UFSM – UNIVERSIDADE FEDERAL DE SANTA MARIA

CENTRO DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

PROCESSOS DE DESENVOLVIMENTO DE SOFTWARE CONFIÁVEIS BASEADOS EM PADRÕES DE SEGURANÇA

DISSERTAÇÃO DE MESTRADO

Rosana Wagner

Santa Maria, RS, Brasil

2011

PROCESSOS DE DESENVOLVIMENTO DE SOFTWARE CONFIÁVEL BASEADOS EM PADRÕES DE SEGURANÇA

por

Rosana Wagner

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Informática, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção de grau de
Mestre em Informática

Orientadora: Professora Doutora Lisandra Manzoni Fontoura

Santa Maria, RS, Brasil
2011

UFSM – UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

PROCESSOS DE DESENVOLVIMENTO DE SOFTWARE CONFIÁVEL BASEADOS EM PADRÕES DE SEGURANÇA

elaborada por
Rosana Wagner

como requisito parcial de obtenção de grau de
Mestre em Informática

COMISSÃO EXAMINADORA:

Lisandra Manzoni Fontoura, Dra.
(Presidente/Orientadora)

Raul Ceretta Nunes, Dr. (UFSM)

Luís Alvaro de Lima Silva, Dr.
(COLÉGIO POLITÉCNICO DA UFSM)

Santa Maria, 1 de março de 2011

W134p Wagner, Rosana
Processos de desenvolvimento de software confiáveis baseados em padrões de segurança / por Rosana Wagner. – 2011.
105 f. ; il. ; 30 cm

Orientador: Lisandra Manzoni Fontoura
Dissertação (mestrado) – Universidade Federal de Santa Maria, Centro de Ciências e Tecnologia, Programa de Pós-Graduação em Informática, RS, 2011

1. Informática 2. 3. Segurança da informação 4. Padrões de segurança 5. Softwares I. Fontoura, Lisandra Manzoni II. Título.

CDU 004.42

Ficha catalográfica elaborada por Denise Barbosa dos Santos – CRB 10/1756
Biblioteca Central UFSM

Agradecimento

A Deus, em primeiro lugar, por ter me dado forças nesta difícil caminhada e continuar me abençoando diariamente.

Aos meus pais, Leonor e Marlene, pelo carinho e atenção dispensados durante toda minha vida, e mais intensamente nesta importante fase.

Ao meu maravilhoso namorado, Douglas, pela atenção e carinho.

Mano Tiago e cunhada Franciela, pela força.

A professora Lisandra, pela excelente orientação, amizade e pelo exemplo que representa para mim.

Ao professor Marcos, pelo ingresso no curso.

As amigas, Cris e Rô. Aos amigos inesquecíveis do PPGEP.

Todos vocês foram extremamente importantes durante esta fase da minha vida.

Obrigada, esta conquista divido com todos vocês.

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Informática
Universidade Federal de Santa Maria

PROCESSOS DE DESENVOLVIMENTO DE SOFTWARE CONFIÁVEL BASEADOS EM PADRÕES DE SEGURANÇA

AUTORA: Rosana Wagner
ORIENTADORA: Prof. Dra. Lisandra Manzoni Fontoura
Local e data da defesa: Santa Maria, 01 de março de 2011.

As organizações enfrentam uma série de dificuldades para atender às exigências previstas pelas normas e modelos de segurança de software. As normas e modelos fornecem um conjunto de boas práticas de segurança que devem ser seguidas, mas não descrevem como essas práticas devem ser implementadas. Padrões de segurança documentam boas soluções de segurança que podem ser incorporadas ao processo de software, mas são difíceis de serem incorporados em cada fase do desenvolvimento de software.

Desta forma, a proposta deste trabalho propõe uma metodologia para adaptação de processos de software com base em requisitos de segurança, preconizados pelas práticas de segurança do *Systems Security Engineering Capability Maturity Model* (SSE-CMM). A adaptação tem como base um *framework* de processo elaborado a partir do *Rational Unified Process* (RUP) e de padrões de segurança propostos na literatura. A partir desta metodologia, os gerentes de projetos, ou papéis relacionados, encontram suporte para suas decisões referentes à implementação de segurança da informação.

