Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008

Josiane Kroll[1], Lisandra M. Fontoura[1,2], Rosana Wagner[2], Marcos C. D'Ornellas[1,2]

[1] Laboratório de Computação Aplicada (LaCA) – Universidade Federal de Santa Maria (UFSM)- Santa Maria, RS – Brasil

[2] Programa de Pós-Graduação em Informática (PPGI) – Universidade Federal de Santa Maria (UFSM)– Santa Maria – RS – Brasil

{josi.unc, lisandramf, rosanawagner, marcosdornellas}@gmail.com

Abstract. *The lack of security in Information Systems has caused a lot of moral and financial losses for the organizations. The majority of organizations does not have a security management program that is well structured and efficient. By using patterns, such organizations can strength their security management programs and even improve their protection assurance. As long as organizations start to use patterns aligned with security standards, the number of security failures in information systems will dramatically decrease. This article shows patterns which are tied to ISO/IEC 21827:2008 and discuss an association among patterns.*

Resumo. *A falta de segurança em Sistemas de Informação tem provocado inúmeros prejuízos financeiros e morais para as organizações. A maioria das organizações não dispõe de um programa de gestão da segurança bem estruturado e eficiente. Usando padrões de segurança, as organizações poderão fortalecer seus programas de gestão de segurança além de aumentar suas garantias de proteção. Se as organizações utilizarem os padrões alinhados a uma norma de segurança, o número de falhas de segurança em Sistemas de Informação irá diminuir consideravelmente. Este artigo apresenta padrões ligados à norma ISO/IEC 21827:2008 e discute as associações entre estes padrões.*

1. Introdução

Um padrão é uma solução reusável para problemas recorrentes [Fernandez et al. 2007]. Ele pode contribuir para solucionar problemas de má implementação de processos de segurança, como também para aumentar a eficiência de procedimentos de segurança já implementados. Ele representa a experiência e o conhecimento de muitos profissionais e quando catalogado é útil para resolver vários problemas [Fernandez et al. 2007]. No contexto organizacional é observado o considerável esforço científico e acadêmico em desenvolver padrões que focalizem soluções para problemas relacionados com a proteção dos Sistemas de Informação [Weiss e Mouratidi 2008]. Entretanto, a aplicação de padrões para o desenvolvimento de processos de gestão da segurança para Sistemas de Informação ainda é pequena por parte das organizações.

As organizações desenvolvem a gestão da segurança atrelada a uma norma, guia ou outras documentações de segurança que dão suporte na formulação da política da

segurança e na definição dos controles que serão implementados [Wiander 2007]. No entanto, para que o desenvolvimento da gestão da segurança traga bons resultados é necessário que controles de segurança, formados por processos e procedimentos, sejam implementados de maneira adequada.

Considerando que uma norma de segurança fornece um conjunto de boas práticas a serem seguidas pelas organizações, e que padrões descrevem boas soluções para implementar as práticas dadas pelas normas de segurança, esse artigo associa padrões de segurança que podem ser usados para implementação da norma de segurança ISO/IEC 21827:2008. As organizações que buscam implantar a norma podem aplicar os padrões sugeridos.

A norma ISO/IEC 21827:2008 é adotada como um guia para o desenvolvimento da gestão da segurança de Sistemas de Informação. Serão associados padrões de segurança para o desenvolvimento das práticas recomendadas pela norma. E, em seguida, esses padrões serão associados de forma a compreender a relação que um padrão possui com outro, estabelecendo uma sequência de implementação dos padrões, útil para as organizações. Também será realizada uma análise da utilização dos padrões para a implantação da norma ISO/IEC 21827:2008 e elaborado um estudo de caso para exemplificar a utilização dos padrões de segurança.

Este artigo está organizado da seguinte forma: na Seção 2, é apresentada a estrutura da norma ISO/IEC 21827:2008 que é utilizada para implantação da gestão da segurança. Na Seção 3, são apresentados os padrões que estão relacionados ao atendimento da norma ISO/IEC 21827:2008, a associação entre esses padrões e um estudo de caso. Na Seção 4, são abordados os trabalhos relacionados com o uso de padrões para a gestão da segurança. Na Seção 5, é feita uma análise da utilização de padrões para a implantação da norma ISO/IEC 21827:2008. Por fim, a Seção 6 traz as conclusões obtidas com o desenvolvimento do estudo.

