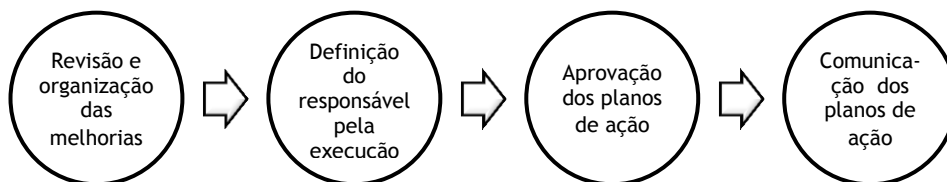


Figura 13. Etapas da consolidação dos planos de ação de segurança da informação

Esta fase pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 7), que orienta que a organização deve “atualizar os planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica”.

3.4.7. Acompanhamento dos planos de ação de segurança da informação

Nesta fase deve ser 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 que tornem necessária uma nova avaliação.

3.4.8. 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 e dos controles de segurança da informação, por comparação com as medições dos ciclos anteriores.

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

3.5. Trabalhos Relacionados

Como trabalhos relacionados à avaliação da segurança da informação e ao uso de modelos de maturidade, podem ser citados:

- Em “Instrumento de avaliação de maturidade em processos de segurança da informação - estudo de caso em instituições hospitalares” (JANSSEN, 2008), Luis Antonio Janssen desenvolveu trabalho semelhante em sua dissertação de mestrado. O objetivo principal do trabalho é propor um instrumento de avaliação da maturidade dos processos de segurança da informação para instituições hospitalares. O trabalho apresenta revisão da literatura para relacionar assuntos ligados à segurança da informação, incluindo modelos existentes de avaliação de processos no contexto de instituições hospitalares, com a aplicação de pré-testes com especialistas em segurança da informação. Foi realizado estudo exploratório, de natureza qualitativa, com aplicação de questionários semiestruturados para estudo de caso em 3 instituições hospitalares. Posteriormente foi realizada análise

do conteúdo dos questionários com relação à aplicabilidade do instrumento, estrutura lógica, clareza das questões e aderência aos objetivos propostos. 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, e a carência em relação às melhores práticas disponíveis na literatura. O trabalho desenvolvido por Janssen se assemelha a este trabalho na utilização da norma ABNT NBR ISO/IEC 27002 para estruturar os controles utilizados para avaliação, e no uso de um modelo de maturidade para realização de medições. A principal diferença para o presente trabalho é que este foi criado para ser 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. O trabalho de Janssen define um modelo especializado, com foco nos requisitos de segurança da informação para cobertura de requisitos legais e regulamentares relacionados às atividades específicas de instituições hospitalares, contendo 40 categorias de análise para avaliação. Outra diferença importante é que o modelo proposto por Janssen apresenta proposições específicas, estáticas, e que pode não possibilitar ao avaliador a adequada análise dos riscos inerentes ao negócio na medida em que haja evolução das tecnologias utilizadas, processos de negócios e/ou requisitos externos aplicáveis à organização.

- Em “Modelo de Governança da Segurança da Informação no Escopo da Governança Computacional” (CUNHA, 2008), Renato Menezes da Cunha desenvolveu dissertação de mestrado com objetivo de 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 forma objetiva os riscos relacionados à informação no momento da definição do planejamento estratégico da organização. A semelhança com o presente trabalho está na utilização da norma ABNT NBR ISO/IEC 27002, o modelo de governança de TI – CobiT, a biblioteca ITIL e avaliações de riscos. A principal diferença está no objetivo do estudo, uma vez que o foco do modelo proposto por Cunha é o alinhamento entre o planejamento estratégico da segurança da informação ao planejamento estratégico da organização, não apresentando um método para medição da situação atual da segurança da

informação e para o acompanhamento da evolução da segurança da informação e dos processos relacionados.

- No artigo “Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação” (Mayer & Fagundes, [2008]), Janice Mayer e Leonardo Lemes Fagundes apresentam modelo para avaliar o nível de maturidade das empresas para gestão de riscos em segurança da informação. O artigo conceitua a gestão de riscos e apresenta normas técnicas relacionadas, discorrendo sobre as fases da gestão de riscos. A semelhança com o presente trabalho é a análise e utilização de normas para gestão de riscos e modelos de maturidade tais como CMM e CobiT, dentre outros apresentados. A diferença está no escopo do artigo, que é a análise do processo de gestão de riscos, não sendo aplicado à gestão da segurança da informação ou à avaliação de maturidade da segurança da informação, objetivo do presente trabalho.

Outros trabalhos relacionados à avaliação da segurança da informação foram consultados. Contudo, o escopo dos trabalhos limitava-se a apresentar características da segurança da informação e realizar análises de adequação à norma ABNT NBR ISO/IEC 27002 através de estudos de caso por avaliação de adequação ou por aplicação de questionários. As avaliações realizadas foram pontuais, não sendo apresentadas formas para medição e acompanhamento da evolução da segurança da informação das organizações avaliadas. Podem-se citar os trabalhos de Neto (2007) e Barreto (2009).

4. ESTUDO DE CASO DE AVALIAÇÃO DA MATURIDADE DA SEGURANÇA DA INFORMAÇÃO

A seguir será apresentado um estudo de caso para aplicação do modelo de avaliação do nível de maturidade da segurança da informação em uma organização, e os principais resultados obtidos.

4.1. A organização

A organização que participou do estudo de caso para avaliação do nível de maturidade da segurança da informação através do modelo descrito neste trabalho possui sua sede administrativa situada em Florianópolis, no Estado de Santa Catarina, e 21 unidades industriais localizadas no território brasileiro.

O *datacenter* da organização está localizado na sede administrativa, onde estão centralizados os principais servidores de aplicativos e bancos de dados que suportam os sistemas corporativos.

A responsabilidade pela segurança da informação está formalmente atribuída à área de Tecnologia da Informação, onde está lotado o responsável pela avaliação.

O responsável pela avaliação da segurança da informação exerce funções relacionadas à segurança da informação e à análise dos processos de gestão de TI para atendimento de requisitos legais e de controle interno da organização.

A organização possui diretrizes para a segurança da informação, normas e diversos procedimentos de gestão relacionados à Tecnologia da Informação, formalmente instituídos e aprovados. A organização possui, também, um programa para divulgação e conscientização da segurança da informação, que visa, principalmente, a conscientização dos empregados aos riscos relacionados à segurança da informação.

4.2. O escopo de avaliação

O escopo de avaliação escolhido foi o conjunto de processos e atividades administrativas da organização, incluindo as atividades administrativas de todas as suas áreas

descentralizadas. Esta escolha foi considerada conveniente pela organização, pois as diretrizes de segurança da informação, normas e demais procedimentos de gestão relacionados à TI e à segurança da informação são aplicáveis a toda a esfera administrativa, independente da localização geográfica.

Não foram inseridos no escopo de avaliação processos industriais e sistemas de controle de processos industriais devido à alta complexidade e especialização necessárias para a avaliação.

A organização já havia realizado, em anos anteriores, avaliações específicas de segurança da informação com método semelhante ao descrito neste trabalho, fato que facilitou as tarefas de avaliação e diminuiu o tempo necessário para análise. A primeira avaliação de segurança da informação realizada pela organização, seguindo a norma BS7799, precursora das ABNT NBR ISO/IEC 27001 e 27002, levou seis meses para ser realizada por uma pessoa integralmente dedicada à análise.

4.3. Análise global dos riscos à segurança da informação

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 abrangente e completa dos controles de segurança da informação seria conveniente para a apuração do atual nível de maturidade da segurança e para a identificação de eventuais riscos desconhecidos, e constituiria importante fonte de informação sobre os controles de segurança da organização.

4.4. Seleção dos controles de segurança da informação

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. Todos os demais 132 controles constantes da norma foram selecionados para avaliação. A lista completa dos controles avaliados encontra-se no anexo A deste trabalho.

4.5. Planejamento da análise dos controles de segurança da informação

A organização pretende realizar um ciclo de avaliação a cada ano, sendo que o prazo para realização deste trabalho foi definido para os meses de janeiro a abril de 2010. Cabe salientar que o cumprimento deste prazo somente foi possível devido à experiência do avaliador com análises de segurança da informação e à documentação gerada em atividades de avaliação realizadas anteriormente na organização.

Foi realizada uma auto avaliação, sob responsabilidade do responsável pela segurança da informação, vinculado ao departamento de TI.

4.6. Análise e avaliação da maturidade dos controles de segurança da informação

A avaliação foi realizada, na sua maior parte, pelo responsável pela segurança da informação da organização, com a possibilidade de consulta aos especialistas de cada área de conhecimento, caso fosse necessário.

As análises e avaliações foram registradas em planilha de avaliação, constante do anexo A deste trabalho. Também foram registradas sugestões para as melhorias consideradas necessárias.

4.6.1. Exemplo de avaliação de controles de segurança da informação

Como o fornecimento de informações detalhadas de todos os controles avaliados não consta no escopo do presente trabalho considerou-se citar exemplos da avaliação realizada sobre dois controles de segurança da informação considerados aplicáveis.