Ainda, algumas regras de associações de padrões às áreas de processo[1], descritas pelo SSE-CMM, foram inicialmente propostas e inseridas no *framework*, porém, são apenas sugestões e devem ser adaptadas conforme a necessidade de cada projeto, bem como do entendimento de cada engenheiro ou gerente de projeto, e devem evoluir a medida que a organização aprenda com projetos passados.

A metodologia e as regras de associações são suportadas por uma ferramenta, a SMT- Tool, desenvolvida com o objetivo de apoiar a realização da tarefa de adaptação de processos.

Palavras-chave: Segurança da Informação, Padrões de Segurança, Processos de Software, SSE-CMM.

[1] Área de Processo – no SSE-CMM, áreas de processos correspondem às 22 divisões criadas no modelo.

ABSTRACT

Master's Dissertation
Graduation Program in Computer Science
Federal University of Santa Maria

RELIABLE SOFTWARE DEVELOPMENT PROCESSES BASED ON SECURITY PATTERNS

AUTHOR: Rosana Wagner
ADVISOR: Prof. Dra. Lisandra Manzoni Fontoura
Place and date: Santa Maria, March 01st, 2011.

Organizations face a series of difficulties in answering to the demands that are projected by the norms and models of software security. The norms and models provide a set of good security practices which should followed but do not describe how these practices must be implemented.

Security patterns document good security solutions which can be incorporated to the software process. However they are difficult to be incorporated in each software development phase. In way, this work proposes a methodology for the adaptation of software processes based on security requirements that are preconized by the security practices of the *Systems Security Engineering Capability Maturity Model* (SSE-CMM).

The basis for adaptation is a process framework that is elaborated from the *Rational Unified Process* (RUP) and security patterns proposed on the literature. By means of this methodology, the project managers, or related roles, find support for their decisions referent to the implementation of information security.

In addition, some process area[2] pattern association rules have initially been proposed and inserted in the framework. Although they are only suggestions and should be adapted according to the necessity of each project. In addition they should be adjusted according to the understanding of each project engineer or manager. Finally, they should evolve to the extent that the organization learns from past projects.

The methodology and the association rules are supported by a developed tool, the SMT- Tool. The aim of this tool is to help the development of the process adaptation task.

Keywords: Information Security, Security Patterns, Software Processes.

[2] Process Area – at SSE-CMM, process areas correspond to the 22 divisions created in the model.

LISTA DE ABREVIATURAS

BSI	-	*Build Security In*
CMM	-	Capability Maturity Model
FDD	-	Feature Driven Development
IDEAL	-	Initiating, Diagnosing, Establishing, Acting and Learning
IEC	-	International Electrotechnical Commission
ISACA	-	Information Systems Audit and Control Foundation
ISO	-	International Organization for Standardization
NIST	-	*National Institute of Standards and Technology*
NSA	-	*National Security Agency*
OMG	-	*Object Management Group*
PA	-	*Process Area*
PDCA	-	*Plan-Do-Check-Act*
PRiMA	-	*Project Risk Management Approach*
PRiMA-F	-	*Project Risk Management Approach - Framework*
PRiMA-M	-	*Project Risk Management Approach - Metamodel*
PSPO	-	Processo de Software Padrão da Organização
PEP	-	Processo Específico para o Projeto
RUP	-	*Rational Unified Process*
SMT	-	*Security Methodology Tailoring*
SEI	-	*Software Engineering Institute*
SGSI	-	Sistema de Gestão da Segurança da Informação
SI	-	Sistemas de Informação
SSE-CMM	-	*Systems Security Engineering Capability Maturity Model*
SSDP	-	*Secure Software Development Process*
TI	-	Tecnologia da Informação
UML	-	*Unified Modeling Language*
XP	-	*Extreme programming*

SUMÁRIO

1 INTRODUCÃO

A falta de segurança em projetos de software é uma das principais preocupações das organizações. É por meio das vulnerabilidades presentes em projetos de software que ocorre a quebra de sigilo e roubo de informações. Devido a esse fator, as organizações estão buscando adotar medidas cada vez mais rigorosas de proteção alinhadas a normas e metodologias de segurança (BRAZ, 2009).

