IX SEGeT 2012
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
Tema: Gestão, Inovação e Tecnologia para a Sustentabilidade

Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança

Marcos Paulo Konzen
marcoskonzen@gmail.com
UFSM

Lisandra Manzoni Fontoura
lisandramf@gmail.com
UFSM

Raul Ceretta Nunes
ceretta@inf.ufsm.br
UFSM

Resumo:O despreparo das organizações para lidar com a segurança da informação as tornam mais vulneráveis às ameaças e os impactos causados pelos eventos negativos tendem a serem maiores. Com isso, a implantação da gestão da segurança das informações é fundamental para minimizar os riscos e garantir a continuidade do negócio, maximizando as oportunidades de competitividade. Este artigo propõe o uso de padrões de segurança para atender as diretrizes da norma ISO/IEC 27005:2008. Para isso, são associados padrões às atividades da norma. Essa associação pode facilitar a elaboração do processo da norma e dar maiores garantias do uso de práticas recomendadas. No final, o artigo ilustra a utilização de padrões de segurança.

Palavras Chave: Gestão de Riscos - Padrões de Segurança - ISO/IEC 27005 - Segurança da Informa - Normas de Segurança

1. INTRODUÇÃO

Na economia atual, a informação é um dos principais ativos das organizações. É através dela que as empresas gerenciam seus produtos ou serviços e traçam suas estratégias, tornando os sistemas de informações ativos críticos que necessitam serem protegidos contra ameaças que podem explorar as vulnerabilidades do sistema. Estas violações na segurança podem causar a perda da confidencialidade, integridade e disponibilidade das informações, gerando perdas financeiras e competitivas por parte das empresas afetadas (KROLL *et al*, 2010; AMARAL; AMARAL; NUNES, 2010).

Muitas organizações, sejam elas públicas ou privadas, ainda se mostram despreparadas para lidar com a segurança da informação. Isso decorre do fato dessas empresas possuírem poucos instrumentos de proteção, agravados pelo despreparo gerencial, tornando-as mais vulneráveis às ameaças, com isso os impactos causados pelos eventos negativos tendem a ser mais fortes (LUNARDI; DOLCI, 2006).

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Gerenciar os riscos pode ser um processo complexo e oneroso, contribuindo para que as empresas não priorizem esse processo em projetos de segurança da informação (OLIVEIRA *et al*, 2009).

Existem normas e metodologias que guiam o desenvolvimento de uma gestão de riscos, onde cada uma fornece um conjunto de diretrizes distintas para o gerenciamento dos riscos. Dentre os modelos de referência para gestão dos riscos que visam nortear as implementações necessárias está a ISO/IEC 27005 (2008). O processo descrito na norma forma um embasamento para a construção de metodologias para gestão de riscos dizendo o que a organização deve fazer, mas não detalha suficientemente como executar as atividades, dificultando a sua implementação por partes das organizações.

Considerando que, Padrões de Segurança (*Security Patterns*) descrevem boas soluções para problemas recorrentes de segurança da informação (WAGNER; FONTOURA; FONTOURA, 2011), a proposta desse trabalho é facilitar a elaboração de metodologias de gestão de riscos por meio da associação de padrões às atividades indicadas na norma. Organizações que desejam elaborar processos consistentes com a ISO/IEC 27005 podem usar os padrões sugeridos para implantação de metodologias de gestão de riscos, dessa forma facilitando a tarefa de elaboração de metodologias e usando práticas já consagradas descritas pelos padrões.

Este artigo faz uma leitura da estrutura do processo da norma ISO/IEC 27005 , identificando as diretrizes de cada atividade e apresenta padrões de segurança que descrevem soluções de gestão de riscos que satisfazem as diretrizes da norma. Padrões de segurança descrevem pequenos processos, ou partes de processo, que podem ser reusados para compor diferentes processos. Deste modo, o artigo tem como principal contribuição a proposição de utilizar padrões de segurança para garantir o uso de práticas recomendadas na implementação de soluções de gestão de risco segundo as diretrizes da norma ISO/IEC 27005 .

O artigo está organizado da seguinte maneira: na Seção 2 é descrito como o processo de gestão de riscos deve ser conduzido, se considerada a norma ISO/IEC 27705 ; na Seção 3 são apresentados os padrões de segurança que podem ser utilizados para a gestão de riscos; na Seção 4 é proposta a associação dos padrões de segurança às atividades do processo de gestão de riscos segundo a norma ISO/IEC 27005 ; na seção 5 é ilustrada uma atividade elaborada a partir de um padrão; na Seção 6 são apresentados alguns trabalhos relacionados; na Seção 7 são apresentadas as considerações finais; e, para concluir, na Seção 8 as referências.

2. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E A NORMA ISO/IEC 27005:2008

Riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade e disponibilidade das informações de uma organização (ABNT NBR ISO/IEC 27005, 2008). Já Oliveira (2006) classifica os riscos como sendo uma oportunidade, uma incerteza ou uma ameaça. Esta última como sendo de maior preocupação, pois está atrelada à ocorrências de efeitos negativos como, por exemplo, perda financeira, fraude, roubo, comprometimento da imagem, infração legal, indisponibilidade de serviços, dentre outros (VASILE; STUPARU; DANIASA, 2010).