2. A Norma ISO/IEC 21827:2008

A norma ISO/IEC 21827:2008 foi criada a partir do modelo SSE-CMM (*Systems Security Engineering Capability Maturity Model*) que foi desenvolvido pelo ISSEA (*International Systems Security Engineering Association*) em 1999. Esta norma descreve as características essenciais que um processo de segurança deve possuir para assegurar a boa segurança [SSE-CMM 2003].

A norma ISO/IEC 21827:2008 não prescreve uma sequência ou um processo particular, mas captura as práticas que são geralmente observadas na indústria. Esta norma é designada para todos os tipos de organizações, sendo usada para a melhoria e avaliação da capacidade de maturidade dos processos de segurança [SG-SBP 2008].

O desenvolvimento da gestão da segurança proposto pela norma ISO/IEC 21827:2008 é dado por uma estrutura de 22 PAs (*Process Areas*), divididas em dois grupos: Práticas Base de Segurança e Práticas Base Organizacionais e de Projeto. No entanto, nem todas as PAs necessitam ser aplicadas para o desenvolvimento de um programa de gestão da segurança, cabendo a cada organização decidir qual PA implementar [SSE-CMM 2003].

Para o desenvolvimento da gestão da segurança proposta nesse artigo, foram selecionadas as PAs da categoria Práticas Base de Segurança, por serem específicas da

área de segurança. As PAs da categoria Práticas Base Organizacionais e de Projeto são mais voltadas para o controle de qualidade e gerencial do projeto. A descrição das PAs da categoria Práticas Base de Segurança é apresentada na Tabela 1.

A norma ISO/IEC 21827:2008 também define níveis de maturidade para os processos de segurança da organização que são ampliados após o estabelecimento e cumprimento das práticas da segurança [Batista 2007]. O processo mais "maduro" define uma organização cujos processos são melhores definidos e conduzidos. São seis níveis de maturidade definidos, onde cada um desses níveis consiste de um número de Práticas Genéricas - GP (*Generic Practices*) que suportam o desempenho das PAs [SSE-CMM 2003].

3. Padrões aplicados para a Gestão da Segurança baseada na norma ISO/IEC 21827:2008

Nesta seção serão apresentados os padrões aplicados as PAs da norma ISO/IEC 21827:2008. A solução dada pelo padrão deve satisfazer os objetivos de implementação da PA. Todas as PAs possuem uma lista de objetivos que indicam os resultados esperados da implementação do processo.

A norma fornece uma lista de BPs (*Base Practices*) que mostram o número e o nome de cada BP. As BPs auxiliam no cumprimento dos objetivos da área de processo. Os padrões serão primeiramente relacionados com as PAs e posteriormente são associados. O critério para seleção dos padrões é baseado na solução dada pelo padrão relacionado com os objetivos e com as BPs estabelecidas por cada PA. Também são considerados exemplos fornecidos na descrição da PA para a identificação do padrão.

3.1. Padrões relacionados com as PAs (*Process Areas*) da ISO/IEC 21827:2008

Um padrão é definido como uma abordagem consolidada que descreve um problema recorrente que surge em uma situação específica e apresenta uma solução comum que pode ser aplicada em outras situações com o mesmo problema [Schumacher et al. 2006]. A solução dada por um padrão consiste da indicação de regras que podem ser arranjadas dentro de estruturas múltiplas de projeto para criar um processo em uma estrutura específica [Yoshioka Honiden Finkelstein 2004].

O processo de gestão da segurança proposto pela ISO/IEC 21827:2008 fundamenta-se na implementação das PAs. Para cada PA um ou mais padrões podem ser selecionados. Os padrões selecionados para as PAs são apresentados a seguir:

PA01 - Administração dos controles de segurança

- *Security Provider* [Romanosky 2002];
- *Controlled Process Creator* [Schumacher et al. 2006];
- *Access Control Requirements* [Schumacher et al. 2006];
- *Role Rights Definition* [Schumacher et al. 2006];
- *Role-Based Access Control* [Schumacher et al. 2006];
- *Authorization Pattern* [Rosado 2006];
- *Multilevel Security Pattern* [Rosado 2006];

