Um Modelo de Sistema de Gestão da Segurança da Informação Baseado nas Normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008

Valdeci Otacilio dos Santos & Renato Baldini Filho

***Abstract*—This paper proposes a model of information security management system, covering the main guidelines recommended in the standards ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. The model aims to guide the implementation of a new system for managing information security in an organization or verify the conformity of an existing system. The work includes the result of a practical application of the proposed model in the verification of an information security management system within an organization.**

***Index Terms*—Information. Information security. Information security management.**

***Resumo*—Este artigo propõe um modelo de sistema de gestão da segurança da informação, contemplando as principais diretrizes preconizadas nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. O modelo visa guiar a implementação de um novo sistema de gestão da segurança da informação em uma organização ou verificar a conformidade de um sistema já existente. O trabalho compreende o resultado de uma aplicação prática do modelo proposto na verificação de um sistema de gestão da segurança da informação de uma organização.**

***Palavras chave*—Informação. Segurança da informação. Gestão da segurança da informação.**

I. Introdução

A informação constitui um bem de grande valor para a sociedade como um todo e, em particular, para as organizações públicas ou privadas. Devido à sua importância e ao crescimento das ameaças e vulnerabilidades nos sistemas de informação, surge a necessidade de adoção de medidas de proteção eficientes.

A segurança da informação é entendida como a preservação das propriedades de disponibilidade, integridade, confidencialidade, autenticidade, responsabilidade, não repúdio e confiabilidade da informação (ABNT, 2006, p. 2).

Segundo a ABNT (2005, p. 2), a segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar o risco aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

Conforme descrito em Brasil (2001, p. 4), a segurança da informação compreende um conjunto de medidas, normas e procedimentos destinados a proteger a informação em todo o seu ciclo de utilidade.

Para garantir a proteção da informação contra as ameaças existentes, tornam-se necessários o estabelecimento e a implementação de políticas, processos e procedimentos que sejam, respectivamente, um conjunto de diretrizes, ações e instruções, que compreendem a chamada gestão da segurança da informação organizacional.

Existem atualmente várias normas nacionais e internacionais que tratam da segurança da informação. Essas normas visam nortear as atividades a serem realizadas a fim de tornarem os sistemas de informação mais seguros. Em particular, destacamos as normas ISO/IEC da família 27000, que são padrões internacionais publicadas pela *International Organization for Standardization* (ISO) e possuem suas versões brasileiras publicadas pela Associação Brasileira de Normas Técnicas (ABNT).

As diversas normas que compõem a família ISO/IEC 27000 abordam os diversos enfoques voltados à segurança da informação de maneira particular, embora haja uma forte relação entre cada norma. A velocidade do avanço tecnológico na área da informação e comunicações faz com que os requisitos de segurança da informação e comunicações organizacionais sejam muito dinâmicos, o que exige um acompanhamento e aprimoramento constante das políticas, processos e procedimentos de segurança. Nesse sentido, a criação de um mecanismo que consolide as orientações e abordagens contempladas nas principais normas e facilite o entendimento da constituição e relacionamentos existentes entre os diversos processos que são desenvolvidos com o objetivo de alcançar um nível de segurança adequado contribuirá para que as organizações implementem ou verifiquem os seus sistemas de gestão da segurança da informação (SGSI) com menores custos, menor tempo e maior eficiência e eficácia.

O objetivo deste trabalho é propor um modelo de sistema de gestão da segurança da informação (SGSI), com mapeamento dos processos, baseado nas normas ABNT NBR ISO/IEC 27001 (ABNT, 2006), 27002 (ABNT, 2005) e 27005 (ABNT, 2008). A finalidade é constituir um guia prático de orientação, que possibilite a uma organização implementar ou averiguar a situação em que se encontra seu sistema de gestão da segurança da informação, em conformidade com as principais normas existentes.