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visam à identificação, avaliação e priorização de riscos, seguido pela aplicação coordenada e econômica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável.

Devido à importância do processo de gestão de riscos para as organizações, algumas normas internacionais foram criadas com o intuito de nortear os conceitos e práticas de gestão de riscos. Dentre estas normas, pode-se citar a ISO/IEC 27005 , que discute - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. A utilização de normas de segurança da informação garante que a organização está seguindo as diretrizes dos processos de gestão da segurança da informação e possibilita com que a organização seja reconhecida pela utilização de boas práticas em gestão da segurança da informação.

A norma internacional ISO/IEC 27005 é parte da série de normas da ISO/IEC 27000, a qual é uma série bem estabelecida de normas de gestão de segurança da informação e é aceita em todo o mundo. O âmbito de aplicação destas normas pode ser na organização como um todo, ou em partes, como os processos de um departamento, uma aplicação de TI ou uma infraestrutura de TI (BECKERS *et al*, 2011). Esta norma internacional fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI).

A ISO/IEC 27005 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização (LUND; SOLHAUG; STØLEN, 2010). Neste contexto, o processo de gestão de riscos é definido por oito atividades, como pode ser observado na Figura 1.

Para cada atividade da norma são propostas diretrizes para implementação que serão brevemente descritas a seguir (ABNT NBR ISO/IEC 27005, 2008).

A. Definição do contexto

Definir o escopo e limites que serão levados em consideração na gestão de riscos. Deverão ser descritos os processos que fazem parte do escopo, garantindo a identificação dos ativos relevantes para a gestão dos riscos. Além disso, a definição do contexto inclui determinar os critérios gerais de aceitação dos riscos para a organização e as responsabilidades para a gestão de riscos.

A atividade de Análise/Avaliação de Riscos é subdividida em outras três atividades: Identificação de riscos; Estimativa de riscos; e Avaliação de riscos.

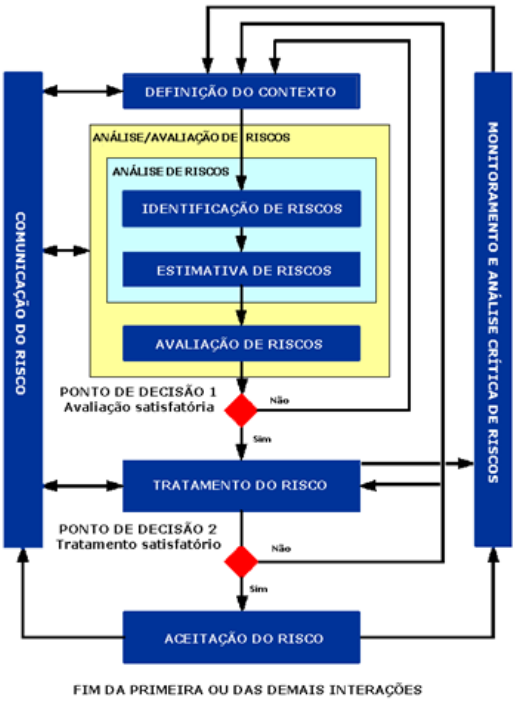

Figura 1: Processo de gestão de riscos de segurança da informação (ABNT NBR ISO/IEC 27005, 2008).

B1. Identificação de riscos

Identificar os eventos que possam ter impacto negativo nos negócios da organização. Devem ser identificados os ativos, suas vulnerabilidades e as ameaças que podem causar *danos aos ativos. Identificar as consequências que as perdas de confidencialidade, de* integridade e de disponibilidade podem ter sobre os ativos.

B2. Estimativa de riscos

Atribuir valor ao impacto que um risco pode ter e a probabilidade de sua ocorrência, de forma qualitativa ou quantitativa. Estimar o risco através da combinação entre a probabilidade de um cenário de incidente e suas consequências.

B3. Avaliação de riscos

Determinar a prioridade de cada risco através de uma comparação entre o nível estimado do risco e o nível aceitável estabelecido pela organização.

O ponto de decisão 1, visto na Figura 1, verifica se a avaliação dos riscos foi satisfatória, conforme os critérios estabelecidos pela organização. Caso não seja satisfatória, a atividade pode ser reiniciada de forma que se possa revisar, aprofundar e detalhar ainda mais a avaliação, assegurando que os riscos possam ser adequadamente avaliados.

C. Tratamento do risco

Implementar controles para reduzir, reter, evitar ou transferir os riscos. Se o tratamento do risco não for satisfatório, ou seja, não resultar em um nível de risco residual que seja aceitável, deve-se iniciar novamente a atividade ou o processo até que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Esta iteração se dá no ponto de decisão 2, como visto na fig. 1.