Tabela 1. Descrição das PAs da categoria práticas base de segurança

PAs *(Process Áreas)*	**Objetivo da PA**
PA01-Administrar controles de segurança	Assegurar que a segurança destinada para o sistema foi integrada dentro do projeto do sistema e é de fato realizada pelo sistema resultante em seu estado operacional.
PA02 - Avaliar impacto	Identificar os impactos que são motivos de preocupação, no que diz respeito ao sistema e para avaliar a ocorrência de impactos. Impactos podem ser tangíveis, tais como a perda de receitas ou de sanções pecuniárias ou imateriais, como a perda de reputação.
PA03 - Avaliar riscos de segurança	Identificar os riscos de segurança envolvidos com o sistema em um ambiente definido. Esta PA avalia os riscos com base no entendimento de como as capacidades e os ativos são vulneráveis às ameaças. Especificamente a atividade envolve a identificação e avaliação da probabilidade da ocorrência de riscos. A avaliação de riscos é realizada para apoiar as decisões relacionadas ao desenvolvimento, manutenção ou operação do sistema o qual o ambiente é conhecido.
PA04 - Avaliar ameaças	Identificar as ameaças de segurança, suas características e propriedades.
PA05 - Avaliar vulnerabilidades	Identificar e caracterizar as vulnerabilidades dos sistemas de segurança. Esta PA inclui a análise e a avaliação do sistema, definindo vulnerabilidades específicas e fornecendo uma avaliação global das vulnerabilidades do sistema.
PA06 - Construir argumentos de segurança	Transmitir claramente que as necessidades de segurança do cliente são cumpridas.
PA07 - Coordenar a segurança	Assegurar que as partes envolvidas com atividades de engenharia da segurança são adequadas e consistentes. Esta coordenação envolve a manutenção aberta da comunicação entre grupos de segurança, com outros grupos de engenheiros e grupos externos.
PA08 - Monitorar a postura da segurança	Assegurar que todas as brechas de tentativa de violação ou erros que poderiam eventualmente conduzir a uma violação de segurança são identificados e comunicados. Os ambientes externos e internos são monitorados por todos os fatores que podem ter um impacto sobre a segurança do sistema.
PA09 - Estabelecer a entrada de segurança	Fornecer aos arquitetos, projetistas, programadores ou usuários do sistema, a informação de segurança a eles necessária. Esta informação inclui arquitetura do sistema, projeto ou implementação alternativa e guia de segurança. A entrada é desenvolvida, analisada, fornecida e coordenada com os membros da organização apropriados, baseados nas necessidades de segurança identificadas na PA01.
PA10 - Especificar necessidades de segurança	Identificar as necessidades relacionadas para segurança do sistema. Esta PA abrange todos os aspectos da segurança de todo o sistema de informação relacionado com as exigências de concepção, desenvolvimento, verificação, operação e manutenção do sistema. As informações obtidas com estes processos são refinadas e atualizadas ao longo do projeto, a fim de assegurar que as necessidades do cliente estão sendo atendidas. A PA10 proporciona a entrada de segurança estando diretamente ligada a PA09.
PA11- Verificar e validar a segurança	Assegurar que as soluções de segurança são verificadas e validadas. Tais soluções são verificadas contra os requerimentos, arquiteturas e projetos, usando observação, demonstração, análises e testes de segurança.

PA02- Avaliação do impacto

- *Risk Determination* [Schumacher et al. 2006];

PA03- Avaliação dos Riscos de segurança

- *Asset Valuation* [Schumacher et al. 2006];
- *Threat Assessment* [Schumacher et al. 2006
- *Vulnerability Assessment* [Schumacher et al. 2006];
- *Risk Determination* [Schumacher et al. 2006];

PA04- Avaliação de ameaças

- *Threat Assessment* [Schumacher et al. 2006];

PA05- Avaliação de Vulnerabilidades

- *Vulnerability Assessment* [Schumacher et al. 2006];

PA06 – Construção de argumentos de garantia

- *Patch Proactively* [Kienzle 2002];
- *Engage Customers (organizational)* [Coplien 1999];
- *Check Point* [Yoder Barcalow 1998];
- *Red Team the Design* [Kienzle 2002];

PA07 – Coordenação da segurança

- *Enterprise Partner Communication* [Schumacher et al. 2006];
- *Share Responsibility for Security* [Kienzle 2002];
- *Gatekeeper* [Coplien 1999];
- *Buffalo Mountain (organizational)* [Coplien 1999];