As ameaças à segurança das informações dos negócios, de propriedade intelectual e a privacidade das informações pessoais estão aumentando. Assim, a necessidade de conter tais ameaças, presentes a cada dia, faz com que o gerenciamento da segurança de informações ganhe mais importância nas empresas. De acordo com um estudo realizado por McAfee (MCAFEE, 2009), o roubo de dados e violações de crimes cibernéticos pode ter custado para as empresas, em 2008 mais que U$ 1 trilhão em razão da perda de propriedade intelectual e dos gastos com a reparação dos prejuízos. Esses dados são assustadores e se pudessem ser previstos certamente poderiam ter sido evitados através da implementação de alguns modelos de segurança como: ISO 27001, ISO 27002, SSE-CMM, entre outros; como indicado por (ERNST; YOUNG, 2008).

O CERT do *Software Engineering Institute* (SEI) é um centro de peritos em Segurança na Internet. Suas estatísticas mostram que o número de vulnerabilidades nas aplicações relatadas aumentou de 171 em 1995 para 6058 em 2008 (CERT, 2008). Uma fonte de problemas de segurança é a não consideração de requisitos de segurança no completo desenvolvimento do sistema (KUMAR, 2009).

Requisitos de segurança são encontrados em normas e modelos como o Modelo SSE-CMM e as normas ISO/IEC 27001, ISO/IEC 15408 e ISO/IEC 13335.

O Modelo SSE-CMM (*System Security Engineering Capability Maturity Model*), (SEI, 2003), atualmente conhecido como o padrão ISO/IEC 21817, fornece um conjunto de boas práticas de segurança que podem ser adotadas pelas organizações para aumentar a segurança do software.

A norma ISO/IEC 27001 – Requisitos para Sistemas de Gestão de Segurança da Informação (ABNT, 2005) foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação.

A Norma ISO/IEC 15498 – Apresenta critérios de avaliação para segurança em TI e a Norma ISO/IEC 13335, apresenta gerenciamento de informações e comunicação da segurança da tecnologia.

Esses modelos e normas são indicados para o desenvolvimento de software seguro e para a elaboração de processos de gerenciamento de segurança. Porém, como qualquer outra norma ou modelo de segurança, estes fornecem as boas práticas de segurança a serem adotadas, mas não descrevem como elas devem ser incorporadas aos processos (BRAZ, 2009).

Os padrões de segurança fornecem soluções já consolidadas para problemas recorrentes de segurança e servem de referência para as organizações que buscam satisfazer requisitos de segurança (SCHUMACHER *et al.*, 2006). Assim, a utilização de padrões de segurança é uma estratégia que pode ser adotada para adaptação de processos de software, visando torná-los confiáveis por meio da inserção de atividades que visam implementar segurança conforme solução descrita no padrão.

Adaptação de processos consiste em alterar ou adaptar as descrições de um processo para um fim particular. Por exemplo, um Processo Específico do Projeto (PEP[3]) é elaborado por adaptar o Processo de Software Padrão da Organização (PSPO[4]) para encontrar os objetivos, restrições e ambiente do projeto em particular. Isto é, a adaptação é o ato de adaptar o processo padrão da organização para encontrar as necessidades específicas de um projeto. Atualmente, a adaptação de processos é considerada uma tarefa obrigatória durante a fase de planejamento, especialmente se a organização obedece a normas internacionais como ISO ou CMMI (*Capability Maturity Model Integration*). Muitas vezes essa tarefa é executada de maneira *ad-hoc*, sem guias ou métodos sistemáticos (RUI; HAO; ZHIQING, 2009).

Neste trabalho, a adaptação dá-se através da seleção e incorporação de padrões ao processo de software da organização, instanciado a partir do *framework*¸ originando o processo de software específico para uso em um projeto. Uma metodologia para adaptação de

[3] PEP –Alterar ou adaptar uma descrição do processo para torná-lo apto para ser utilizado em uma situação particular (SEI, 2009).

[4] PSPO – A definição dos processos básicos utilizados como base para o estabelecimento dos processos comuns a toda a organização. Descreve os elementos do processo fundamentais que se espera que sejam incorporados aos processos (SEI, 2009).

processos baseada no *framework* é proposta. A contribuição deste trabalho consiste na proposta da metodologia para adaptação de processos de software e pelo *framework*, que pode ser customizado pelo usuário.

1.1 Definição do Problema

A crescente necessidade de produtos de software que suportam processos de negócios tem motivado consideravelmente pesquisadores no melhoramento de processos de desenvolvimento de software. Neste sentido, a engenharia da segurança da informação aumentou sua importância, tornando-se parte de processos de negócios a fim de proteger os ativos e as informações das organizações. De acordo com CERT, defeitos de segurança em software são as principais preocupações que profissionais de segurança lidam (NUNES; BELCHIOR; ALBUQUERQUE, 2009).