D. Aceitação do risco

Registrar formalmente a aprovação dos planos de tratamento do risco e os riscos residuais resultantes, juntamente com a responsabilidade pela decisão.

E. Comunicação do risco

Desenvolver planos de comunicação dos riscos para assegurar que todos tenham consciência sobre os riscos e controles a serem adotados.

F. Monitoramento e análise crítica de riscos

Monitorar continuamente os riscos e seus fatores a fim de identificar eventuais mudanças no contexto. Certificar que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriados nas circunstâncias presentes.

A norma ISO/IEC 27005 não inclui uma metodologia específica para a gestão de riscos de segurança da informação, cabendo a cada organização definir a melhor abordagem conforme o contexto na qual está inserida.

3. PADRÕES DE SEGURANÇA (*SECURITY PATTERNS*)

Os padrões de segurança fornecem soluções já consolidadas para problemas recorrentes de segurança e podem servir de referência para atingir os requisitos de segurança (WAGNER; FONTOURA; FONTOURA, 2011). Os padrões capturam a experiência de especialistas em segurança da informação que podem ser aplicados por qualquer organização, definindo uma solução para um problema de segurança dentro de diversos contextos (YOSHIOKA; WASHIZAKI; MARUYAMA, 2008; SUPAPORN; PROMPOON; ROJKANGSADAN, 2007). Os padrões de segurança ajudam na identificação e formulação das práticas e procedimentos de segurança descritos pelas normas de segurança da informação (ROMANOSKY, 2002).

Neste sentido, observa-se que os padrões de segurança podem ser úteis para satisfazer os requisitos de segurança de um SGSI através da reutilização de práticas bem sucedidas para a segurança da informação, podendo ser associados a modelos de referência e utilizados para implementar um processo de gestão de riscos de segurança da informação.

Padrões descrevem detalhadamente soluções para problemas de segurança da informação, por isso podem ser usados para implementar normas. A solução dada pelo padrão deve satisfazer aos objetivos indicados e aos resultados esperados pela implantação dos processos de uma norma (KROLL *et al*, 2010). Neste artigo, propõe-se o uso de padrões de segurança para a definição de atividades para gerenciar os riscos de acordo com a norma ISO/IEC 27005 . Esta proposta pode ajudar as empresas a criar uma base de práticas de segurança que poderá ser reusada para a elaboração de abordagens de segurança e definição de controles.

De acordo com Shumacher *et al* (2006) e Rosado *et al* (2006), os catálogos de padrões incluem uma breve descrição do padrão, que identifica o problema a qual ele propõe resolver e a solução para o problema. A solução descreve as tarefas, a sequência de execução, papéis, relacionamento entre padrões, detalhados suficientemente para facilitar sua implementação. Para facilitar o entendimento de como os padrões são estruturados é apresentado na Seção 5 uma ilustração do uso de padrões com sua descrição e os passos para implementar a solução.

Na Tabela 1, são mostrados alguns padrões que descrevem práticas relacionadas com a gestão de riscos e uma descrição de seus objetivos.

A organização deverá aplicar as soluções que atendam as diretrizes da norma e que sejam suficientes para garantir os requisitos mínimos de segurança para o negócio.

Tabela 1: Padrões de Segurança Relacionados com a Gestão de Riscos.

Padrão de Segurança	*Descrição*
Security needs Identification for Enterprise Assets (SHUMACHER *et al*, 2006)	Identificar as necessidades de segurança e quais propriedades de segurança que devem ser aplicadas para cada ativo.
Asset Valuation (SHUMACHER *et al*, 2006)	Determinar a importância de cada ativo para os negócios da empresa.
Threat Assessment (SHUMACHER *et al*, 2006)	Identificar as ameaças aos ativos; determinar a probabilidade e o potencial de prejuízo de cada ameaça.
Vulnerability Assessment (SHUMACHER *et al*, 2006)	Identificar as vulnerabilidades dos ativos da empresa e a gravidade caso sejam exploradas.
Risk Determination (SHUMACHER *et al*, 2006)	Avaliar e priorizar os riscos para os ativos.
Enterprise Security Approaches (SHUMACHER *et al*, 2006)	Selecionar a abordagem de segurança para fornecer uma base de decisão sobre quais controles aplicar. As abordagens são prevenir, detectar ou responder.
Enterprise Security Services (SHUMACHER *et al*, 2006)	Selecionar serviços (controles) de segurança para mitigar os riscos.
Enterprise Partner Communication (SHUMACHER *et al*, 2006)	Assegurar que as partes envolvidas com atividades de segurança tenham uma coordenação aberta da comunicação entre grupos de segurança, com outros grupos de parceiros e grupos externos.
Share Responsibility for Security (KIENZLE; ELDER, 2002)	Definir os papéis e as responsabilidades de cada participante do processo de segurança.
Document the Security Goals (KIENZLE; ELDER, 2002)	Documentar as metas de segurança baseadas nos objetivos gerais da organização e seus negócios.
Security Accounting Requirements (SHUMACHER *et al*, 2006)	Definir um conjunto de requisitos de responsabilidades sobre as atividades de segurança. Resolver os conflitos entre os requisitos de segurança e processos de negócio.
Security Accounting Design (SHUMACHER *et al*, 2006)	Desenvolver um plano de revisão das responsabilidades sobre a segurança.
Audit Requirements (SHUMACHER *et al*, 2006)	Definir um conjunto de requisitos para auditoria nos processos de gestão de riscos.
Audit Design (SHUMACHER *et al*, 2006)	Criar mecanismos de auditoria que satisfaçam os seus requisitos.
Audit Trails & Logging Requirements (SHUMACHER *et al*, 2006)	Definir um conjunto de requisitos de trilhas de auditoria e registros de logs para permitir a reconstrução e análise de eventos.
Audit Trails & Logging Design (SHUMACHER *et al*, 2006)	Fornecer orientações para criar trilhas de auditoria e mecanismos de registros de logs.
Non-Repudiation Requirements (SHUMACHER *et al*, 2006)	Definir um conjunto de requisitos para manter as evidências em que os usuários não podem negar que participaram de determinadas atividades.
Non- Repudiation Design (SHUMACHER *et al*, 2006)	Fornecer orientações para criar mecanismos de não-repúdio.