PA08 – Monitoração da postura da segurança

- *Minefield* [Kienzle 2002];
- *Security Accounting Requirements* [Schumacher et al. 2006];
- *Security Accounting Design* [Schumacher et al. 2006];
- *Audit Requirements* [Schumacher et al. 2006];
- *Audit Design* [Schumacher 2006];
- *Audit Trails & Logging Requirements* [Schumacher et al. 2006];
- *Audit Trails & Logging Design* [Schumacher et al. 2006];
- *Non-Repudiation Requirements* [Schumacher et al. 2006];
- *Non- Repudiation Design* [Schumacher et al. 2006];

PA09 – Fornecer a entrada segurança

- *Document the Security Goals* [Kienzle 2002];
- *Document the Server Configuration* [Kienzle 2002];
- *Enterprise Security Approaches* [Schumacher et al. 2006];
- *Enterprise Security Services* [Schumacher et al. 2006];

PA10 – Especificar as necessidades de segurança

- *Security needs Identification for Enterprise Assets* [Schumacher et al. 2006];

PA11 – Verificação e validação da segurança

- *Task Process Pattern – Technical Review* [Ambler 1998];
- *Check Point Pattern* [Rosado 2006];
- *Whitehat, Hack Thyself* [Romanosky 2003];
- *Technical Guide to Information Security Testing and Assessment* [Scarfone et al. 2008].

Os padrões são documentados por diversos autores e possuem recomendações que devem ser seguidas conforme descrito em seus catálogos.

Para atender as recomendações de uma determinada PA pode ser necessária a implantação de apenas um padrão, quando este satisfaz completamente a PA; ou de vários padrões, sendo que neste caso cada padrão atende parte das recomendações da PA. Apesar de serem encontrados vários padrões que poderiam ser aplicados, optou-se por selecionar padrões de um mesmo autor quando possível. Isso tende a facilitar a associação entre padrões durante a implementação, quando os mesmos fazem a troca de informações.

3.2. Associações entre padrões para a implantação da gestão da segurança

Com o estudo das características dos padrões propostos para a implantação da Gestão da Segurança baseada na ISO/IEC 21827:2008 foi possível verificar que alguns padrões dependem de outros para serem desenvolvidos. Conforme o catálogo de alguns padrões há uma sequência de atividades que devem ser seguidas e que utilizam os resultados encontrados por outros padrões.

Para que se possa compreender como os padrões selecionados podem ser utilizados para a implantação da Gestão da Segurança baseada na ISO/IEC 21827:2008 foi primeiramente verificado como as PAs estão interligadas e qual a sequência que deve ser seguida para a implantação das PAs. Na Figura 1 podem ser observados esses dados, onde o processo de implantação da ISO/IEC 21827:2008 começa pela PA04 e termina com a PA06. O processo de análise riscos é desenvolvido por três PAs em paralelo que fornecem informações para identificação e avaliação dos riscos. A partir da PA03 é seguida uma sequência até a PA08 que retorna para a PA03. Essas informações obtidas pelas PAs são coordenadas pela PA07 e em seguida seguem para um processo de validação, verificação e construção de argumentos de garantia de segurança.

A associação entre os padrões ocorre no momento que foi estabelecida a sequência de desenvolvimento dos padrões. Observa-se que para usar o padrão *Risk Determination* [Schumacher et al. 2006] são necessários outros padrões como o *Threat Assessment* [Schumacher et al. 2006], *Vulnerability Assessment* [Schumacher et al. 2006] e *Asset Valuation* [Schumacher et al. 2006]. Esses padrões são precedidos do padrão *Security needs Identification for Enterprise Assets* [Schumacher et al. 2006] que determina a necessidade de segurança para os ativos encontrados.

Outros padrões associados são o padrão *Access Control Requirements* [Schumacher et al. 2006] com o padrão *Controlled Process Creator* [Schumacher et al. 2006] que necessita da identificação das necessidades de acesso para criar um processo controlado de acesso às informações.