II. Gestão da Segurança da Informação

A grande maioria das organizações atuais possui todos os seus processos baseados ou suportados por sistemas digitais de informação. Para que esses sistemas funcionem adequadamente, de modo a propiciar um serviço confiável e de qualidade aos seus clientes, torna-se necessária uma perfeita gestão da segurança da informação e comunicações, visando alinhá-la aos objetivos de negócio da organização.

Conforme descrito em Brasil (2008, p. 2), a gestão da segurança da informação e comunicações é entendida como: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

Segundo a ABNT (2006, p. 1), o sistema de gerenciamento da segurança da informação é projetado para assegurar a seleção de controles de segurança adequados para proteger os ativos de informação da organização.

A. A Norma ABNT NBR ISO/IEC 27001:2006

A norma ABNT 27001 (ABNT, 2006) é uma evolução da norma BS 7799-2, que foi publicada pelo BSI (*British Standard Institute*) em 1999. Ela fornece um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Essa norma utiliza o modelo "*Plan-Do-Check-Act*" (PDCA), que é aplicado na estruturação de processos de melhoria contínua. A Tabela I descreve os estágios do ciclo de tal modelo com suas respectivas atividades.

TABELA I
CICLO DO MODELO PDCA APLICADO AO SGSI.

ESTÁGIO	ATIVIDADES
Plan (P) Planejar	Planejamento das ações de segurança a serem desenvolvidas, de acordo com as características, objetivos e requisitos da organização. Incluem o estabelecimento de políticas, processos e procedimentos de segurança, objetivos a serem alcançados e gestão de riscos.
Do (D) Fazer	Implementação das ações de segurança planejadas no estágio anterior.
Check (C) Verificar	Avaliação das ações de segurança implementadas e análise crítica dos resultados alcançados.
Act (A) Agir	Aperfeiçoamento das ações de segurança, de acordo com o monitoramento realizado ou novas informações obtidas, de modo que seja alcançada a melhoria contínua do sistema.

B. A Norma ABNT NBR ISO/IEC 27002:2005

A norma ABNT 27002 (ABNT, 2005) integra o conjunto de normas ISO/IEC 27000, voltadas para a gestão da segurança da informação. Essa norma teve origem na BS 7799-1, publicada pelo BSI (*British Standard Institute*) em 1995, que em 2000 tornou-se a norma ISO 17799. A norma 27002 estabelece um conjunto de controles, com as respectivas diretrizes de implementação, visando à gestão da segurança da informação. Os diversos controles sugeridos pela norma estão grupados em onze seções descritas como: política de segurança da informação; organizando a segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção dos sistemas de informação; gestão de incidentes de segurança da informação; gestão da continuidade do negócio; e conformidade.

C. A Norma ABNT NBR ISO/IEC 27005:2008

A norma ABNT 27005 (ABNT, 2008) fornece as diretrizes para o processo de gestão de riscos de segurança da informação de uma organização. Essa norma foi originalmente publicada em 2005 como BS 7799-3 pelo BSI. A Tabela II descreve as atividades que são desenvolvidas nesse processo.

TABELA II
ATIVIDADES DO PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO.

ATIVIDADE	DESCRIÇÃO
Definição do contexto	- Definição de critérios básicos para a gestão de riscos (critérios para avaliação do risco, determinação dos impactos dos incidentes e aceitação do risco). - Definição do escopo e limites da gestão de riscos. - Estabelecimento de organização apropriada para operar a gestão de riscos.
Identificação de riscos	- Identificação dos ativos. - Identificação das ameaças. - Identificação dos controles existentes. - Identificação das vulnerabilidades. - Identificação das consequências dos incidentes de segurança sobre os ativos identificados.
Estimativa de riscos	Atribui valores aos riscos de acordo com as consequências que o risco pode causar e a sua probabilidade de ocorrência. A metodologia a ser utilizada pode ser qualitativa ou quantitativa.
Avaliação de riscos	Ordenação dos riscos por prioridade de acordo com os critérios de avaliação de riscos definidos no contexto.
Tratamento do risco	- Seleção dos controles para reduzir o risco (baixar o nível do risco para valor aceitável). - Reter o risco (quando o risco atende aos critérios de aceitação definidos na definição do contexto). - Evitar o risco (para riscos considerados demasiadamente elevados, compreende a eliminação da atividade ou mudança das condições de operação). - Transferir o risco (compartilhar ou transferir o risco para outra entidade). - Definição do plano de tratamento do risco.
Aceitação do risco	Registro formal da decisão de aceitar o risco por parte dos gestores.
Comunicação do risco	Troca de informação sobre risco entre o tomador de decisão e demais partes interessadas.
Monitoramento e análise crítica de riscos	Atividades que visam identificar mudanças no contexto organizacional e panorama de riscos (ativos, ameaças, vulnerabilidades, controles, impactos, probabilidade de ocorrência), visando aprimorar o processo de gestão de riscos.