Padrão de Segurança	*Descrição (continuação)*
Documentation Review (SCARFONE *et al*, 2008)	Revisar todos os documentos (políticas de segurança, requisitos, procedimentos, memorandos etc.), provenientes das atividades de segurança a fim de localizar lacunas e deficiência nos processos.
Log Review (SCARFONE *et al*, 2008)	Analisar os logs para verificar a eficácia dos controles implementados e possíveis falhas nos processos.

4. ASSOCIANDO PADRÕES DE SEGURANÇA COM A NORMA ISO 27005

A seleção dos padrões tomou como base a descrição do padrão e sua solução. Alguns padrões possuem uma ligação direta com as atividades da norma ISO/IEC 27005 e estes podem satisfazer completamente as diretrizes destas atividades. Para algumas atividades foi selecionado mais de um padrão, já que estes complementam o atendimento dos requisitos propostos nos processos da norma.

Para fazer a associação dos padrões com as atividades da norma ISO/IEC 27005 foram estudados as ações que cada atividade da norma preconiza, onde são descritos as diretrizes que guiam a execução de uma série de tarefas. Para realizar a associação dos padrões com os processos da norma o estudo compara as soluções que os padrões implementam para verificar o nível de atendimento com as diretrizes de cada atividade da norma.

Para exemplificar a associação, considere a atividade "Definição do Contexto" da ISO/IEC 27005 e o padrão de segurança *Security needs Identification for Enterprise Assets* (SHUMACHER *et al*, 2006). A dinâmica da solução descrita pelo padrão é implementada em cinco etapas, que são:

1) Identificar os ativos de negócio da organização (atende a diretriz "identificação dos ativos relevantes para a gestão dos riscos");

2) Identificar os fatores comerciais que influenciam as necessidades de segurança de proteção de ativos (atende a diretriz "definir o escopo e limites que serão levados em consideração na gestão de riscos");

3) Determinar quais ativos se relaciona com os fatores de negócio (atende a diretriz "identificação dos ativos relevantes para a gestão dos riscos");

4) Identificar quais os tipos de segurança pode ser necessário (atende a diretriz "determinar os critérios gerais de aceitação dos riscos para a organização");

5) Determinar para cada tipo de ativo o tipo de segurança que é necessário (não foi identificada uma ligação direta com as diretrizes da norma).

Além disso, a solução indica o recurso humano necessário para realizar as atividades (atende a diretriz "determinar as responsabilidades para a gestão de riscos").

A atividade da norma é considerada suportada quando a solução apresentada pelo padrão atende pelo menos 75% das diretrizes apontadas por ela. As atividades da ISO 27005 são desenvolvidas implementando as soluções propostas pelos padrões associados.

A Tabela 2 mostra os padrões associados com as atividades de gestão de risco da norma ISO 27005.

Conforme a Tabela 2, a atividade de Definição do Contexto é associado com o padrão *Security Needs Identification for Enterprise Assets* que ajuda a identificar os tipos de ativos de

negócio, fatores que influenciam a segurança do negócio, a relação entre os ativos e fatores de negócio e as propriedades de segurança necessárias para cada ativo.

Tabela 2: Associação de Padrões de Segurança com as Atividades da Norma ISO/IEC 27005.