Através do conhecimento da literatura, pode-se afirmar claramente que problemas relacionados à segurança existem, e ao mesmo tempo existem normas de segurança que buscam solucionar tais problemas. Estas normas não são escassas, porém, cada uma delas trata de determinados problemas. A integração destas, através do reconhecimento das partes mais importantes consideradas em cada uma delas e para cada projeto especificamente, pode tornar-se mais eficaz e apresentar um processo mais robusto e completo.

Neste sentido, o problema definido para esta pesquisa é:

> Como elaborar processos de software seguros?

1.2 Escopo e contribuições da pesquisa

Esta dissertação apresenta como contribuição a proposta de uma abordagem sistemática para associar requisitos de segurança a padrões de segurança, chamada de SMT – *Security Methodology Tailoring*. A elaboração de um processo, para uso em projetos específico de software, ocorre com base no processo padrão da organização e nos bens de processos, armazenados em uma base de conhecimento. Base de conhecimento pode ser definida como um repositório centralizado para informações (a base de conhecimento utilizada nesta dissertação estava parcialmente cadastrada na PRiMA-Tool e compreende nos dados cadastrados na ferramenta utilizada para a validação), e bens de processo são elementos utilizados para a elaboração dos processos como atividades, artefatos, disciplinas, entre outros.

Este trabalho é uma extensão de um trabalho anterior intitulado "PRiMA: *Project Risk Management Approach*" (FONTOURA, 2006). PRiMA consiste em uma sistemática para permitir a elaboração de um processo específico para um dado projeto, visando minimizar a exposição do projeto aos riscos, identificados e mensurados de acordo com o contexto do projeto.

A principal contribuição deste trabalho é experimentar o uso de padrões de segurança para adaptação de processos de software com base na análise da segurança a ser empregada em cada projeto. Outras contribuições do trabalho incluem:

- ✓ Estudo, análise e apresentação das principais normas de segurança;
- ✓ O estabelecimento de uma base de dados inicial e de um *framework* de processo.
- ✓ Extensão do *framework* PRIMA-F para englobar requisitos de segurança dando origem ao *framework* SMT, e a complementação da Base de Conhecimento existente para incorporar padrões e elementos (atividades, artefatos, papéis) relacionados à segurança;
- ✓ Descrição de dois estudos de caso realizados, relatando os resultados obtidos no uso da sistemática SMT.

1.3 Estrutura da dissertação

O texto está organizado como segue. No capítulo 2 são apresentados os referenciais teóricos relacionados a definições e normas de modelos de segurança, e os requisitos de segurança que foram gerados a partir destas normas e modelos.

No capítulo 3 conceituam-se processos de software e os modelos de processo de software como RUP, XP e SCRUM, que são os processos de software utilizados no PRiMA *Framework.*

No capítulo 4 Padrões de Segurança são introduzidos e descreve-se como estes são associados a requisitos de segurança.

No capítulo 5 são apresentadas a metodologia proposta, a base de conhecimento, e a associação dos requisitos de segurança aos padrões.

No capítulo 6 é descrita a ferramenta desenvolvida para suportar a automatização dos processos de integração de segurança nas atividades do processo.

No capítulo 7 são descritos dois estudos de casos realizados para validação da metodologia proposta.

O capítulo 8 conclui com os trabalhos relacionados, as considerações finais e os trabalhos futuros a esta dissertação.

2 SEGURANÇA DA INFORMAÇÃO

Softwares geram informações. Neste sentido, segurança do software está diretamente relacionado à segurança da informação. Segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada (FONTES, 2008).

Proteger informações confidenciais é um fator crítico de sucesso para qualquer organização. A reputação de "segurança" de uma empresa está se tornando um ponto importante à medida que mais e mais clientes estão considerando práticas de segurança e privacidade como um fator importante para a tomada de decisão ao escolher um fornecedor de serviços (COMPAGNA et al., 2008).

Segurança é a base para dar às empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. A segurança de software corresponde à habilidade do software resistir e tolerar eventos que intencionalmente ameacem sua dependabilidade (BRAZ, 2009). Para McGraw (MCGRAW, 2005), a segurança de software refere-se à "construção de software seguro: projetá-lo para que seja seguro, se certificar da sua segurança e educar desenvolvedores, arquitetos e usuários sobre como construir produtos seguros."