O processo de gestão de riscos de segurança da informação proposto pela norma ABNT 27005 é executado de maneira iterativa, sendo constituído pelas seguintes atividades: definição do contexto, identificação de riscos, estimativa de riscos, avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica

do risco (ABNT, 2008).

As atividades de identificação e estimativa de riscos constituem a análise de riscos. Ao final da fase de análise e avaliação de riscos e da fase de tratamento dos riscos, existe um ponto de decisão entre a continuidade do processo ou o retorno para alguma fase anterior, caso o resultado não esteja em um nível considerado satisfatório. O número de iterações a serem realizadas no processo dependerá do nível de adequação aos requisitos de segurança da informação da organização, alcançado ao término das fases de análise e avaliação de riscos e de tratamento do risco.

Além da abordagem das diversas atividades constituintes do processo de gestão de riscos, a norma ABNT 27005 contempla, em seus anexos, informações como: detalhamento da definição de contexto, identificação e valoração dos ativos, avaliação do impacto, exemplos de ativos, ameaças, vulnerabilidades comuns e diferentes abordagens sobre análise/avaliação de riscos de segurança da informação e restrições relativas à redução do risco (ABNT, 2008).

A busca da segurança da informação é realizada por meio da implementação de controles que visam minimizar os riscos existentes. Dessa forma, é possível perceber a importância que a gestão de riscos representa para a segurança da informação, pois o desconhecimento da magnitude dos riscos aos quais determinada organização está exposta certamente comprometerá a tarefa de decisão sobre investimentos em controles de segurança.

III. Modelo de Sistema de Gestão da Segurança da Informação (SGSI)

Esta seção apresenta um modelo de sistema de gestão da segurança da informação que procura abranger as diretrizes preconizadas nas normas ABNT NBR ISO/IEC 27001 (que trata dos requisitos de um SGSI), 27002 (código de prática com a descrição dos controles de segurança a serem implementados) e 27005 (gestão de riscos de segurança da informação). Nesse modelo, cada enfoque referente a um sistema de gestão da segurança da informação é visto sob a perspectiva de um processo, cada qual com seus objetivos, que recebem entradas, executam atividades e oferecem saídas. Dessa forma, o SGSI é constituído por um conjunto de processos inter-relacionados. As Figuras 1 e 2 ilustram o modelo de sistema de gestão de segurança da informação proposto, onde são mapeados, respectivamente, os processos que interligam o SGSI com o ambiente externo e os processos que constituem o sistema propriamente dito, o qual denominamos núcleo do SGSI.

Analisando a Figura 1, percebe-se que interagem com o SGSI os seguintes componentes: a direção da organização, por meio dos processos de análise crítica do sistema e de sua implementação e manutenção, os intervenientes e a infraestrutura de tecnologia da informação.

A direção é responsável pelo estabelecimento e manutenção do SGSI, apoiando e manifestando seu comprometimento com a segurança da informação, bem como pela realização da análise crítica do sistema.

A análise crítica do sistema é o processo que consiste na verificação do SGSI, apontando suas deficiências e implementando melhorias.