Atividades da ISO/IEC 27005	*Padrões de Segurança*
Definição do contexto	• *Security needs Identification for Enterprise Assets*
Identificação dos Riscos	• *Threat Assessment*
Análise de riscos	• *Asset Valuation* • *Threat Assessment* • *Vulnerability Assessment* • *Enterprise Security Approaches*
Avaliação de riscos	• *Risk Determination*
Tratamento do risco	• *Enterprise Security Services*
Aceitação do Risco	• *Security needs Identification for Enterprise Assets* • *Enterprise Security Approaches* • *Document the Security Goals*
Comunicação do risco	• *Enterprise Partner Communication* • *Share Responsibility for Security* • *Document the Security Goals*
Monitoramento e Análise Crítica de Riscos	• *Security Accounting Requirements* • *Security Accounting Design* • *Audit Requirements* • *Audit Design* • *Audit Trails & Logging Requirements* • *Audit Trails & Logging Design* • *Non-Repudiation Requirements* • *Non- Repudiation Design* • *Documentation Review* • *Log Review*

As atividades de Análise e Avaliação de Riscos são associadas com os padrões *Asset Valuation, Threat Assessment, Vulnerability Assessment, Enterprise Security Approaches* e *Risk Determination*. A aplicação destes padrões possibilita determinar a importância dos ativos para os negócios da empresa, avaliar as ameaças para estes ativos e suas probabilidades de ocorrerem e avaliar a gravidade das vulnerabilidades encontradas. Com isso, a empresa é capaz de determinar e priorizar os riscos dos ativos para, posteriormente, escolher qual a melhor abordagem de proteção. Além disso, ao aplicar o padrão *Threat Assessment* as diretrizes da atividade Identificação dos Riscos são consequentemente atendidas.

Com os riscos identificados e priorizados a organização deverá implementar controles para que estes riscos sejam minimizados a um nível aceitável. A atividade de Tratamento do Risco poderá ser associada com o padrão *Enterprise Security Services*, que irá ajudar na seleção dos controles de segurança mais adequados. Este padrão define os controles como serviços de proteção aos ativos, conforme a melhor abordagem identificada na etapa anterior. Controle de acesso, criptografia, antivírus, monitoramento de rede de comunicação, alarmes e câmeras de monitoramento são exemplos de controles que podem ser utilizados nesta atividade.

A atividade de Aceitação do Risco tem de assegurar que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Esta atividade é associada com os padrões *Security Needs Identification for Enterprise Assets, Enterprise Security Approaches e Document the Security Goals*, pois com as soluções propostas por estes padrões é possível associar as necessidades de segurança com metas gerais e objetivos de negócio.

Durante todo o processo de gestão de riscos é importante que os riscos sejam comunicados às partes interessadas, possibilitando aos gestores lidar com os incidentes e eventos não previstos da maneira mais efetiva. Os padrões *Enterprise Partner Communication, Share Responsibility for Security e Document the Security Goals* são associados com a atividade de Comunicação do Risco, identificando as partes interessadas no processo de segurança da informação, desenvolvendo mecanismos de comunicação entre as partes interessadas, assim como documentando as metas de segurança baseadas nos objetivos gerais da organização e seus negócios.

Monitorar constantemente as mudanças no contexto, novas ameaças e vulnerabilidades garante detectar mudanças necessárias na gestão de riscos. Vários padrões podem ser associados para com a atividade de Monitoramento e Análise Crítica de Riscos. Os padrões *Security Accounting Requirements, Security Accounting Design* formam um conjunto de soluções que visam definir as responsabilidades sobre as atividades de segurança. Auditorias frequentes possibilitam identificar possíveis falhas e desvios na gestão de riscos examinando, por exemplo, os *logs* dos sistemas. Por isso, foram associados os padrões *Audit Requirements, Audit Design, Audit Trails & Logging Requirements, Audit Trails & Logging Design, Documentation Review e Log Review. Non-Repudiation Requirements, Non- Repudiation Design* os quais são padrões que fornecem soluções para desenvolver e implementar requisitos de auditoria, trilhas de auditoria, revisar documentos e mecanismos de não-repúdio.

5. ILUSTRANDO O USO DE PADRÕES DE SEGURANÇA

A fim de ilustrar a utilização de padrões para desenvolver as atividades da norma ISO/IEC 27005, é descrito, como exemplo, um sistema de gestão acadêmica de uma instituição de ensino privada. Este sistema gerencia os dados acadêmicos e financeiros dos alunos da instituição. Os dados acadêmicos compreendem as informações da vida acadêmica do aluno como, notas, frequência, disciplinas cursadas, histórico entre outros. Os dados financeiros incluem às mensalidades pagas, mensalidades a vencer, créditos e débitos do aluno junto à instituição.

As informações ficam armazenadas em um servidor localizado em um *data center* fora da instituição. Os dados são acessados através de uma interface *web* nas estações de trabalho do balcão de atendimento ao aluno e nas estações utilizadas para o processamento dos dados. Somente pessoas autorizadas podem ter acesso aos dados dos alunos.

Vulnerabilidades no sistema e na infraestrutura de comunicação podem causar falhas de segurança, comprometendo a integridade, a confiabilidade e a disponibilidade das informações dos alunos. As ameaças que podem explorar tais vulnerabilidades devem ser identificadas na atividade de Identificação de Riscos da ISO/IEC 27005 . Essa atividade tem o propósito de identificar os eventos que possam ter impacto negativo nos negócios, assim como as ameaças que podem explorar as vulnerabilidades dos ativos.