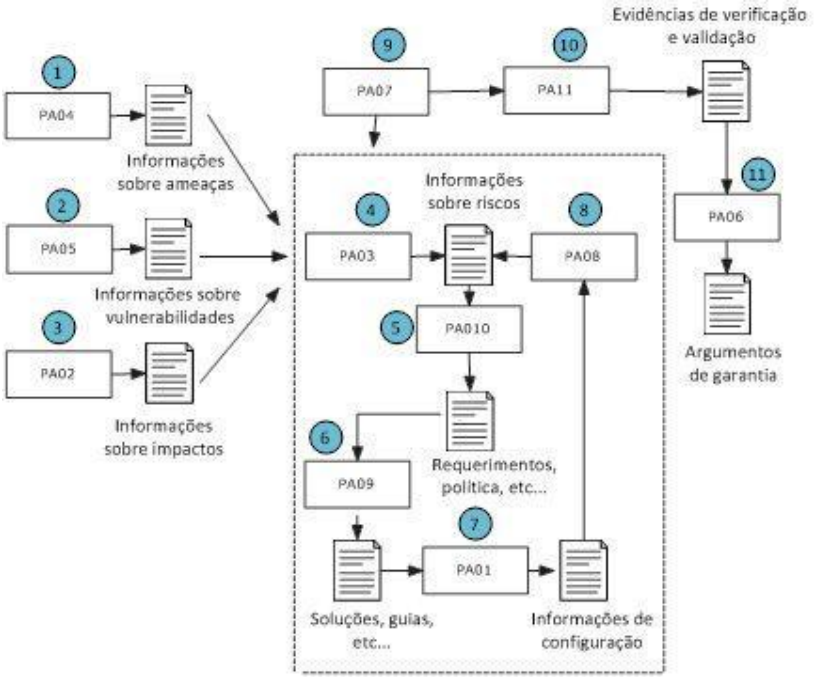

Figura 1. Sequência para a implantação da norma ISO/IEC 21827:2008

Para a elaboração da política da segurança é necessária a definição de objetivos, serviços e abordagens que serão utilizadas. Dessa forma o padrão o *Enterprise Security Services* [Schumacher et al. 2006] depende do padrão *Enterprise Security Approaches* [Schumacher et al. 2006] para selecionar serviços de acordo com a abordagem de segurança adotada.

Os padrões *Non-Repudiation Requirements* [Schumacher et al. 2006] e *Non-Repudiation Design* [Schumacher et al. 2006] são aplicados para garantir que as informações sobre o projeto e requisitos de segurança fornecidos, não serão negados. Dessa forma, eles associam-se aos padrões *Audit Trails & Logging Requirements* [Schumacher et al. 2006] e *Audit Trails & Logging Design* [Schumacher et al. 2006] respectivamente, por serem uma continuidade do processo de auditoria fornecido por esses padrões.

Outros padrões também possuem dependência do fornecimento de dados de outros padrões para serem aplicados eficientemente, como por exemplo, o padrão *Controlled Process Creator* [Schumacher et al. 2006] com o padrão *Access Control Requirements* [Schumacher et al. 2006], o padrão *Minefield* [Kienzle 2002] e *Security Accounting Design* [Schumacher et al. 2006] como o padrão *Security Accounting Requirements* [Schumacher et al. 2006], o padrão *Task Process Pattern – Technical Review* [Ambler 1998] com os padrões *Check Point Pattern* [Rosado 2006], *Whitehat, Hack Thyself* [Romanosky 2003] e *Technical Guide to Information Security Testing and Assessment* [Scarfone 2008] entre outros que estão associados.

3.3 Estudo de Caso

Para descrever como os padrões de segurança satisfazem as recomendações da norma ISO/IEC 21827:2008, será adotado como exemplo um sistema de transferência bancária. Nesse tipo de sistema se desenvolve uma transação distribuída entre bancos.

Na transação, o cliente confirma a transferência de valores entre contas de diferentes bancos localizados em diferentes lugares. A transferência é uma transação de muitas transações de uma aplicação chamada sistema de controle de conta corrente. A transação distribuída deve preservar as propriedades do ACID (atomicidade, concorrência, isolamento e durabilidade).

O sistema é composto por vários gerentes de transação que cooperam para executar transações globais. Cada local do sistema consiste de dois subsistemas como mostrado na Figura 2. Na Figura 2, o gerente de transação (GT) é responsável por executar as transações locais e manter o acesso a dados armazenados localmente. O coordenador da transação (CT) coordena e executa várias transações (globais e locais), as quais são localmente iniciadas.