Sêmola (SÊMOLA, 2003) define segurança da informação como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Pode-se também considerar como a prática de gestão de riscos de incidentes que impliquem no comprometimento de três principais conceitos da segurança: confiabilidade, integridade e disponibilidade da informação. Em relação aos aspectos da segurança da informação o autor diz que alguns elementos são considerados essenciais na prática da segurança da informação, dependendo do objetivo que se pretende alcançar.

2.1 Normas e Modelos de Segurança

Normas e modelos de segurança apresentam práticas fundamentais para que organizações possam estar de acordo com um nível esperado de segurança. Nessa seção são descritas normas e modelos que foram considerados no desenvolvimento desta dissertação. Estas foram escolhidas por serem atualmente as principais normas presentes na literatura que tratam de segurança de sistemas.

2.1.1 Modelo SSE-CMM

A iniciativa do SSE-CMM com um patrocínio da NSA (*National Security AgencY*) aconteceu em Abril de 1993, com pesquisa nos trabalhos existentes *sobre Capability Maturity Models* (CMMs) e investigação sobre a necessidade de um modelo de CMM especializado para tratar de engenharia de segurança.

O SSE-CMM é um modelo de processo de referência. Centra-se nos requisitos para implementação de segurança e em um sistema ou de uma série de sistemas que estão relacionadas com o domínio da tecnologia da segurança da informação. O SSE-CMM foi desenvolvido para evoluir a prática da engenharia de segurança e com o objetivo de melhorar a qualidade e a disponibilidade, reduzindo o valor gasto na produção de sistemas seguros e de produtos confiáveis (LACHAPELLE, 2007). Em 2002 tornou-se a norma ISO/IEC 21827, com a iniciativa de sedimentar internacionalmente a eficácia da aplicação do modelo.

O SSE-CMM afirma que a segurança é parte integrante dos esforços de engenharia que tratam dos problemas de segurança do hardware, software, sistemas ou empresa. Este modelo define características de um processo de engenharia de segurança, o qual é explicitamente definido, gerenciado, medido, controlado e eficaz (SEI, 2003). O objetivo é entrar em um contínuo ciclo de avaliação do estado atual, fazendo melhorias e repetindo o ciclo. As etapas do SSE-CMM para melhorar processo seguem o modelo IDEAL do SEI (SEI, 2003).

As Práticas base do modelo SSE-CMM diretamente relacionadas à segurança são mostradas na Tabela 2.1

Tabela 2.1: Práticas base do modelo SSE-CMM diretamente relacionadas à segurança.

PA (Process Area)	Objetivo
PA01-Administração dos 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- Avaliação do Impacto	Identificar os impactos que são motivos de preocupação no que diz respeito ao sistema e para avaliar a ocorrência de impactos.
PA03-Avaliação os 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 a ameaças. Especificamente a atividade envolve a identificação e avaliação da probabilidade da ocorrência de riscos.
PA04-Avaliação das ameaças	Identificar as ameaças de segurança, suas características e propriedades.
PA05-Avaliação das 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-Construção de argumentos de garantia	Transmitir claramente que as necessidades de segurança do cliente são cumpridas.
PA07-Coordenação da segurança	Assegurar que as partes envolvidas com atividades de engenharia da segurança são adequadas e consistentes. Esta coordenação envolve a manutenção da aberta – comunicação entre grupos de segurança, outros grupos de engenheiros e grupos externos.
PA08-Monitoração da postura de 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.
PA09-Fornecer entrada de segurança	Fornecer a 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 este processo 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-Verificação e validação da segurança	Assegurar que 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.

SSE-CMM divide engenharia de segurança em três áreas básicas: risco, engenharia e garantia (TOVAR et al., 2006):

- Risco - visa identificar e priorizar riscos associados com o desenvolvimento de produtos ou sistemas.
- Engenharia - trabalha com outros disciplinas para implementar soluções para os perigos identificados, neste caso, relacionados com a engenharia de software.

- Garantia - visa certificar que as soluções implementadas são confiáveis.