As diretrizes dadas por esta atividade podem ser atendidas com a implementação do padrão *Threat Assessment* (SHUMACHER *et al*, 2006). Conforme o catálogo desse padrão, a solução identifica e avalia de forma sistemática as ameaças e determina os níveis de probabilidade de ocorrência dos eventos negativos. Ela é implementada com uma sequência

de quatro passos e preferencialmente devem ser executados por um gerente executivo ou por um gerente estratégico. Além disso, o catálogo do padrão sugere uma sequência de execução das tarefas, como pode ser visto na Figura 2.

1) Identificação das ameaças: identificação da fonte, da ação e da consequência de uma ameaça.

- A fonte da ameaça é o que inicia um ataque ou faz com que um evento aconteça;
- A ação é o método específico através da qual um ataque ou evento é executado;
- A consequência da ameaça é a violação de segurança que resulta de um ataque ou evento negativo bem sucedido.

A origem das ameaças pode ser oriunda de um agente, seja ele interno ou externo, que intercepte e roube uma senha de acesso ao sistema, tendo acesso não autorizado a informações ou insira código malicioso nas estações para burlar as barreiras de proteção. Como ação, o agente causador da ameaça pode utilizar uma combinação de senhas e obter acesso não autorizado ao sistema, tendo como consequência a quebra do sigilo das informações, alteração das informações, podendo causar, também, a indisponibilidade dos dados.

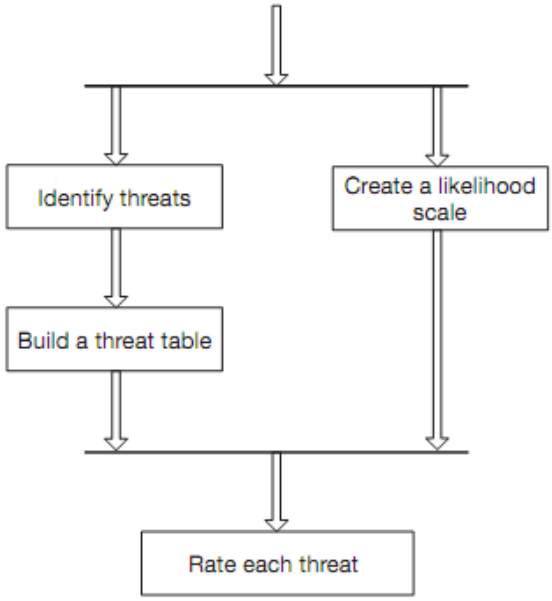

Figura 2: Sequência de execução do padrão *Threat Assessment* (SHUMACHER *et al*, 2006).

2) Construção de uma tabela de ameaças: relaciona as ameaças identificadas com os tipos de ativos e as fontes de ameaça.

É feito um agrupamento das ameaças identificadas com os tipos de ativos e as fontes. A ameaça de roubo de informações pode ser iniciada por um *hacker* externo ou por um funcionário da instituição. No entanto, a frequência de roubo por parte dos empregados pode ser maior do que a de um *hacker* e estar relacionada a vulnerabilidades de mais de um ativo.

3) Criação de escala de probabilidade: criação de níveis de probabilidade dos eventos negativos ocorrerem

Cria-se uma escala de probabilidade de ocorrência das ameaças identificadas. A probabilidade de ocorrência das ameaças pode ser medida em termos quantitativos ou qualitativos, como visto da Tabela 3:

Tabela 3: Probabilidade dos Eventos

Nível	*Probabilidade*	*Descrição*
5	Muito Alta	A ação da ameaça ocorre muito frequentemente
4	Alta	A ação da ameaça ocorre regularmente
3	Média	A ação da ameaça ocorre com pouca frequência
2	Baixa	A ação da ameaça ocorre raramente
1	Muito Baixa	A ação da ameaça é muito improvável de ocorrer

4) Avaliação das ameaças: estimativa de cada ameaça de acordo com a escala de probabilidade.

É revisado o histórico das ameaças, levando em consideração a frequência de ocorrência de cada ameaça, o sucesso da ação da ameaça e a probabilidade de um novo ataque. Registros gerenciais de segurança, aplicativos gerenciais de segurança, análise de fatores humanos e naturais podem ser importantes instrumentos para caracterização das estimativas das ameaças.

Suponha-se que, através da implementação da atividade de Definição do Contexto (ABNT NBR ISO/IEC 27005, 2008), associado ao padrão *Security Needs Identification for Enterprise Assets* (SHUMACHER *et al*, 2006), a instituição identificou os seguintes ativos de informação e físicos:

Ativos de informação

- Dados dos funcionários
- Dados dos alunos
- Dados financeiros
- Dados de históricos acadêmicos

Ativos físicos

- Instalações prediais
- Computadores
- Funcionários
- Rede de comunicação

Através dos passos 1 ao 4, a instituição identificou uma breve lista de ameaças aos ativos de informação e físicos, como mostrado nas Tabelas 4 e 5, respectivamente.