Um dos controles selecionados para exemplo é o item 11.2.4 - *Análise crítica dos direitos de acesso de usuário*, pertencente à seção 11 - *Controle de Acessos*, objetivo de controle 11.2 - *Gerenciamento de acesso do usuário*. De acordo com a ABNT NBR ISO/IEC 27002 (2005, p. 68 e 69), “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 a sistemas, dados, ambientes computacionais e serviços de comunicação.

As atividades realizadas nos cinco passos de avaliação do controle foram:

- a) **Identificação dos processos e atividades relacionadas:** a organização possuía um processo semestral de revisão dos direitos de acesso dos usuários. O processo compreendia a revisão de todos os direitos de acesso aos sistemas aplicativos, ambiente de rede, correio eletrônico e demais formas 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. Os *usuários chave* são responsáveis pela definição dos requisitos de negócio, legais e regulamentares aplicáveis aos sistemas, e pelo treinamento do usuário no uso do recurso sob sua responsabilidade. Houve treinamento aos coordenadores responsáveis pela revisão e há material de apoio disponível no portal da organização para consulta em caso de dúvidas. A coordenação do processo era realizada pelo responsável pela segurança da informação. Entretanto, a solicitação da revisão dos direitos de acesso e a resposta de conclusão do processo eram realizadas por e-mail, com pouco controle sobre a execução do processo em todos os sistemas e módulos;
- 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 para o processo, 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, de maneira a garantir que a revisão fosse realizada periodicamente. 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 seja executada de acordo com o planejado. Como consequência a organização considerou necessário melhorar o processo de revisão de direitos de acesso de usuários de modo a atingir o nível de maturidade 4 - **Gerenciado**.

- d) **Definição de melhorias necessárias:** para alcançar o nível 4 de maturidade (gerenciado) no processo de revisão periódica de direitos de acesso de usuários as seguintes melhorias foram sugeridas:
- i. Desenvolver 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 haja controle documentado sobre a realização das revisões e sobre a tomada de ação no caso de haver algum sistema, módulo ou ambiente que não tenha a revisão concluída no prazo estipulado;
 - iii. Realizar comunicação formal ao gerente da área de TI, auditoria interna, e ao gerente da área de negócio responsável pelo sistema, módulo ou ambiente que não tenha seu processo de revisão concluído no prazo estipulado;
 - iv. Realizar comunicação formal sobre o acompanhamento do processo ao gerente da área de TI e auditoria interna sobre a finalização de cada ciclo de revisão de direitos de acesso.
- e) **Comunicação dos resultados aos responsáveis pelo controle:** as alterações propostas foram documentadas e encaminhadas ao gerente de TI e auditoria interna da organização.

Outro controle selecionado para exemplo é o item 10.1.3 – *Segregação de funções*, pertencente à seção 10 – *Gerenciamento das operações e comunicações*, objetivo de controle 10.1 – *Procedimentos e responsabilidades operacionais*. De acordo com a ABNT NBR ISO/IEC 27002 (2005, p. 41), “convém que funções e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização”, a fim de se tomarem cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem autorização, ou iniciar, aprovar e executar atividades em um mesmo processo que levem ao erro ou à fraude.

As atividades realizadas nos cinco passos de avaliação do controle foram:

- a) **Identificação dos processos e atividades relacionadas:** a organização possuía análises informais de segregação de tarefas para a administração dos ambientes computacionais. A organização possui relatório de atividades incompatíveis, baseado nos perfis de acesso dos sistemas corporativos, disponibilizado a usuários

- autorizados no portal corporativo. As consultas aos relatórios de incompatibilidade de responsabilidade deveriam ser realizadas periodicamente pelos responsáveis pelos sistemas críticos no que se refere a processos financeiros. No entanto, as consultas eram esporádicas e não havia controle sobre a realização da verificação, ou sobre medidas a serem tomadas quando da identificação de possíveis problemas;
- b) **Análise do nível de maturidade do controle:** de acordo com a escala de maturidade utilizada neste trabalho, a existência de um processo sem que seja formalmente definido e aprovado, sem a definição formal de responsabilidades e sem o treinamento dos envolvidos caracteriza o nível de maturidade 2 – **Repetitivo**;
- c) **Avaliação do nível de maturidade do controle:** a organização, por estar submetida a exigências de controles nos processos financeiros, necessitava demonstrar que possuía controle sobre a realização de análises de segregação de tarefas tanto na administração do ambiente computacional quanto nos perfis de acesso aos sistemas para suportar a segregação de tarefas nos processos de negócio. Neste caso a organização deve garantir que a análise seja executada a intervalos de tempo pré-definidos, e as ações de correção ou de contorno sejam documentadas e aprovadas. Como consequência, a organização considerou necessário melhorar o processo de análise de segregação de tarefas de modo a atingir o nível de maturidade 4 - **Gerenciado**.
- d) **Definição de melhorias necessárias:** para alcançar o nível 4 de maturidade (gerenciado) no processo de análise de segregação de tarefas nos perfis dos sistemas, as seguintes melhorias foram sugeridas:
- i. Desenvolver um sistema para registrar todas as análises de segregação de tarefas nos perfis dos sistemas, módulos e ambientes em que a análise for necessária;
 - ii. Implantar um processo de análise de segregação de tarefas para que haja controle documentado sobre a realização das análises, sobre a tomada de ação no caso de haver algum problema identificado, e sobre a aprovação de possíveis ações pelo gestor competente.
- e) **Comunicação dos resultados aos responsáveis pelo controle:** as alterações propostas foram documentadas e encaminhadas ao gerente de TI e auditoria interna da organização.

4.7. Consolidação dos planos de ação de segurança da informação

Após a finalização da avaliação do nível de maturidade de todos os controles de segurança da informação selecionados, as melhorias propostas foram consolidadas, dando origem a planos de ação. Os planos de ação foram entregues sob a responsabilidade das áreas de TI, recursos humanos, jurídico, e segurança física e patrimonial da organização.

Os planos de ação que não necessitavam de investimento para serem executados, tais como adequação de diretrizes, procedimentos e cláusulas contratuais, foram selecionados para serem executados primeiro.

Os planos de ação que necessitavam de investimento ou exigiam mudanças maiores em infraestrutura de TI ou em processos de negócio serão reavaliados no próximo ciclo de avaliação de maturidade da segurança da informação (a ser realizado a cada ano), para correta destinação de recursos de acordo com as prioridades do negócio.

4.7.1. Exemplo de consolidação de um plano de ação

Para exemplificar esta etapa, faz-se necessário considerar a avaliação dos controles 11.2.4 - *Análise crítica dos direitos de acesso de usuário*, e 10.1.3 – *Segregação de funções*, citados neste trabalho como exemplo de avaliação de controles de segurança de informação.

As melhorias sugeridas para os dois controles foram combinadas de forma a criar um único plano de ação capaz de cumprir com os objetivos de ambos os controles de segurança, dentro de um mesmo processo documentado e gerenciado.

O plano de ação criado tinha como objetivo redefinir o processo de revisão semestral dos direitos de acesso dos usuários e segregação de tarefas nos perfis de sistemas. O plano de ação estava sob a responsabilidade da área de TI, com as seguintes ações:

- a) Desenvolver 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 do sistema em questão;
- b) Inserir no sistema de revisão de direitos de acesso o registro da análise de segregação de tarefas nos perfis dos sistemas, módulos e ambientes, de modo a documentar as incompatibilidades encontradas, realizar a comunicação ao gerente responsável, e registrar a decisão do gerente para tomada de ação no caso de haver

algum problema identificado (exemplos: remover o direito de acesso incompatível ou adotar controles compensatórios para casos de menor risco);

- c) Modificar o processo de revisão de direitos de acesso e segregação de tarefas para que haja controle documentado sobre a realização das revisões e sobre a tomada de ação no caso de haver algum sistema, módulo ou ambiente que não tenha a revisão concluída no prazo estipulado;
- d) Realizar comunicação formal ao gerente da área de TI, auditoria interna, e ao gerente da área de negócio responsável pelo sistema, módulo ou ambiente que não tenha seu processo de revisão concluído no prazo estipulado;
- e) Realizar comunicação formal sobre o acompanhamento do processo ao gerente da área de TI e auditoria interna, na finalização do ciclo de revisão dos direitos de acesso e segregação de tarefas.

Cabe salientar que a maneira apresentada para cumprir com os objetivos dos controles citados nos exemplos, considerando as medidas tomadas para melhoria dos controles e a vinculação das atividades em um mesmo plano de ação, não é a melhor ou a única forma possível de tratar os riscos envolvidos e cumprir com as exigências específicas de qualquer organização. Uma análise específica deve ser realizada em cada organização para identificar a forma mais adequada de promover a melhoria necessária aos seus processos.

4.8. Acompanhamento dos planos de ação de segurança da informação

Os planos de ação relacionados à segurança da informação serão acompanhados pela organização. A cada novo ciclo de avaliação da maturidade da segurança da informação os controles aplicáveis serão reavaliados e os planos de ação pendentes serão revisados.

4.9. Fechamento, documentação e emissão de relatórios

A tabela 9 apresenta os resultados dos níveis de maturidade médios apurados para cada seção da norma ABNT NBR ISO/IEC 27002, extraídos da planilha de avaliação.