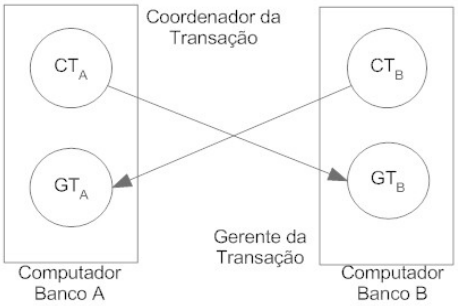

Figura 2. Sistema de transferência entre bancos

Durante a operação de transferência bancária podem ocorrer várias falhas de segurança causadas por vulnerabilidades no sistema. Para identificar as ameaças que podem explorar tais vulnerabilidades durante uma operação de transferência bancária, pode ser implementada a PA04.

A PA04 tem o propósito de identificar e caracterizar as ameaças, avaliando a capacidade e a motivação do agente da ameaça, a probabilidade de manifestação e a evolução da ameaça. As práticas de segurança dadas pela PA04 podem ser atendidas com aplicação do padrão *Threat Assessment* [Schumacher et al. 2006]. O catálogo desse padrão determina a sequência de implementação em 4 passos:

1. Identificar ameaças: consiste na identificação da origem, da ação e da consequência de uma ameaça;
2. Criar escala de probabilidade: determinar em termos quantitativos e valores qualitativos o valor estimado correlacionado a ocorrência da ameaça;
3. Categorizar ameaças: identificar as ameaças que têm frequência de ocorrência, sucesso de violação e que podem causar maiores danos.
4. Redigir relatório: armazenar dados obtidos na avaliação.

No passo 1, referente a identificação das ameaças, a origem das ameaças pode ser oriunda de um agente que roube a senha, clone cartões, insira um código malicioso no software que efetua a operação de transferência bancária ou que de alguma forma consiga burlar as barreiras de proteção do sistema. Em termos de ação, o agente causador da ameaça busca interceptar a transação bancária e usá-la a seu favor. A consequência dessa ação é a quebra de sigilo bancário e a perda financeira. Neste passo o grupo responsável pela segurança irá aplicar ferramentas para a identificação da origem, da ação e da consequência de uma ameaça. Essas ferramentas podem ser

aplicativos computacionais, *cheklists, brainstorming*, questionários, não limitados a estes.

No passo 2, cria-se uma escala de probabilidade de ocorrência das ameaças identificadas. Essa escala pode conter termos quantitativos e valores qualitativos ao valor estimado correlacionado a ocorrência da ameaça. A escala estabelecida de probabilidade da ocorrência da ameaça pode ser, por exemplo: Muito alta, Alta, Média, Baixa ou Muito baixa.

No passo 3, é revisado o histórico das ameaças que já causaram danos ao sistema, levando em consideração a frequência de ocorrência de cada ameaça, o sucesso de violação e a probabilidade de um novo ataque. O método utilizado neste passo para categorizar as ameaças pode ser baseado em relatórios gerenciais de segurança, aplicativos de gerenciamento de segurança, observação de fatores humanos e naturais de probabilidade da ocorrência das ameaças, não se limitando a estes.

No passo 4, são documentadas as informações obtidas em todo o processo de avaliação das ameaças. Essas informações servirão para a tomada de decisões e elaboração de estratégias de segurança mais eficazes.

Com a avaliação das ameaças existentes em uma operação de transferência bancária são obtidas informações que contribuem também para a identificação de vulnerabilidades e riscos de segurança que podem ocorrer nesse tipo de transação entre bancos.

4. Trabalhos Relacionados

Como exemplo de trabalhos que relatam a utilização dos padrões para o atendimento dos requisitos de segurança cita-se o trabalho de Fernandez e Larrondo-Petrie (2006), que propõem uma metodologia para construir sistemas seguros usando padrões. Nesse trabalho a metodologia proposta é voltada para o desenvolvimento seguro de *software*, onde a ideia básica é a utilização de padrões para orientar a segurança em cada estágio do desenvolvimento.

Fernandez et al. (2008) também propõe uma metodologia que incorpora padrões para atender requisitos de segurança em projetos de *software*. Essa metodologia visa suprir as necessidades de catálogos de padrões que não trazem informações suficientes de como aplicar o padrão. A metodologia mescla três metodologias existentes e mostra a necessidade de metodologias que permitam aos usuários aplicar esses padrões para situações práticas. Como resultados obtidos por este trabalho observou-se a necessidade do uso de padrões para uma metodologia unificada para construir sistemas seguros.