Tabela 4: Ameaças aos ativos de informação

Ameaça	*Probabilidade*	*Consequência*
Falta de energia	Média (3)	Incapacidade de acesso, corrupção da informação.
Roubo de informação	Média (3)	Apropriação indébita, incapacidade de acesso, mau uso, exposição, corrupção da informação.
Acesso não autorizado	Alta (4)	Exposição, falsificação, apropriação indébita, incapacidade de acesso.
Erro de entrada de dados	Alta (4)	Corrupção da informação.
Vazamento de informações confidenciais	Média (3)	Exposição das informações.

Tabela 5: Ameaças aos ativos físicos

Ameaça	*Probabilidade*	*Consequência*
Incêndio	Média (3)	Incapacitação dos ativos físicos
Alagamento	Média (3)	Incapacitação dos ativos físicos
Desgaste dos equipamentos	Média (3)	Incapacitação dos ativos físicos
Falha em sistemas de alarme e monitoramento	Alta (4)	Roubo de equipamentos e de informação, intrusão
Agressão física contras os funcionários	Baixa (2)	Incapacitação dos funcionários
Danos acidentais a estrutura e equipamentos	Média (3)	Incapacitação da estrutura e equipamentos
Configuração incorreta de equipamentos	Alta (4)	Incapacitação de equipamentos, indisponibilidade de acesso

Este processo descrito acima é importante, pois fornece à empresa uma compreensão melhor dos fatores de ameaças e suas probabilidades, assim como identificar as consequências decorrentes de eventos negativos. O resultado deste processo servirá como entrada para a próxima tarefa e servirá para a tomada de decisões e elaboração de estratégias de segurança mais eficazes.

Restrições como a insuficiência de dados históricos sobre a frequência das ações das ameaças e o esforço demasiado para conceber todas as ameaças possíveis podem trazer dificuldades para realizar este processo.

6. TRABALHOS RELACIONADOS

A utilização de padrões de segurança para o desenvolvimento de normas de segurança pode ser visto também em Kroll *et al* (2010), que propõe a utilização de padrões de segurança para implementar a norma ISO/IEC 21827:2008, onde os padrões são associados às *Process Areas* (PA) relacionadas com as práticas de desenvolvimento seguro de *softwares*.

Uma metodologia para a adaptação de processos de *software* com base em requisitos de segurança do *Systems Security Engineering Capability Maturity Model* (SSE-CMM) e o *Rational Unified Process* (RUP) é proposto em Wagner, Fontoura e Fontoura (2011). Aqui, padrões de segurança são associados com as áreas de processos do SSE-CMM, incorporando práticas de segurança em processos de desenvolvimento de *software.*

O trabalho desenvolvido por Beckers *et al* (2011) utiliza padrões de segurança para apoiar o desenvolvimento das atividades Estabelecimento do Contexto e a Identificação dos Ativos, com base na norma ISO/IEC 27005. Neste trabalho padrões são utilizados para garantir a qualidade dos resultados na execução das atividades em um ambiente de computação em nuvem.

Em Kienzle e Elder (2002) padrões de segurança são utilizados para o desenvolvimento de aplicativos *web*. Neste trabalho é elaborado um repositório, composto por 26 padrões, que podem ser utilizados e compreendidos por desenvolvedores que não são profissionais de segurança.

Uma metodologia que incorpora padrões para atender requisitos de segurança em projetos de *software* é proposta também por Fernandez *et al* (2007). Essa metodologia visa suprir as necessidades de segurança que não trazem informações suficientes de como aplicar a segurança em projetos de *software*. A metodologia incorpora outras três metodologias existentes que permitam aos usuários aplicar os padrões para situações práticas. Este trabalho mostra a necessidade do uso de padrões para uma metodologia unificada para construir sistemas seguros.

No entanto, este trabalho difere dos demais pois propõe a utilização de padrões de segurança para implementar as atividades do processo de gestão de riscos baseado na norma ISO/IEC 27005. A utilização de práticas já consolidadas para implementar normas de segurança pode aumentar a garantia de resultados satisfatórios e facilitar o desenvolvimento das atividades necessárias.

7. CONSIDERAÇÕES FINAIS

O embasamento das diretrizes de modelos de referência pode ser fundamental para as organizações implementarem processos bem definidos e com resultados satisfatórios. Porém, a maioria das normas para gestão da segurança da informação diz o que tem que ser feito, mas não detalha suficientemente como deve ser feito. A norma ISO/IEC 27005 define uma estrutura de atividades para gestão de riscos. Cada atividade possui diretrizes que servem de guia, dizendo o que deve ser alcançado ao final de cada iteração.

O presente trabalho associou padrões de segurança com os processos da norma ISO/IEC 27005, relacionando as diretrizes de cada atividade da norma com as soluções propostas por cada padrão. Alguns padrões estão ligados diretamente com as atividades da norma, atendendo as diretrizes mínimas descritas por cada uma delas. Observou-se que alguns padrões podem atender as diretrizes de mais de uma atividade da norma, o que possibilita reduzir o tempo para o desenvolvimento das atividades.