O processo de implementação, manutenção e melhoria destina-se a estabelecer, manter e melhorar o SGSI, de acordo com os princípios, requisitos gerais e expectativas de segurança da informação da organização.

Os intervenientes são as partes interessadas, representados pelos sócios de uma organização privada ou a sociedade em geral, para uma organização pública. Fornecem ao sistema os requisitos gerais de segurança, os princípios que norteiam tal organização, bem como as expectativas em relação à segurança da informação.

A infraestrutura de tecnologia da informação é a base que dá suporte ao desenvolvimento do sistema de gestão de segurança da informação. Portanto a infraestrutura de tecnologia da informação é o alicerce de todos os demais elementos do sistema.

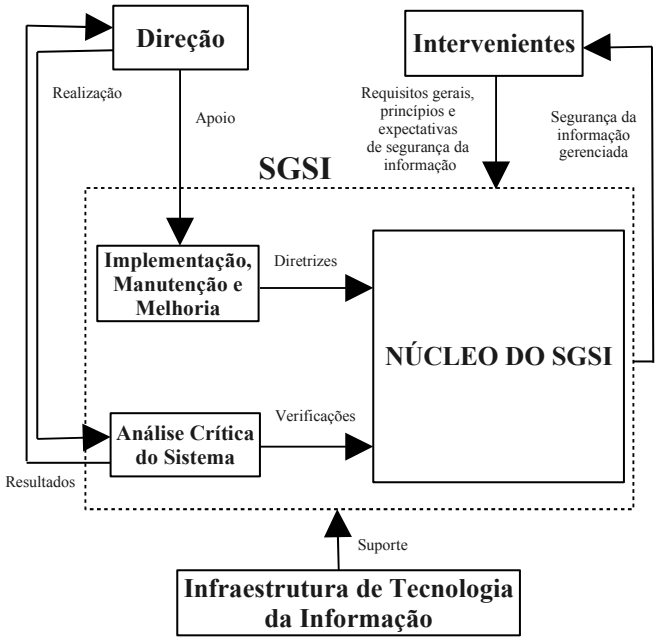

Fig. 1. Mapeamento do SGSI com o ambiente externo.

A Figura 2 apresenta os diversos processos que constituem o núcleo do SGSI e que implementam os controles visando a busca da segurança da informação, onde se desenvolvem os seguintes processos básicos: política de segurança da informação, assessoria jurídica e gestão de riscos de segurança da informação.

Esse modelo serve de guia de orientação na implementação de um SGSI, bem como de verificação da conformidade de um sistema implementado, possibilitando analisar o nível de aderência, que representa o grau de conformidade dos processos existentes ao que está preconizado nas normas ABNT NBR ISO/IEC 27001, 27002 e 27005.

Cada processo do SGSI deve implementar as atividades descritas nas normas utilizadas como referência em um nível compatível com os requisitos de segurança e as características da organização onde o sistema é empregado.