Tabela 9. 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

O gráfico 3 apresenta a visualização dos níveis de maturidade médios apurados.

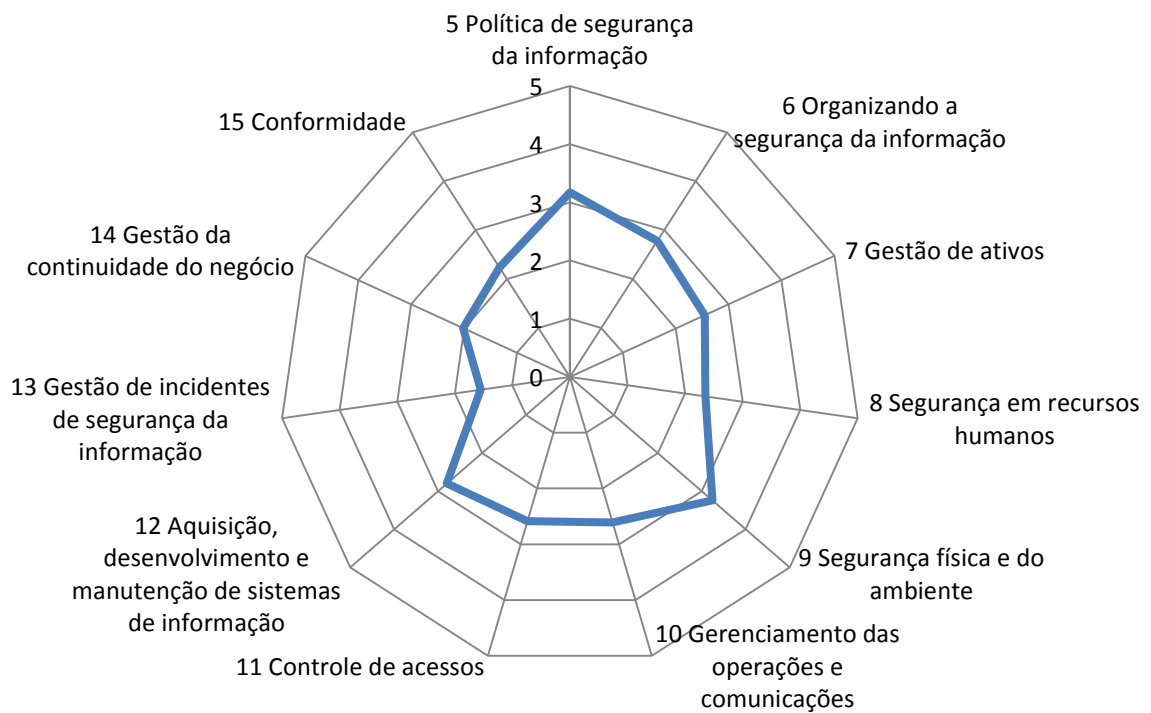


Gráfico 3. Visualização dos níveis de maturidade médios apurados no estudo de caso

4.9.1. Avaliação dos resultados

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 formalmente definidos. A organização considera que a maioria dos seus processos de segurança possui nível de maturidade adequado à sua realidade, sendo os principais controles relacionados à conformidade com requisitos externos classificados com níveis de maturidade entre 3 e 4. Diversos planos de ação criados estavam relacionados a pequenas melhorias nos processos, não estando, necessariamente, vinculados à alteração do nível de maturidade para um nível maior.

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, quando poderia ter indicado um especialista para cada controle aplicável, nas respectivas áreas de domínio. Esta indicação teria o intuito de gerar comprometimento do especialista com a avaliação e de melhorar a qualidade da avaliação dos controles. O fato de o responsável pela avaliação estar subordinado ao departamento de TI poderia caracterizar falta de independência para avaliação dos controles e emissão de parecer. Considera-se, contudo, que tal situação tem pouca influência na avaliação do método em si e nos benefícios gerados pela sua utilização.

4.10. Percepção da organização sobre o método de avaliação

Segundo percepção da organização, o método de avaliação dos objetivos de controle da norma ABNT NBR ISO/IEC 27002 por meio de níveis de maturidade proporcionou vantagens para a organização, conforme relato do responsável pela área de TI da organização:

“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 da documentação necessária para avaliação e direcionamento dos esforços de várias áreas da organização para a melhoria da segurança da informação. Muitas ações de melhoria foram identificadas em virtude da avaliação individual de cada item de controle da norma, e o modelo de maturidade auxilia na identificação e priorização das ações de melhoria necessárias.”

A organização irá manter as avaliações de maturidade da segurança da informação através de ciclos anuais de avaliação.

5. CONSIDERAÇÕES FINAIS

Este trabalho apresenta um instrumento de avaliação que pode ser utilizado por diversos tipos de organizações, através da adoção de uma abordagem de processo para avaliação e melhoria contínua da segurança da informação, do uso de normas sedimentadas e completas relacionadas à segurança da informação, e da medição por níveis de maturidade. Pretendeu-se contribuir com os demais estudos já realizados sobre segurança da informação e maturidade dos processos de gestão.

As considerações finais apresentadas a seguir foram baseadas nas conclusões sobre o estudo da literatura relacionada e da estrutura do modelo, e em sugestões para trabalhos e pesquisas futuras.

5.1. Conclusões

A utilização de um instrumento de avaliação da maturidade da segurança da informação pode ser considerada altamente relevante para as organizações, em decorrência da importância que as informações possuem para a realização e continuidade das atividades de negócio.

O presente estudo reúne diversos pontos relevantes sobre o tema segurança da informação e poderá servir de base para novos estudos e pesquisas acadêmicas.

Considera-se que a apresentação e detalhamento de um método para a gestão da segurança da informação de uma organização através da avaliação periódica da maturidade e melhoria contínua dos seus controles foi alcançado. A pesquisa bibliográfica sobre as principais fontes de referência para a segurança da informação e sobre o uso de modelo de maturidade foi ampla o suficiente para embasamento e sustentação do instrumento de avaliação. O uso de uma escala de maturidade, aliado à abordagem de 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 principais trabalhos relacionados apresentados está no uso da norma ABNT NBR ISO/IEC 27002 (ou ISO/IEC 27002) como base de controles para a avaliação, e no uso de um modelo de maturidade para as medições. Este comparativo reforça que a abordagem utilizada por este método de avaliação é adequada ao

seu propósito. A principal diferença reside no fato de que os modelos propostos apresentam proposições específicas, estáticas, e que podem não possibilitar ao avaliador a adequada análise dos riscos inerentes ao negócio na medida em que haja evolução das tecnologias, processos e/ou requisitos externos aplicáveis. Outra importante diferença é que este trabalho procura definir um modelo genérico de avaliação, aplicável a todos os tipos de organização independente de tamanho ou área de atuação, através do uso de todos os objetivos de controle de segurança da informação constantes da norma ABNT NBR ISO/IEC 27002.

O autor considera que o uso de modelos com proposições estáticas e específicas para um determinado setor da indústria é útil para avaliadores iniciantes ou inexperientes na interpretação dos controles da norma, pois pode conter exemplos do que deveria ou 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 adequado para avaliadores iniciantes, que devem primeiro compreender e interpretar a norma; 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.

Através dos trabalhos relacionados, que utilizam abordagens semelhantes de avaliação, e da percepção da organização que participou do estudo de caso, pode-se concluir que o método de avaliação apresentado é eficaz para avaliar o estado atual da segurança da informação da organização, para auxiliar nos processos de gestão da segurança da informação e identificação de riscos, e para apoiar a melhoria dos processos e controles internos da organização.

5.2. Sugestões para pesquisas e trabalhos futuros

Como sugestão para pesquisas e trabalhos futuros que venham a contribuir para a melhoria do processo de gestão da segurança da informação, podem ser citados os seguintes itens:

- a) Especificar método para avaliação individual dos riscos dos objetivos de controle, considerando os processos, atividades e controles envolvidos, e vinculando os resultados encontrados a níveis de maturidade mínimos a serem atingidos pela organização;

- b) Aplicar o instrumento de avaliação proposto em outras organizações a fim de se obter uma pesquisa quantitativa sobre a maturidade da segurança da informação e possibilitar comparações entre organizações do mesmo setor;
- c) Melhorar a documentação do processo de análise, criando-se modelos que possam ser utilizados em todas as fases e etapas de avaliação;
- d) Inserir no ciclo de avaliação uma fase para auditoria independente dos resultados, para os casos em que a organização optar pela auto avaliação.