A ilustração mostrou como um padrão pode ser implementado para desenvolver uma atividade da norma. Neste caso, desenvolveu-se a atividade de Identificação de Riscos, que contribui para a identificação de riscos de segurança que podem ocorrer em um sistema de informação e servirá para a tomada de decisões e elaboração de estratégias de segurança mais eficazes.

O uso de padrões para o desenvolvimento de uma gestão de riscos baseada na norma ISO/IEC 27005 pode contribuir para uma melhoria na definição de processos para gestão de segurança da informação, a fim de dar maiores garantias para o cumprimento dos requisitos definidos pelas normas. Propor a utilização de padrões de segurança pelas organizações pode ser uma garantia para o atingimento dos objetivos a qual a norma se propõe. Cabe a cada organização escolher os padrões que mais se adequam aos seus objetivos de negócios.

Este trabalho não pretende esgotar as possibilidades de uso de padrões de segurança e limitou-se a associar padrões de segurança que estão relacionados com o processo de gestão de riscos. Em trabalhos futuros pretende-se verificar os aspectos de dependência entre os padrões, já que alguns podem necessitar de informações provenientes de outro padrão.

8. REFERÊNCIAS

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

AMARAL, E. H.; AMARAL, M. M. & NUNES, R. C. Metodologia para Cálculo do Risco por Composição de Métodos. X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2010, p. 461-473.

BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C. & FAßBENDER. S. Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. Sixth International Conference on Availability, Reliability and Security, 2011, p.327-333.

FERNANDEZ, E. B.; YOSHIOKA, N.; WASHIZAKI, H. & JURJENS, J. Using security patterns to build secure systems. Workshop on Software Patterns and Quality (SPAQu'07), 2007, Nagoya, Japan, with the 14th Asia-Pacific Software Engineering Conference (APSEC).

KIENZLE, D. M.; & ELDER, M. C. Security Patterns for Web Application Development. Final Technical Report, Univ. of Virginia, 2002, Report DARPA Contract # F30602-01-C-0164.

KROLL, J.; FONTOURA, L. M.; WAGNER, R. & DORNELLAS, M. C. Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008. Simpósio Brasileiro de Sistemas de Informação (SBSI), 2010, Marabá. Anais do Simpósio Brasileiro de Sistemas de Informação (SBSI), 2010.

LUNARDI, G. L. & DOLCI, P. C. Adoção de Tecnologia da Informação e seu Impacto no Desempenho Organizacional: um estudo realizado com micro e pequenas empresas. 30º Encontro da ANPAD, Salvador: ENANPAD, 2006.

LUND, M. S.; SOLHAUG, B. & STØLEN, K. Evolution in relation to risk and trust management. IEEE Computer Society, 2010, p. 49-55.

OLIVEIRA, M. A. F.; ELLWANGER, C.; VOGT, F. C. & R. C. NUNES. Framework para gerenciamento de riscos em processos de gestão de segurança da informação baseado no modelo DMAIC. XXIX Encontro Nacional de Engenharia de Produção (ENEGEP), 2009, Salvador, XXIX Encontro Nacional de Engenharia de Produção. Rio de Janeiro: Abepro, 2009. v. 1. p. 11-20.

OLIVEIRA, V. L. Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE. Dissertação de Mestrado, UNICAMP, Campinas, Brasil, 2006.

ROMANOSKY, S. Security design patterns, in SecurityFocus, 2002. Disponível em: http://www.securityfocus.com/guest/9793

ROSADO, D. G.; MEDINA, E. F.; PIATTINI, M. & GUTIERREZ, C. A Study of Security Architectural Patterns. Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), 2006, p. 358-365.

SCARFONE, K.; SOUPPAYA, M.; CODY, A. & OREBAUGH, A. Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST) Special Publication 800-115. 2008. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

SCHUMACHER, M.; FERNANDEZ, E. B.; HYBERTSON, D.; BUSCHMANN, F. & SOMMERLAD, P. Security Patterns: integrating security and systems engineering, Series in Software Designs Patterns, USA: J.Wiley & Sons, 2006.

SUPAPORN, K.; PROMPOON, N. & ROJKANGSADAN, T. An approach: Constructing the grammar from security pattern. Proc. 4th International Joint Conference on Computer Science and Software Engineering (JC-SSE2007), 2007.

VASILE, T; STUPARU, D. & DANIASA, C. The relative risk weighting process. Annals Economic Science Series, vol. XVI, p. 540-544, 2010.

WAGNER, R.; FONTOURA, L. M. & FONTOURA, A. B. Using Security Patterns to Tailor Software Process. Proceedings of the 23rd International Conference on Software Engineering Knowledge Engineering (SEKE'2011), 2011, Eden Roc Renaissance, Miami Beach, USA, July 7-9, p. 672-677.

YOSHIOKA, N.; WASHIZAKI, H. & MARUYAMA, K. A survey on security patterns. Progress in Informatics, 2008, No. 5, p.35–47.