Weiss e Mouratidis (2008) apresentam uma abordagem para a seleção dos padrões que permite verificar em profundidade os *trade-offs* envolvidos nos padrões e as implicações de um padrão de segurança para atender vários requisitos. Esse trabalho apóia a busca de uma combinação de padrões de segurança que objetiva atender aos requisitos de segurança.

Outros trabalhos também citam o uso de padrões para atender critérios de segurança em outras áreas, como o trabalho apresentado por Muñoz-Arteaga (2008) que fala da utilização de padrões para projetos de segurança de HCI (*Human-Computer Interaction*). No entanto, os trabalhos encontrados não citam como os padrões apóiam a gestão da segurança de Sistemas de Informação. O trabalho proposto nesse artigo se

difere dos demais por apresentar o uso de padrões para a implantação de uma norma de segurança, a ISO/IEC 21827:2008 e consequentemente o desenvolvimento da gestão da segurança. É importante verificar como os padrões podem ser úteis para a implantação de normas e como eles estão associados. Com os resultados obtidos neste estudo é possível avaliar a adequação do uso de padrões para a gestão da segurança de Sistemas de Informação baseada em recomendações de uma norma.

5. Uma análise da aplicação de padrões para o desenvolvimento da ISO/IEC 21827:2008

A implantação da norma ISO/IEC 21827:2008 possui uma estrutura que possibilita que os padrões sejam adequados às PAs sem que ocorra a necessidade da utilização de um mesmo padrão mais de uma vez. Os padrões aplicados tendem a estar atrelados formando um ciclo de informações úteis para processos de gerenciamento e auditoria da segurança.

Embora o objetivo da utilização dos padrões para esse contexto não seja a redução de tempo gasto para o desenvolvimento das atividades e nem a redução de custos, há uma tendência que esses objetivos sejam cumpridos. Ainda, a norma ISO/IEC 21827:2008 não determina quais PAs devem ser implementadas cabendo a cada organização selecionar quais PAs vão de encontro com seus objetivos e dessa forma aplicar os padrões úteis para desenvolvê-las.

Alguns padrões são dependentes de outros e dessa forma estão associados. No entanto, outros não possuem uma sequência de implementação e podem ser implementados conforme o plano de segurança de cada organização. Na norma ISO/IEC 21827:2008 isso foi observado em algumas PAs tais como a PA09, PA10 e PA11.

Um fator importante para a implantação de uma norma de segurança é que ela cumpra com os objetivos para os quais ela foi proposta e dessa forma resulte numa possível certificação para organização. Os critérios adotados para a seleção de padrões consideram os objetivos não só da norma, mas como de todas as PAs que formam o processo de gestão da segurança. Dessa forma, os padrões que foram selecionados estão alinhados com a norma, mas podem ser substituídos por outros que tenham a mesma função.

Outras normas de segurança também podem fazer uso dos padrões apresentados, pois considerando que a norma ISO/IEC 21827:2008 aplica-se para o desenvolvimento da gestão da segurança, alguns processos podem ser similares entre outras normas.

6. Conclusões

O presente trabalho discutiu o uso de padrões para a gestão da segurança de Sistemas de Informação baseada na norma ISO/IEC 21827:2008. Buscou-se verificar como os padrões podem ser úteis para implantação da gestão da segurança alinhada a uma norma de segurança, tal como a ISO/IEC 21827:2008. E também como a utilização de padrões de segurança contribui para o fornecimento de maiores garantias de segurança para os Sistemas de Informação das organizações.

A gestão da segurança proposta pela ISO/IEC 21827:2008 é implantada por meio do desenvolvimento das PAs. Essas PAs possuem uma lista de objetivos os quais foram usados para a seleção dos padrões. Pode-se observar que nesse processo de

seleção, alguns padrões cumpriam com mais de um objetivo da PA possibilitando que fosse reduzido o tempo para o desenvolvimento da PA.

Com os padrões aplicados a ISO/IEC 21827:2008 foi possível desenvolver um processo de gestão da segurança que envolve a maioria dos aspectos de segurança de Sistemas de Informação. O desenvolvimento da gestão de riscos que contribui para a identificação das necessidades de segurança é a principal contribuição para a formulação de um processo de gestão da segurança alinhado aos objetivos organizacionais.