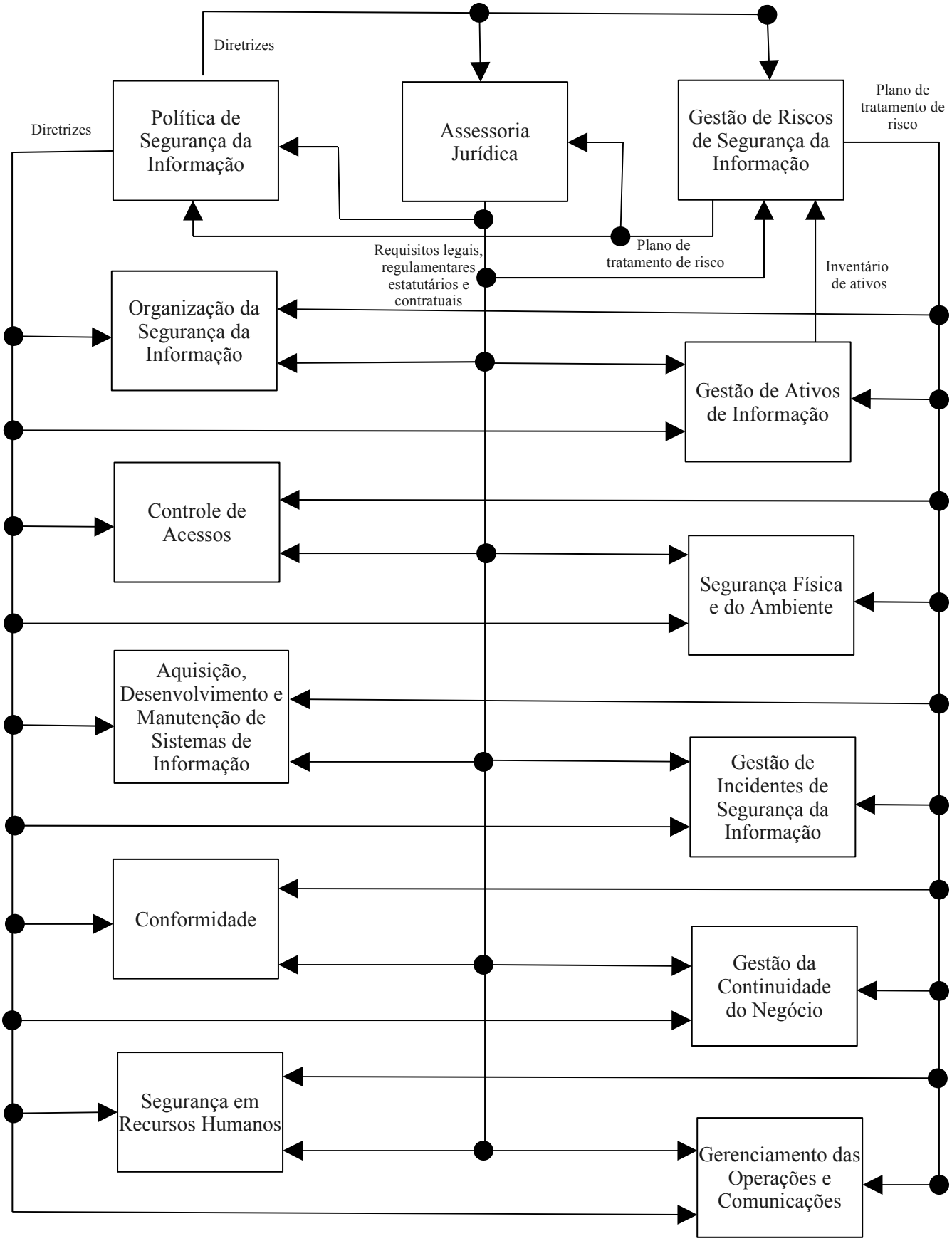

Fig. 2. Mapeamento dos Processos Integrantes do Núcleo do SGSI.

IV. Resultados da Aplicação do Modelo de Sistema de Gestão da Segurança da Informação

O modelo de gestão da segurança da informação proposto foi aplicado na verificação do nível de aderência da gestão da segurança da informação de uma organização.

A verificação da situação da organização foi realizada por meio da análise de documentos e arquivos, entrevista com pessoas que integram as diversas áreas da organização e observação direta dos sistemas de informação, junto ao ambiente organizacional.

Para quantificar o nível de aderência da organização ao que está preconizado nas normas contempladas pelo modelo, as atividades que compõem os diversos processos que fazem parte do sistema de gestão da segurança da informação, estabelecidas nas normas ABNT 27001, 27002 e 27005, foram valoradas de duas maneiras, conforme abaixo descritas:

- **Ponderação quanto ao grau de relevância:** determina o valor que cada atividade representa para o negócio da organização, conforme especificado na Tabela III.
- **Valoração quanto ao nível de implementação:** refere-se ao valor atribuído para cada atividade de acordo com seu nível de implementação por parte da organização, conforme discriminado na Tabela IV.