6. REFERÊNCIAS

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO GUIA 73:2009: Gestão de Riscos - Vocabulário**. Rio de Janeiro, 2009. 12 p.
2. _____. **ABNT NBR ISO 31000:2009: Gestão de Riscos - Princípios e diretrizes**. Rio de Janeiro, 2009. 24 p.
3. _____. **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.
4. _____. **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.
5. _____. **ABNT NBR ISO/IEC 27004:2010: Tecnologia da informação – Técnicas de segurança – Gestão da Segurança da Informação – Medição**. Rio de Janeiro, 2010. 59 p.
6. _____. **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.
7. BARRETO, Danilo Muniz. **Uma Abordagem Sobre Política da Segurança da Informação Implantada**. Centro Paula Souza. Centro Tecnológico da Zona Leste. Faculdade de Tecnologia da Zona Leste. 2009. Disponível em <<http://www.fateczl.edu.br/TCC/2009-1/tcc-11.pdf>>. Acesso em 29 abril 2010.
8. CUNHA, Renato Menezes da. **Modelo de Governança da Segurança da Informação no Escopo da Governança Computacional**. Universidade Federal de Pernambuco. Programa de Pós-Graduação em Engenharia de Produção. 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.
9. FERREIRA, Fernando Nicolau Freitas. **Segurança da informação**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2003. 162p.
10. HINTZ, Marco Aurélio. **Process Institutionalization**. [S.I. : s.n.], 2010. Disponível em <<http://www.softexpert.com.br/downloads.php?prod=24&pg=83>>. Acesso em: 11 junho 2010.
11. 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.
12. _____. **CobiT Mapping – Overview of international IT Guidance, 2nd Edition**. Rolling Meadows – USA: [s.n.], 2006. Disponível em

- <<http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>>. Acesso em: 05 junho 2008.
13. ITPCG - *IT POLICY COMPLIANCE GROUP. Best Practices for Managing information Security*. [S.I. : s.n.], 2010. Disponível em <http://www.itpolicycompliance.com/research_reports/>. Acesso em: 11 junho 2010.
 14. ITSMF – *The IT Service Management Forum. An Introductory Overview of ITIL V3*. [S.I.: s.n], 2007. Disponível em <<http://www.itsmfi.org/content/introductory-overview-itil-v3-pdf>> Acesso em 12 setembro 2010.
 15. JANSSEN, Luis Antonio. **Instrumento de avaliação de maturidade em processos de segurança da informação: estudo de caso em instituições hospitalares**. Pontifícia Universidade Católica do Rio Grande do Sul. Faculdade de Administração, Contabilidade e Economia. Mestrado em Administração e Negócios. 2008. Disponível em < http://tede.pucrs.br/tde_arquivos/2/TDE-2008-04-22T140541Z-1200/Publico/400421.pdf >. Acesso em: 29 abril 2010.
 16. MARANHÃO, Mauriti; **ISO Série 9000: manual de implementação: versão ISO 2000**. 6ª ed. Rio de Janeiro: Qualitymark, 2001. 220p.
 17. MAYER, Janice; FAGUNDES, Leonardo Lemes. **Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação**. Universidade do Vale do Rio dos Sinos. [2008]. VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Disponível em <http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st02_03_wticg.pdf>. Acesso em: 29 abril 2010.
 18. NETO, Abner Silveira. **Gestão da Segurança da Informação: fatores que influenciam a sua adoção em pequenas e médias empresas**. Universidade Municipal de São Caetano do Sul. Pró Reitoria de Pós-Graduação e Pesquisa. Programa de Mestrado em Administração. 2007. Disponível em <http://www.uscs.edu.br/posstricto/administracao/dissertacoes/2007/abner_da_silva_netto/dissertacao_AbnerNetto.pdf >. Acesso em 29 abril 2010.
 19. NIST - National Institute of Standards and Technology. Technology Administration. U.S. Department of Commerce. **An Introduction to Computer Security: The NIST Handbook**. [S.I. : s.n.], 1995. Special Publication 800-12. Disponível em: <<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>>. Acesso em: 04 junho 2010.
 20. PINHEIRO, Patrícia Peck. **Segurança da Informação Amadurecida**. [S.I. : s.n.], 2010. Disponível em <<http://www.itweb.com.br/blogs/blog.asp?cod153&arquivo=10/2010>>. Acesso em: 09 outubro 2010.
 21. PINHEIRO, Patrícia Peck; SLEIMAN, Cristina Moraes. **Tudo o que você precisa saber sobre direito digital no dia-a-dia**. São Paulo: Saraiva, 2009. 58p.

22. RAMOS, Anderson (org.). **Security Officer - 1: guia oficial para formação de gestores em segurança da informação**. Porto Alegre: Zouk, 2006. 460p. Módulo Security Solutions.
23. SÊMOLA, Marcos. **Gestão da Segurança da Informação: visão executiva da segurança da informação: aplicada ao Security Officer**. Rio de Janeiro: Campus, 2003. 154 p.

Modelo de Avaliação da Maturidade da Segurança da Informação

Evandro Alencar Rigon¹

¹Centro Tecnológico - Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 - 88.040-970 - Florianópolis - SC - Brasil

rigon@inf.ufsc.br

Abstract. *Business processes are supported by information technologies, although many processes and information systems were not designed to be safe. 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 pointed the method to be 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

Viver na era da informação, na era da sociedade digital, significa estar mais acessível e, conseqüentemente, mais exposto. As comunicações são mais rápidas e dinâmicas, passando do âmbito local para o alcance global. A troca de informações entre as organizações, de qualquer tipo ou finalidade, também passou a ser feita através do meio eletrônico, principalmente com a chegada do comércio eletrônico e da disponibilização de serviços bancários online. A natureza das informações organizacionais trocadas por meios eletrônicos é cada vez mais diversa, e a quantidade e a criticidade das informações em trânsito aumentam substancialmente (PINHEIRO; SLEIMAN, 2009).

O desconhecimento das ameaças e das vulnerabilidades existentes nas tecnologias da informação e nos processos de negócio, cada vez mais complexos e interdependentes, expõe as organizações a um nível de risco muito alto à continuidade das suas atividades e, conseqüentemente, à sua própria existência.

A avaliação crítica e metódica dos controles relacionados à segurança da informação torna-se necessária pelo simples fato de que tecnologias, processos de negócio e pessoas mudam, em um ritmo muito rápido, alterando constantemente o nível de risco atual e gerando novos riscos à organização.

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.

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 assunto está dividido em cinco seções. A primeira seção apresenta a introdução ao artigo, a motivação, o problema, a proposta e a estrutura de organização do artigo. A segunda sessão apresenta os principais trabalhos relacionados. A terceira sessão apresenta as principais normas técnicas relacionadas à segurança da informação e à gestão de riscos. A quarta sessão é dedicada à especificação do modelo de avaliação da segurança da informação através da medição de níveis de maturidade, com a integração dos conceitos e normas apresentados nos capítulos anteriores. A quinta sessão apresenta um estudo de caso onde o modelo foi aplicado em uma organização para verificação da sua eficácia. A sexta sessão apresenta as conclusões e considerações finais.

2. Trabalhos relacionados

Em “Instrumento de avaliação de maturidade em processos de segurança da informação - estudo de caso em instituições hospitalares” (JANSSEN, 2008), Luis Antonio Janssen desenvolveu trabalho semelhante em sua dissertação. O objetivo principal do trabalho é propor um instrumento de avaliação da maturidade dos processos de segurança da informação para instituições hospitalares. Foi realizado estudo exploratório, de natureza qualitativa, com aplicação de questionários semiestruturados para estudo de caso em 3 instituições hospitalares. Posteriormente foi realizada análise do conteúdo dos questionários com relação à aplicabilidade do instrumento, estrutura lógica, clareza das questões e aderência aos objetivos propostos. 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, e a carência em relação às melhores práticas disponíveis na literatura. O trabalho desenvolvido por Janssen se assemelha a este trabalho na utilização da norma ABNT NBR ISO/IEC 27002 como fonte de controles a serem avaliados, e no uso de um modelo de maturidade para realizar medições. A principal diferença para o presente trabalho é que este apresenta 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. O trabalho de Janssen define um modelo especializado, com foco nos requisitos de segurança da informação para cobertura de requisitos legais e regulamentares relacionados às atividades específicas de instituições hospitalares, contendo 40 categorias de análise para avaliação. Outra diferença importante é que o modelo proposto por Janssen apresenta proposições específicas, estáticas, e que pode não possibilitar ao avaliador a adequada análise dos riscos na medida em que haja evolução das tecnologias utilizadas, processos de negócio e/ou requisitos externos aplicáveis à organização.

Em “Modelo de Governança da Segurança da Informação no Escopo da Governança Computacional” (CUNHA, 2008), Renato Menezes da Cunha desenvolveu dissertação com objetivo de 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 forma objetiva os riscos relacionados à informação no momento da definição do planejamento estratégico da organização. A semelhança com o presente trabalho está 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 é o alinhamento entre o planejamento estratégico da segurança da informação ao planejamento estratégico da organização, não apresentando um método para medição da situação atual da segurança da informação e do acompanhamento evolução da segurança da informação e de seus processos relacionados.

4. Principais normas técnicas relacionadas à segurança da informação

A expressão “segurança da informação”, por si só, é um termo ambíguo, podendo significar tanto uma prática interdisciplinar adotada para tornar um ambiente seguro (segurança como um meio), como a característica que a informação adquire ao ser alvo de uma prática da segurança (segurança como fim) (SÊMOLA, 2003, p. 44).

A segurança da informação pode ser considerada como uma forma de “blindagem” para a proteção do patrimônio intangível de uma organização, e “engloba um conjunto de ações que devem ser planejadas e programadas de forma a abranger as questões técnicas, comportamentais e, também, jurídicas” (PINHEIRO; SLEIMAN, 2009, p.27.).