Com relação à aplicação de padrões para o desenvolvimento de normas de segurança, verificou-se vários aspectos de dependência de informações entre os padrões. Um padrão pode necessitar de informações provenientes de outro padrão para o desenvolvimento de uma nova atividade. Essa associação entre padrões contribui para a vinculação dos processos de segurança. Também foi observado que para alguns padrões não há essa dependência e eles podem ser implementados de acordo com a necessidade da organização.

O uso de padrões para a gestão da segurança contribui, principalmente, para uma melhoria na definição de processos para gestão de segurança, além de proporcionar a redução de custos. É observado também que os padrões contribuem para o desenvolvimento de processos de segurança mais seguros, para o estabelecimento de medidas adequadas de segurança entre outros benefícios que podem ser identificados. Isso demonstra que a probabilidade do objetivo de uma norma de segurança não ser atingido se torna reduzido. O intuito é fazer com que cada vez mais as organizações promovam a gestão de segurança de forma adequada e satisfatória. Cabe a cada organização escolher qual norma de segurança adotar para a gestão de segurança e quais padrões selecionar.

Referências

Ambler, S. W. (1998) “An introduction to process patterns”, in SIGS Books/Cambridge University Press.

Appleton, B. (1997) “Patterns for conducting process improvement”, In: PLoP 97 conference. Disponível em <http://www.bradapp.net/docs/patterns-intro.html> acesso em janeiro de 2010.

Batista, C. F. A. (2007) “Métricas de Segurança de Software”, Dissertação do Programa de Pós-Graduação em Informática do Departamento de Informática da PUC-Rio. Universidade Pontifícia Católica, Rio de Janeiro.

Fernandez, E. B. and Larrondo-Petrie, M. M. (2006) “A methodology to build secure systems using patterns”, In: 22nd Annual Computer Security Applications Conference (ACSAC), Works in Progress, Miami Beach, FL.

Fernandez, E. B., Yoshioka, N., Washizaki, H. and Jurjens, J. (2007) “Using security patterns to build secure systems”, In: Workshop on Software Patterns and Quality (SPAQu'07), Nagoya, Japan, with the 14th Asia-Pacific Software Engineering Conference (APSEC).

Kienzle, D. M. and Elder, M. C. (2002) “Security Patterns for Web Application Development”, Final Technical Report, Univ. of Virginia.

Muñoz-Arteaga, González, M. R. and Vanderdonckt, J. (2008) “A classification of security feedback design patterns for interactive web applications”, In: Proc. Int. Conf. on Internet Monitoring and Protection, pp. 166-171.

Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. (2008) “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. Disponível e <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf> acesso em janeiro de 2010.

Romanosky, S. (2002) “Security design patterns”, In: SecurityFocus. Disponível em <http://www.securityfocus.com/guest/9793> acesso em janeiro de 2010.

Romanosky, S. (2003) “Operational security patterns”, In: EuroPLoP. Disponível em < http://hillside.net/europlop/europlop2003/papers/WritingGroup/WG4_RomanoskyS. doc> acesso em janeiro de 2010.

Schumacher, M., Fernandez, E. B., Hybertson, D., Buschmann, F. and Sommerlad, P. (2006) “Security Patterns”, J.Wiley & Sons.

SG-SBP (2008) “Recommendation for Creating a Comprehensive Framework for Risk Management and Compliance in the Financial Services and Insurance Industries”, Information Technology Industry Council (ITI). Disponível em <www.incits.org/tc_home/sbp.htm> acesso em janeiro de 2010.

SSE-CMM Project (2003) “Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document”, Version 3.0. Disponível em <www.sse-cmm.org> acesso em dezembro de 2009.

Weiss, M. and Mouratidis, H. (2008) “Selecting Security Patterns that Fulfill Security Requirements”, In: 16th IEEE International Requirements Engineering Conference pages 169–172. IEEE Computer Society.

Wiander, T. (2007) “ISO/IEC 17799 Standard’s Intended Usage and Actual Use by the Practitioners”, In: 18th Australasian Conference on Information Systems. Toowoomba, 5-7.

Yoder, J. and Barcalow J. (1997) “Architectural Patterns for Enabling Application Security”, In: 4th Conference on Pattern Languages of Programs.

Yoshioka, N., Honiden, S. and Finkelstein, A. (2004) “Security Patterns: A Method for Constructing Secure and Efficient Inter-Company Coordination Systems”, In: 8th IEEE Intl Enterprise Distributed Object Computing Conf (EDOC 2004).