Para tornar possível o cômputo do nível de aderência das atividades de cada processo, houve a necessidade de estabelecer um valor de referência, que representa a situação julgada ideal para aquela organização específica. Tal valor de referência foi obtido pela multiplicação da valoração correspondente ao grau de relevância da atividade pela valoração máxima possível da Tabela IV, ou seja, atividade com nível de implementação total.

Por meio da pesquisa junto ao ambiente organizacional, obteve-se o valor apurado para cada atividade, que é calculado multiplicando-se a valoração obtida quanto ao grau de relevância da atividade para a organização pela valoração referente ao nível de implementação da referida atividade. Esse valor apurado foi comparado com o valor de referência da atividade, sendo expressa em termos percentuais.

A descrição e os níveis de aderência das atividades que compõem cada processo do sistema analisado não fazem parte dos escopo deste trabalho, sendo apresentada apenas a consolidação dos níveis de aderência por processo do SGSI.

A Tabela V apresenta os níveis de aderência, em termos percentuais, de cada processo que compõe o sistema de gestão da segurança da informação (SGSI) observado, em relação ao que está previsto nas normas que serviram de base para confecção do modelo. Tais níveis foram obtidos por meio da comparação entre o somatório dos valores apurados e de referência, relativos às diversas atividades que compõem o processo.

TABELA III
Ponderação do Grau de Relevância das Atividades.

GRAU DE RELEVÂNCIA	VALOR
Nenhuma relevância	0
Baixa relevância	1
Média relevância	2
Alta relevância	3

TABELA IV
Valoração do Nível de Implementação das atividades.

NÍVEL DE IMPLEMENTAÇÃO	VALOR
Não implementada	0
Implementação parcial baixa	1
Implementação parcial alta	2
Implementação total	3

TABELA V
Nível de Aderência por Processo do SGSI.

PROCESSO	NÍVEL DE ADERÊNCIA
Implementação, Manutenção e Melhoria do Sistema de Gestão da Segurança da Informação (SGSI)	59,26%
Organização da Segurança da Informação	65,79%
Política de Segurança da Informação	69,00%
Gestão de Riscos de Segurança da Informação	19,54%
Assessoria Jurídica	66,66%
Gestão de Ativos de Informação	55,55%
Segurança em Recursos Humanos	69,23%
Segurança Física e do Ambiente	86,49%
Gerenciamento de Operações e Comunicações	77,55%
Controle de Acessos	88,13%
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	85,03%
Gestão de Incidentes de Segurança da Informação	33,33%
Gestão da Continuidade do Negócio	51,11%
Conformidade	64,37%
Análise Crítica do Sistema de Gestão da Segurança da Informação (SGSI)	27,78%

A média geral da aderência do SGSI analisado, obtida por meio do cômputo da média aritmética dos processos, foi de 61,25%. Esse valor demonstra o grau de conformidade da gestão da segurança da informação organizacional em relação ao que está previsto nas normas utilizadas como referência para confecção do modelo utilizado.

Analisando os níveis de aderência de cada processo, percebe-se que os processos de gestão de riscos de segurança da informação (com 19,54%), análise crítica do sistema de gestão da segurança da informação (com 27,78%) e gestão de incidentes de segurança da informação (com 33,33%) destacam-se por possuírem valores muito abaixo da média geral do sistema.

V. Conclusões

Este trabalho procurou elaborar um modelo de sistema de gestão da segurança da informação em que os principais processos que compõem tal sistema foram mapeados. O

modelo procurou abranger as diretrizes contidas nas normas ABNT NBR ISO/IEC 27001, 27002 e 27005, de forma que fosse possível a obtenção de uma visão geral dos pontos relacionados à segurança da informação em uma organização.

O modelo proposto pode ser usado como um guia para implementação de um sistema de gestão da segurança da informação ou para a verificação da conformidade de um sistema já existente. Ele não visa, de forma alguma, substituir as normas que serviram de base para a sua confecção, mas, sim, realizar uma consolidação das diretrizes que são estabelecidas em tais normas.