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.

O conceito de segurança é, em essência, bastante abstrato. A forma que uma organização considera adequada para gerenciar a segurança das suas informações pode não ser a melhor maneira na opinião de outras organizações (RAMOS, 2006, p. 38).

Com o objetivo de diminuir ou mesmo evitar esta subjetividade este artigo procurou utilizar normas técnicas adotadas internacionalmente por organizações que buscam um direcionamento para as suas iniciativas de segurança.

Uma norma técnica regulamenta boas práticas de forma unificada e consensada internacionalmente. Ao segui-la, caso a organização sofra algum incidente, poderá alegar que fez tudo o que estava ao seu alcance para evitá-lo, visto que pratica recomendações internacionais (PINHEIRO; SLEIMAN, 2009, p. 27).

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).

Cabe salientar que a conformidade com uma norma técnica, por si só, não confere imunidade à organização em relação às suas obrigações legais (ABNT NBR ISO/IEC 27001, 2006, p. 1).

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, p. v).

ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação: versão atualizada da ABNT NBR ISO/IEC 17799 de 2005, é o fundamento normativo da segurança da informação (PINHEIRO; SLEIMAN, 2009, P. 27). 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, p.1). 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. Por esse motivo o documento deve ser utilizado com uma postura crítica para o que é adequado ao negócio (RAMOS, 2006, p. 39). 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 irá determinar a necessidade de mudanças e a priorização destas 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 especificados na ABNT NBR ISO/IEC 27001, para uma implementação da segurança da informação baseada na gestão de riscos e suas atividades (ABNT NBR ISO/IEC 27005, 2008, p. 1 a 3).

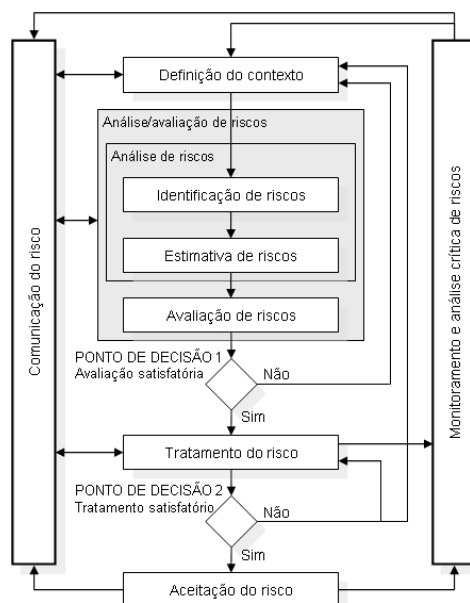


Figura 1. Processo de gestão de riscos de segurança da informação (adaptado de ABNT NBR ISO/IEC 27005, 2008 p. 5).

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.

5. O modelo de avaliação por níveis de maturidade

Com base nas características da segurança da informação e das principais normas apresentadas, o modelo de avaliação apresentado no presente artigo procurou reunir as seguintes características principais:

- 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 um conjunto específico e adequado de controles, internacionalmente reconhecidos, e que tratem a segurança da informação de forma abrangente, 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 e nas condições dos processos de negócio da organização, suportado pelo uso da ABNT NBR ISO/IEC 27005.

O modelo apresentado neste artigo tem como principais propósitos avaliar a segurança da informação de maneira abrangente, integrando as diversas áreas de controle da organização, e fazer com que o foco da segurança da informação seja convergido para um ponto em comum de acordo com os objetivos organizacionais.

5.1. Avaliação e melhoria contínua

Os computadores, o ambiente no qual eles operam e os riscos envolvidos são dinâmicos. Como consequência os requisitos de segurança da informação são alterados constante e indefinidamente. Esses fatores demonstram que se torna necessária a reavaliação periódica da segurança da informação, através de um processo cíclico de gestão.

O ciclo *Plan-Do-Check-Act* (PDCA) pode ser considerado como o método mais geral para trabalhar com qualidade, podendo-se condicionar a gestão das organizações a um ciclo lógico de melhorias contínuas para alcançar os resultados esperados (MARANHÃO, 2001, p.11, 52 e 53).

Em sintonia com os padrões adotados pela norma de qualidade ISO9000, a norma ABNT NBR ISO/IEC 27001 adota o modelo PDCA para estruturar os processos do SGSI. Esta abordagem encoraja que os usuários administradores do SGSI enfatizem a importância de melhoria contínua baseada em medições objetivas.

5.2. Controles de segurança da informação

O modelo de avaliação apresentado neste artigo utiliza a estrutura de objetivos de controle e controles da norma ABNT NBR ISO/IEC 27002, internacionalmente reconhecidos como adequados à gestão da segurança da informação. A versão utilizada, de 2005, define 133 controles, que poderão ser avaliados.

5.3. Medição e Acompanhamento

A grande quantidade e variedade de objetivos de controle e controles aplicáveis à segurança da informação tornam a sua gestão um processo complexo.

A avaliação dos processos de acordo com um modelo de maturidade é atividade chave para implementação de governança. 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. A medição por níveis de maturidade, além de dar transparência ao processo de gestão, permite realizar comparações entre ciclos de avaliação e mesmo entre organizações - *benchmark* (ITGI, 2007, p. 9). Os níveis de maturidade utilizados neste artigo seguiram os conceitos definidos pelo CobiT (*Control Objectives for Information and Related Technology*), representados na figura 2.

O CobiT é um conjunto de boas práticas obtidas através do consenso de experts, mais focadas 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, assim como o CobiT, em uma escala de maturidade. Utilizando-se de uma analogia entre a segurança de TI e a segurança da informação como um todo, este modelo pretende dar subsídio para que o processo de gestão da segurança de informação possa atingir níveis mais altos de maturidade.

Os níveis de maturidade estão representados graficamente na figura 2.

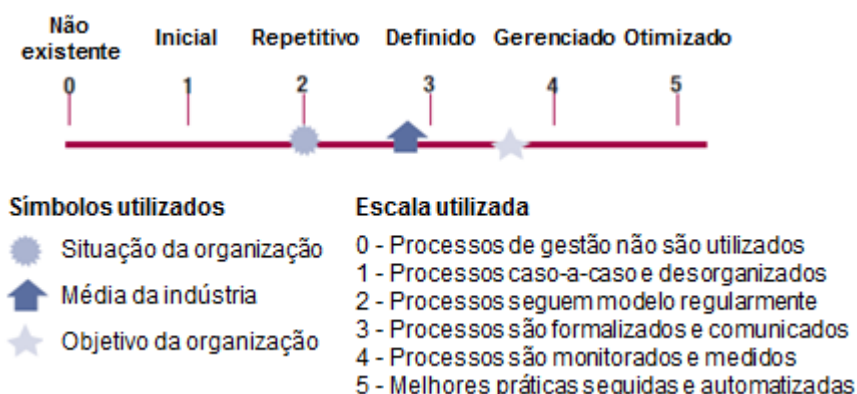


Figura 2. Representação gráfica do modelo de maturidade utilizado no CobiT (adaptado de ITGI, 2007 p. 18).

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, p. 19. Tradução livre do autor)

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.

Nível	Características
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 e 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.
5 Otimizado	Os processos foram refinados ao nível de melhores práticas, baseado no resultado de melhorias contínuas e de comparação da maturidade com outras organizações. TI é utilizada de maneira integrada para automatizar os fluxos de trabalho, fornecendo ferramentas para melhorar a qualidade e efetividade, e tornando fácil para a organização se adaptar.

5.4. Fases do ciclo de avaliação e melhoria contínua

Uma métrica, ou indicador, por si só, não são a resposta para gerenciar os problemas de segurança da informação de uma organização, pois não considera o tempo, fator relevante para o tipo de análise proposto. Além de medir, deve existir ação sobre os problemas encontrados e o acompanhamento da evolução ao longo do tempo.