O resultado da aplicação do modelo, na verificação da situação da segurança da informação em uma organização, mostrou o nível de aderência do sistema existente com as diretrizes previstas na normatização. Analisando os resultados da verificação, é possível identificar os pontos fortes e fracos em cada processo que constitui o sistema, quando comparados com a situação julgada ideal, de acordo com as características do negócio da organização. Os pontos fortes são constituídos pelo alto nível de implementação por parte da organização das atividades consideradas relevantes para a segurança da informação organizacional, já os pontos fracos são aqueles em que as atividades previstas no modelo, apesar de serem relevantes para a segurança da informação, apresentam um baixo grau de implementação.

O resultado da aplicação realizada mostra um ponto considerado relevante, no que se refere ao processo de gestão de riscos de segurança da informação, pois o referido processo apresentou o nível de aderência mais baixo do sistema, com 19,54%. Essa constatação é considerada importante pelo fato da gestão de riscos de segurança da informação constituir um dos pilares do sistema de gestão da segurança da informação, haja vista que a idealização de qualquer plano de defesa sobre algum risco só será viabilizada se tal risco for conhecido e mensurado.

A aplicação do modelo descrita na Seção IV utilizou, como forma de cálculo do nível geral de aderência do sistema de gestão da segurança da informação analisado, a média aritmética dos percentuais de aderência obtidos em cada processo. Ao ser adotada essa forma de cálculo, partimos do princípio de que todos os processos que constituem o sistema possuem o mesmo grau de relevância para a segurança da informação da organização. Porém uma outra maneira de realizar o cômputo geral do nível de aderência do SGSI de uma organização seria o cálculo da média ponderada dos diversos processos, em que cada processo teria um peso que representaria a sua importância para a segurança da informação para aquela organização especificamente.

Portanto a forma como será determinado o nível de segurança ideal, bem como calculado o nível de aderência do sistema, é flexível e adaptável às características de cada organização.

Como pode ser observado pela análise das Figuras 1 e 2, o estabelecimento e implementação de uma política de segurança da informação e de um processo de gestão de riscos de segurança da informação, aliados à infraestrutura de tecnologia da informação, podem ser considerados os pilares fundamentais de um sistema de gestão da segurança da informação.

Sendo assim, o aprimoramento desses três elementos contribui de maneira significativa para a implementação dos demais componentes do sistema, fazendo com que a organização gerencie a segurança da informação de forma mais eficiente e eficaz.

Como trabalhos futuros, é sugerido que o modelo proposto, composto pelo arcabouço de tópicos utilizados, seja replicado em outras organizações com características semelhantes, possibilitando, dessa forma, a verificação de tendências nos resultados alcançados, bem como o aprimoramento desse modelo, por meio da inserção de outros elementos/enfoques julgados relevantes e exclusão daqueles considerados sem aplicação no contexto da organização pesquisada. Um trabalho mais amplo estenderia a aplicação do modelo na verificação dos sistemas de gestão da segurança da informação em um número de organizações que integram áreas distintas, tanto do setor público como privado, tais como comércio, educação, saúde, etc. Dessa forma, seria possível traçar um perfil de como é tratada a segurança da informação nas mais diversas áreas e setores.

Referências

[1] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002: *Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação*, 2005.

[2] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27001: *Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação – Requisitos*, 2006.

[3] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005: *Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação*, 2008.

[4] BRASIL. Exército Brasileiro. Gabinete do Comandante do Exército. *Instruções Gerais de Segurança da Informação para o Exército Brasileiro*. Brasília, DF, 2001.

[5] BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Instrução Normativa GSI/PR nº 1*. Brasília, DF, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: julho de 2012.

Valdeci Otacilio dos Santos é tecnólogo em processamento de dados (FATEC-AM, 2004) e especialista em gestão da segurança da informação e comunicações (UNB, 2011).

Renato Baldini Filho é professor titular do departamento de comunicações, da faculdade de engenharia elétrica da Unicamp.