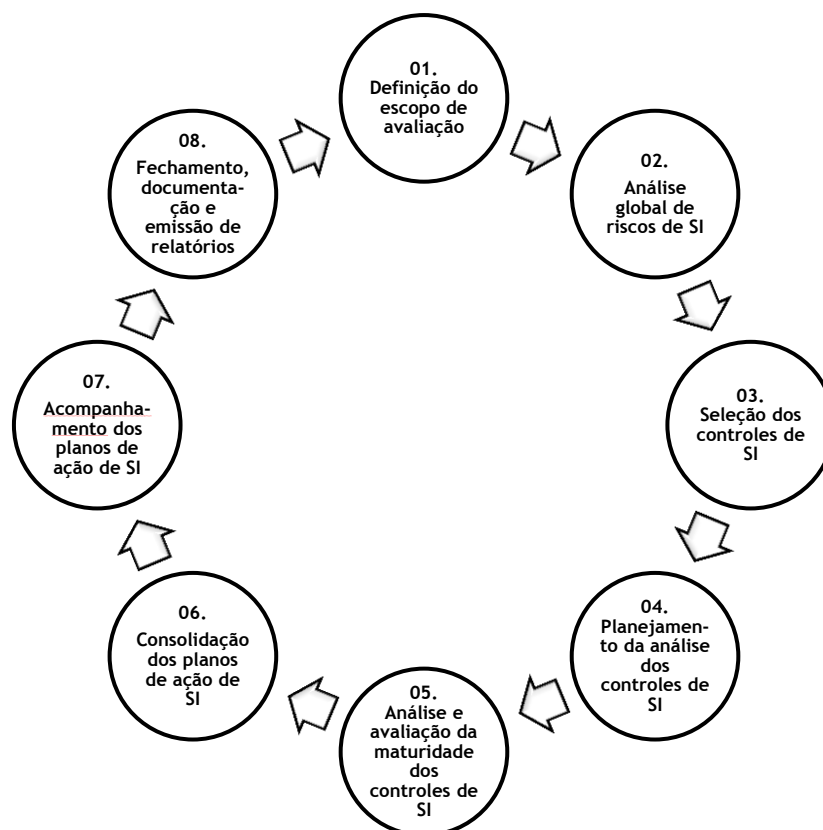


Figura 3. Fases do ciclo de avaliação e melhoria da segurança da informação (SI)

A figura 3 apresenta as oito fases que compõem o ciclo de avaliação da maturidade da segurança da informação (SI). As principais atividades realizadas em cada fase do ciclo de avaliação e melhoria da segurança da informação são apresentadas a seguir.

5.4.1. Definição do escopo de avaliação

Nesta fase será 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 de negócio da organização que serão incluídos no processo de avaliação do nível de maturidade da segurança da informação. O escopo e os limites do SGSI devem ser definidos “nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo” (ABNT NBR ISO/IEC 27001, 2006, p. 4).

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 para análise sejam os controles relacionados ao tratamento dos riscos aos quais a organização estiver submetida. A documentação do SGSI deve conter “uma descrição da metodologia de análise/avaliação de riscos” (ABNT NBR ISO/IEC 27001, 2006, p. 8).

A análise de riscos pode ser realizada em diferentes graus de detalhamento, dependendo da criticidade dos ativos e extensão das vulnerabilidades. A metodologia de análise pode ser quantitativa, qualitativa ou uma combinação de ambas, dependendo das circunstâncias de avaliação. 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, p.14).

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.

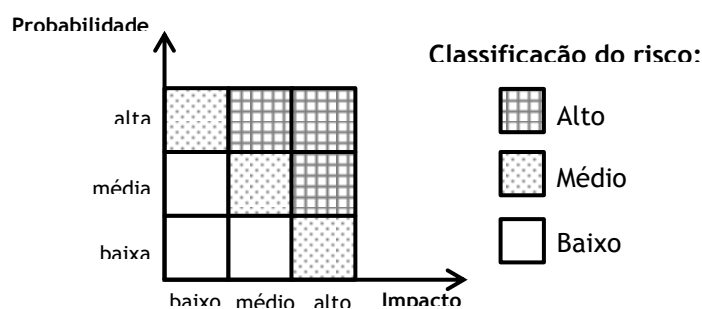


Figura 4. Escala para análise e classificação de riscos

A figura 4 apresenta a escala utilizada para análise e classificação dos riscos relacionados à segurança da informação.

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.

Esta fase do modelo pretende cumprir com o disposto na ABNT NBR ISO/IEC 27001 (2006, p. 6), que orienta que os “objetivos de controle e controles devem ser selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos [...]”, e que a organização deva preparar uma declaração de aplicabilidade, onde serão apresentados os objetivos de controle e controles selecionados a partir do anexo A da referida norma.

Apesar de o modelo estudado utilizar a estrutura de controles da norma ABNT NBR ISO/IEC 27002 como base de avaliação, as organizações devem ser capazes de identificar outros controles pertinentes que devam ser avaliados, considerando, por exemplo, a análise dos riscos relacionados à segurança da informação, a análise dos riscos corporativos, a gestão da conformidade (*compliance*), outras fontes de requisitos legais ou regulamentares aplicáveis ao negócio, 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 cada controle de segurança da informação selecionado deve ser avaliado, juntamente com os processos, atividades e controles relacionados, para determinar o nível de maturidade do controle de acordo com a escala de maturidade utilizada pelo modelo. O nível de maturidade de cada controle será comparado com a análise de riscos e, caso necessário, um plano de ação deve ser documentado 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 diferentes atividades com níveis de maturidade distintos relacionadas ao mesmo controle;

- 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. São documentadas possíveis falhas no cumprimento dos controles, relacionando os problemas observados e, quando possível, relacionando sugestões de possíveis melhorias que poderiam ser implementadas;
- d) Definição de melhorias necessárias: com base nas possíveis deficiências encontradas no cumprimento dos controles, nesta etapa serão documentadas as alterações e melhorias nas atividades relacionadas ao controle de segurança, ou mesmo a criação de novas atividades, para manter o nível de risco adequado de acordo com o apetite de risco da organização. As alterações devem ser documentadas em conjunto com os responsáveis pelos processos de negócio envolvidos;
- e) Comunicação dos resultados aos responsáveis pelo controle: nesta etapa os resultados da análise do controle de segurança avaliado são comunicados aos seus 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. Esta etapa visa criar uma visão integrada de todas as ações de melhoria julgadas necessárias para diminuir o esforço de implementação através 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 pelos gestores responsáveis pelas atividades que serão desenvolvidas. Nesta etapa ocorre, também, a priorização dos planos de ação e a definição de uma data para o provável início da execução;
- d) Comunicação dos planos de ação: nesta etapa os planos de ação são comunicados aos responsáveis pela gestão da organização e demais partes interessadas, de maneira a torná-los conscientes dos trabalhos que serão 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 NBR ISO/IEC 27001, 2006, p. 7).

5.4.7. Acompanhamento dos planos de ação de segurança da informação

Nesta fase será realizado um acompanhamento da execução dos planos de ação, junto aos responsáveis pela sua execução, para verificar o cumprimento dos prazos e avaliar possíveis desvios que gerem a necessidade de 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 os relatórios operacionais e gerenciais. Nesta fase é documentada a evolução do nível de maturidade dos objetivos de controle, por comparação com as medições dos ciclos anteriores.

A documentação de fechamento deverá ser completa o suficiente para demonstrar a evolução da segurança da informação, conscientizar a alta direção para os principais pontos de atenção e riscos remanescentes, justificar a necessidade de recursos para a melhoria do 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 abrangente e completa dos controles de segurança da informação seria conveniente para a apuração do atual nível de maturidade da segurança da informação, identificação de eventuais riscos desconhecidos e constituiria importante fonte de informações sobre os controles de segurança da organização.

Inicialmente, em virtude da grande extensão dos processos de negócio da organização, decidiu-se por considerar como sendo aplicáveis 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. Todos os demais 132 controles constantes da norma foram selecionados para avaliação.

A avaliação dos controles foi realizada pelo responsável pela segurança da informação da organização, com a possibilidade de consulta aos especialistas em cada área de conhecimento, caso necessário.

Foi selecionado como exemplo o controle 11.2.4 - *Análise crítica dos direitos de acesso de usuário*, pertencente à seção 11 - *Controle de Acessos*, objetivo de controle 11.2 - *Gerenciamento de acesso do usuário*. De acordo com a ABNT NBR ISO/IEC 27002 (2005, p. 68 e 69), “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 a sistemas, dados, ambientes computacionais e serviços de comunicação. 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 dos usuários, que compreendia a revisão de todos os direitos de acesso aos sistemas aplicativos, ambiente de rede, correio eletrônico e demais formas 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 aos coordenadores responsáveis pela revisão e há material de apoio disponível para consulta em caso de dúvidas. A coordenação do processo era realizada pelo responsável pela segurança da informação. Entretanto, a solicitação da revisão dos direitos de acesso e a resposta de conclusão eram realizadas por e-mail, com pouco controle sobre a execução do processo em todos os sistemas e módulos;

- 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, de maneira a garantir que a revisão fosse realizada periodicamente. 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 planejado. Como consequência a organização considerou necessário melhorar o processo de revisão de direitos de acesso de usuários de modo a atingir o nível de maturidade 4 - Gerenciado.
- d) Definição de melhorias necessárias: para alcançar o nível 4 de maturidade (gerenciado) no processo de revisão periódica de direitos de acesso de usuários as seguintes melhorias foram sugeridas:
 - i. Desenvolver 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 haja controle documentado sobre a realização das revisões e sobre a tomada de ação no caso de haver algum sistema, módulo ou ambiente que não tenha a revisão concluída no prazo estipulado;
 - iii. Realizar comunicação formal ao gerente da área de TI, auditoria interna, e ao gerente da área de negócio responsável pelo sistema, módulo ou ambiente que não tenha 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 de direitos de acesso.
- e) Comunicação dos resultados aos responsáveis pelo controle: as alterações propostas foram documentadas e encaminhadas ao gerente de TI e auditoria interna da organização.

Após a finalização das avaliações do nível de maturidade de todos os controles selecionados as melhorias propostas foram consolidadas, dando origem a planos de ação. Os planos de ação foram entregues sob a responsabilidade das áreas de TI,

recursos humanos, jurídico, e segurança física e patrimonial da organização. Os planos de ação que não necessitavam de investimento para serem executados, tais como adequação de diretrizes, procedimentos e cláusulas contratuais, foram selecionados para serem executados primeiro. Os planos de ação que necessitavam de investimento ou exigiam mudanças maiores em infraestrutura de TI ou em processos de negócio serão acompanhados pela organização. A cada novo ciclo de avaliação da maturidade da segurança da informação os controles aplicáveis serão reavaliados e os planos de ação pendentes serão revisados.

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

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

O gráfico 1 apresenta a visualização dos níveis de maturidade médios apurados.

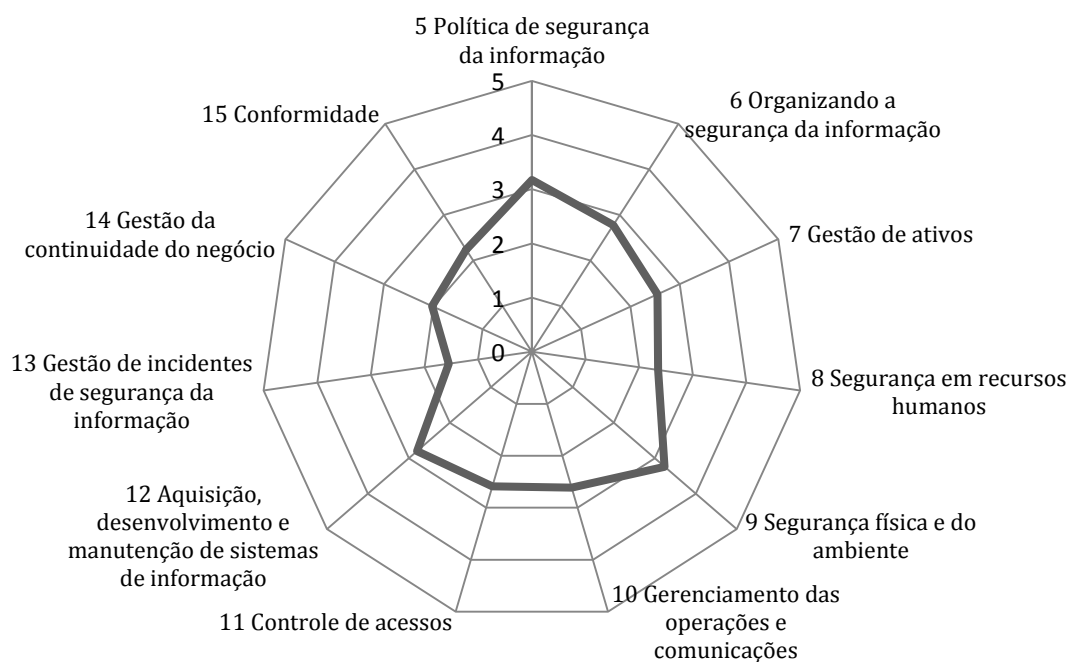


Gráfico 1. Visualização dos níveis de maturidade médios apurados no estudo de caso

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 de segurança possui nível de maturidade adequado à sua realidade, sendo os principais controles relacionados à conformidade com requisitos externos classificados com níveis de maturidade entre 3 e 4. Diversos planos de ação criados estavam relacionados a pequenas melhorias no processo, não necessariamente estando vinculados à alteração do nível de maturidade para um nível maior.

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, quando poderia ter indicado um especialista para cada controle aplicável, nas respectivas áreas de domínio. Esta indicação teria o intuito de gerar comprometimento do especialista com a avaliação e de melhorar a qualidade da avaliação dos controles. O fato de o responsável pela avaliação estar subordinado ao departamento de TI poderia caracterizar falta de independência para avaliação dos controles e emissão de parecer. 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 objetivos de controle da norma ABNT NBR ISO/IEC 27002 por meio de níveis de maturidade proporcionou algumas vantagens para a organização, conforme relato do responsável pela área de TI da organização: “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 necessária para avaliação e direcionamento dos esforços de várias áreas da organização para a melhoria da segurança da informação. Muitas ações de melhoria foram identificadas em virtude da avaliação individual de cada item de controle da norma NBR ISO/IEC 27002, e o modelo de maturidade auxilia na identificação e priorização das ações de melhoria necessárias”.

A organização irá manter as avaliações de maturidade da segurança da informação através de ciclos anuais de avaliação.

7. CONSIDERAÇÕES FINAIS

Este artigo apresenta um instrumento de avaliação que pode ser utilizado por diversos tipos de organizações, através da adoção de uma abordagem de processo para avaliação e melhoria contínua da segurança da informação, do uso de normas sedimentadas e completas relacionadas à segurança da informação, e da medição por níveis de maturidade. Pretendeu-se contribuir com os demais estudos já realizados sobre segurança da informação e maturidade dos processos de gestão.

7.1. Conclusões

A utilização de um instrumento de avaliação da maturidade da segurança da informação pode ser considerada altamente relevante para as organizações, em decorrência da importância que as informações possuem para a realização e continuidade das atividades de negócio.

O presente estudo reúne diversos pontos relevantes sobre o tema segurança da informação e poderá servir de base para novos estudos e pesquisas acadêmicas.

Considera-se que a apresentação e detalhamento de um método para a gestão da segurança da informação de uma organização através da avaliação periódica da maturidade e melhoria contínua dos seus controles foi alcançado. A pesquisa bibliográfica sobre as principais fontes de referência para a segurança da informação e sobre o uso de modelo de maturidade foi ampla o suficiente para embasamento e sustentação do instrumento de avaliação. O uso de uma escala de maturidade, aliado à abordagem de 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 principais trabalhos relacionados apresentados está no uso da norma ABNT NBR ISO/IEC 27002 (ou ISO/IEC 27002) como base de controles para a avaliação, e no uso de um modelo de maturidade para as medições. Este comparativo reforça que a abordagem utilizada por este método de avaliação é adequada ao seu propósito. A principal diferença reside no fato de que os modelos propostos apresentam proposições específicas, estáticas, e que podem não possibilitar ao avaliador a adequada análise dos riscos inerentes ao negócio na medida em que haja evolução das tecnologias, processos e/ou requisitos externos aplicáveis. Outra importante diferença é que este trabalho procura definir um modelo genérico de avaliação, aplicável a todos os tipos de organização independente de tamanho ou área de atuação, através do uso de todos os objetivos de controle de segurança da informação constantes da norma ABNT NBR ISO/IEC 27002.

O autor considera que o uso de modelos com proposições estáticas e específicas para um determinado setor da indústria é útil para avaliadores iniciantes ou inexperientes na interpretação dos controles da norma, pois pode conter exemplos do que deveria ou 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 adequado para avaliadores iniciantes, que devem primeiro compreender e interpretar a norma; 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.

Através dos trabalhos relacionados, que utilizam abordagens semelhantes de avaliação, e da percepção da organização que participou do estudo de caso, pode-se concluir que o método de avaliação apresentado é eficaz para avaliar o estado atual da segurança da informação da organização, para auxiliar nos processos de gestão da segurança da informação e identificação de riscos, e para apoiar a melhoria dos processos e controles internos da organização.

7.2. Sugestões para pesquisas e trabalhos futuros

Como sugestão para pesquisas e trabalhos futuros que venham a contribuir para a melhoria do processo de gestão da segurança da informação, podem ser citados os seguintes itens:

- a) Especificar método para avaliação de riscos dos objetivos de controle, considerando os processos, atividades e controles envolvidos, e vinculando os resultados encontrados a níveis de maturidade mínimos a serem atingidos pela organização;

- b) Aplicar o instrumento de avaliação proposto em outras organizações a fim de se obter uma pesquisa quantitativa sobre a maturidade da segurança da informação e possibilitar comparações entre organizações do mesmo setor;
- c) Melhorar a documentação do processo de análise, criando-se modelos que possam ser utilizados em todas as fases e etapas de avaliação;
- d) Inserir no ciclo de avaliação uma fase para auditoria independente dos resultados, para os casos em que a organização optar pela auto avaliação.

8. Referências

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 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.
- CUNHA, Renato Menezes da. Modelo de Governança da Segurança da Informação no Escopo da Governança Computacional. Universidade Federal de Pernambuco. Programa de Pós-Graduação em Engenharia de Produção. 2008. Disponível em <http://www.btdt.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. Pontifícia Universidade Católica do Rio Grande do Sul. Faculdade de Administração, Contabilidade e Economia. Mestrado em Administração e Negócios. 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.
- 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. Módulo Security Solutions.
- SÊMOLA, Marcos. Gestão da Segurança da Informação: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de Janeiro: Campus, 2003. 154 p.

**ANEXO A – Formulário para avaliação do nível de maturidade da
segurança da informação**

Formulário para avaliação do nível de maturidade da segurança da informação

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual	Nível de Maturidade Objetivo	Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
5			Política de segurança da informação						
5	1		Política de segurança da informação						
5	1	1	Documento da política de segurança da informação						
5	1	2	Análise crítica da política de segurança da informação						
6			Organizando a segurança da informação						
6	1		Organização interna						
6	1	1	Comprometimento da organização com a segurança da informação						
6	1	2	Coordenação da segurança da informação						
6	1	3	Atribuição de responsabilidades para a segurança da informação						
6	1	4	Processo de autorização para os recursos de processamento da informação						
6	1	5	Acordos de confidencialidade						
6	1	6	Contato com autoridades						
6	1	7	Contato com grupos especiais						
6	1	8	Análise crítica independente da segurança da informação						
6	2		Partes externas						
6	2	1	Identificação dos riscos relacionados com partes externas						
6	2	2	Identificando a segurança da informação, quando tratando com os clientes						
6	2	3	Identificando segurança da informação nos acordos com terceiros						
7			Gestão de ativos						
7	1		Responsabilidade pelos ativos						
7	1	1	Inventário dos ativos						
7	1	2	Proprietário dos ativos						
7	1	3	Uso aceitável dos ativos						
7	2		Classificação da informação						
7	2	1	Recomendações para classificação						
7	2	2	Rótulos e tratamento da informação						
8			Segurança em recursos humanos						
8	1		Antes da contratação						
8	1	1	Papéis e responsabilidades						
8	1	2	Seleção						
8	1	3	Termos e condições de contratação						
8	2		Durante a contratação						
8	2	1	Responsabilidades da direção						

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual	Nível de Maturidade Objetivo	Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
8	2	2	Conscientização, educação e treinamento em segurança da informação						
8	2	3	Processo disciplinar						
8	3		Encerramento ou mudança da contratação						
8	3	1	Encerramento de atividades						
8	3	2	Devolução de ativos						
8	3	3	Retirada de direitos de acesso						
9			Segurança física e do ambiente						
9	1		Áreas seguras						
9	1	1	Perímetro de segurança física						
9	1	2	Controles de entrada física						
9	1	3	Segurança em escritórios, salas e instalações						
9	1	4	Proteção contra ameaças externas e do meio ambiente						
9	1	5	Trabalhando em áreas seguras						
9	1	6	Acesso do público, áreas de entrega e de carregamento						
9	2		Segurança de equipamentos						
9	2	1	Instalação e proteção do equipamento						
9	2	2	Utilidades						
9	2	3	Segurança do cabeamento						
9	2	4	Manutenção dos equipamentos						
9	2	5	Segurança de equipamentos fora das dependências da organização						
9	2	6	Reutilização e alienação segura de equipamentos						
9	2	7	Remoção da propriedade						
10			Gerenciamento das operações e comunicações						
10	1		Procedimentos e responsabilidades operacionais						
10	1	1	Documentação dos procedimentos de operação						
10	1	2	Gestão de mudanças						
10	1	3	Segregação de funções						
10	1	4	Separação dos recursos de desenvolvimento, teste e de produção						
10	2		Gerenciamento de serviços terceirizados						
10	2	1	Entrega de serviços						
10	2	2	Monitoramento e análise crítica de serviços terceirizados						
10	2	3	Gerenciamento de mudanças para serviços terceirizados						
10	3		Planejamento e aceitação dos sistemas						
10	3	1	Gestão de capacidade						
10	3	2	Aceitação de sistemas						
10	4		Proteção contra códigos maliciosos e códigos móveis						
10	4	1	Controles contra códigos maliciosos						
10	4	2	Controles contra códigos móveis						
10	5		Cópias de segurança						
10	5	1	Cópias de segurança das informações						

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual	Nível de Maturidade Objetivo	Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
10	6		Gerenciamento da segurança em redes						
10	6	1	Controles de redes						
10	6	2	Segurança dos serviços de rede						
10	7		Manuseio de mídias						
10	7	1	Gerenciamento de mídias removíveis						
10	7	2	Descarte de mídias						
10	7	3	Procedimentos para tratamento de informação						
10	7	4	Segurança da documentação dos sistemas						
10	8		Troca de informações						
10	8	1	Políticas e procedimentos para troca de informações						
10	8	2	Acordos para troca de informações						
10	8	3	Mídias em trânsito						
10	8	4	Mensagens eletrônicas						
10	8	5	Sistemas de informações de negócios						
10	9		Serviços de comércio eletrônico						
10	9	1	Comércio eletrônico						
10	9	2	Transações online						
10	9	3	Informações publicamente disponíveis						
10	10		Monitoramento						
10	10	1	Registros de auditoria						
10	10	2	Monitoramento do uso do sistema						
10	10	3	Proteção das informações dos registros (log)						
10	10	4	Registros (log) de administrador e operador						
10	10	5	Registros (log) de falhas						
10	10	6	Sincronização dos relógios						
11			Controle de acessos						
11	1		Requisitos de negócio para controle de acesso						
11	1	1	Política de controle de acesso						
11	2		Gerenciamento de acesso do usuário						
11	2	1	Registro de usuário						
11	2	2	Gerenciamento de privilégios						
11	2	3	Gerenciamento de senha do usuário						
11	2	4	Análise crítica dos direitos de acesso de usuário						
11	3		Responsabilidades dos usuários						
11	3	1	Uso de senhas						
11	3	2	Equipamento de usuário sem monitoração						
11	3	3	Política de mesa limpa e tela limpa						
11	4		Controle de acesso à rede						
11	4	1	Política de uso dos serviços de rede						
11	4	2	Autenticação para conexão externa do usuário						
11	4	3	Identificação de equipamentos em redes						

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual	Nível de Maturidade Objetivo	Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
11	4	4	Proteção de portas de configuração e diagnóstico remotos						
11	4	5	Segregação de redes						
11	4	6	Controle de conexão de rede						
11	4	7	Controle de roteamento de redes						
11	5		Controle de acesso ao sistema operacional						
11	5	1	Procedimentos seguros de entrada no sistema (log-on)						
11	5	2	Identificação e autenticação de usuário						
11	5	3	Sistema de gerenciamento de senha						
11	5	4	Uso de utilitários de sistema						
11	5	5	Limite de tempo de conexão						
11	5	6	Limitação de horário de conexão						
11	6		Controle de acesso à aplicação e à informação						
11	6	1	Restrição de acesso à informação						
11	6	2	Isolamento de sistemas sensíveis						
11	7		Comutação móvel e trabalho remoto						
11	7	1	Computação e comunicação móvel						
11	7	2	Trabalho remoto						
12			Aquisição, desenvolvimento e manutenção de sistemas de informação						
12	1		Requisitos de segurança de sistemas de informação						
12	1	1	Análise e especificação dos requisitos de segurança						
12	2		Processamento correto nas aplicações						
12	2	1	Validação dos dados de entrada						
12	2	2	Controle do processamento interno						
12	2	3	Integridade de mensagens						
12	2	4	Validação dos dados de saída						
12	3		Controles criptográficos						
12	3	1	Política para o uso de controles criptográficos						
12	3	2	Gerenciamento de chaves						
12	4		Segurança dos arquivos do sistema						
12	4	1	Controle de software operacional						
12	4	2	Proteção dos dados para teste de sistema						
12	4	3	Controle de acesso ao código-fonte de programa						
12	5		Segurança em processos de desenvolvimento e suporte						
12	5	1	Procedimentos para controle de mudanças						
12	5	2	Análise crítica técnica das aplicações após mudanças no sistema operacional						
12	5	3	Restrições sobre mudanças em pacotes de software						
12	5	4	Vazamento de informações						
12	5	5	Desenvolvimento terceirizado de software						
12	6		Gestão de vulnerabilidades técnicas						

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual	Nível de Maturidade Objetivo	Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
12	6	1	Controle de vulnerabilidades técnicas						
13			Gestão de incidentes de segurança da informação						
13	1		Notificação de fragilidades e eventos de segurança da informação						
13	1	1	Notificação de eventos de segurança da informação						
13	1	2	Notificação de fragilidades de segurança da informação						
13	2		Gestão de incidentes de segurança da informação e melhorias						
13	2	1	Responsabilidades e procedimentos						
13	2	2	Aprendendo com os incidentes de segurança da informação						
13	2	3	Coleta de evidências						
14			Gestão da continuidade do negócio						
14	1		Aspectos da continuidade do negócio, relativos à segurança da informação						
14	1	1	Incluindo segurança da informação no processo de gestão da continuidade do negócio						
14	1	2	Continuidade de negócios e análise/avaliação de riscos						
14	1	3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação						
14	1	4	Estrutura do plano de continuidade do negócio						
14	1	5	Testes, manutenção e reavaliação dos planos de continuidade do negócio						
15			Conformidade						
15	1		Conformidade com requisitos legais						
15	1	1	Identificação da legislação aplicável						
15	1	2	Direitos de propriedade intelectual						
15	1	3	Proteção de registros organizacionais						
15	1	4	Proteção de dados e privacidade de informações pessoais						
15	1	5	Prevenção de mau uso de recursos de processamento da informação						
15	1	6	Regulamentação de controles de criptografia						
15	2		Conformidade com normas e políticas de segurança da informação e conformidade técnica						
15	2	1	Conformidade com as políticas e normas de segurança da informação						
15	2	2	Verificação da conformidade técnica						
15	3		Considerações quanto à auditoria de sistemas de informação						
15	3	1	Controles de auditoria de sistemas de informação						
15	3	2	Proteção de ferramentas de auditoria de sistemas de informação						