Este modelo também pode ser relacionado a processos de gestão como o *Control Objetives for Information and related Technology* (COBIT), conforme no artigo intitulado Análise dos Critérios de Segurança do COBIT baseado no Modelo SSE-CMM, publicado no CLEI 2010. (WAGNER, 2010), onde é descrita uma avaliação do COBIT baseada nas práticas base do *System Security Engineering Capability Maturity Model* (SSE-CMM). Para cada prática base (PB) identificada em cada área de processo (PA) das práticas base de segurança (PA01 a PA11), o COBIT foi avaliado para determinar se ele satisfaz a PB ou não. Para cada PA, o percentual de PB suportado foi calculado, e os resultados foram tabulados.

Observou-se que apenas quatro das onze práticas base do modelo SSE-CMM foram atendidas pelo COBIT. Sabe-se que o COBIT não é voltado apenas para a segurança de software como acontece com o modelo SSE-CMM, e desta forma conclui-se que através dos processos do COBIT, em relação à governança de TI, tem-se uma gama relativamente grande de processos ligados a segurança. O COBIT apresenta um processo bem definido de governança de TI, mas não é uma abordagem centrada no que diz respeito à segurança da informação. Portanto, ele precisa de complementos com implantação de novas práticas preconizadas por modelos de segurança para que a organização possa tornar-se mais confiante neste sentido.

2.1.2 Norma ISO/IEC 17799 e ISO/IEC 27001

As normas ISO/IEC 17799 e ISO/IEC 27001 foram preparadas para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização. É esperado que o SGSI e seus sistemas de apoio mudem com o passar do tempo e que a implementação seja escalada conforme as necessidades da organização (LACHAPELLE, 2007).

Estas normas têm grandes semelhanças, sendo que muitos dos processos podem ser considerados como princípios básicos para o estabelecimento da segurança em qualquer tipo

de organização. A principal diferença entre estas normas é que a ISO/IEC 17799 como é mais detalhada, descreve controles e regras a serem seguidos na implementação da segurança, e a ISO/IEC 27001 trata de segurança em um nível mais elevado, voltado para a direção e alta administração da organização.

A norma ISO/IEC 27001:2006 aplica um sistema de processos dentro da organização, junto com a identificação e interações destes processos. Essa abordagem de processos enfatiza a importância dos seguintes aspectos:

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;

- Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos globais do negócio;

- Monitoração e analise critica do desempenho e da eficácia do SGSI; e

- Melhoria contínua baseada em medições objetivas.

A norma ISO/IEC 27001 adota o modelo conhecido como PDCA - "*Plan-Do-Check-Act*", que é aplicado para estruturar todos os processos do SGSI. O ciclo PDCA baseia-se no ciclo de melhoria continua que consiste em: planejar (*Plan* - P), fazer (*Do* - D), verificar (*Check* - C) e agir (*Act* - A). O ciclo PDCA é uma ferramenta importante para a análise e melhoria dos processos organizacionais contribuindo para a tomada de decisões gerenciais e para o alcance das metas e objetivos da organização (KAJAVA et al., 2006)

2.1.3 ISO/IEC 15408

A ISO/IEC 15408, também chamada de *Common Criteria*, é um conjunto de critérios que permite a especificação da segurança de uma aplicação, baseado nas características do ambiente de desenvolvimento.

A norma ISO/IEC 15408 permite a realização de uma comparação entre os resultados das avaliações independentes da segurança. Através disso, a norma visa fornecer um conjunto de requisitos comuns para as funções de segurança em produtos e sistemas e para garantia de medidas aplicadas a eles durante uma avaliação de segurança (ISO, 2005).

O processo de avaliação estabelece um nível de confiança de que as funções de segurança desses produtos e dos sistemas e da garantia das medidas aplicadas para eles

atendem a esses requisitos. Os resultados dessa avaliação podem auxiliar os consumidores a determinar se o produto ou sistema é seguro o suficiente para o que a sua aplicação se destina e se os riscos de segurança implícita em seu uso são toleráveis (BRAZ, 2009).

Seu objetivo é ser usado como base para avaliação de propriedades de segurança de produtos e sistemas de TI, permitindo a comparação entre os resultados de avaliações independentes de segurança, por meio de um conjunto de requisitos padronizados a ser atingidos. O processo de avaliação estabelece níveis de confiabilidade de que as funções avaliadas atingem os requisitos estabelecidos, ajudando os usuários a determinar se tais sistemas ou produtos possuem os níveis desejados de segurança e se os riscos advindos de seu uso são toleráveis. Seu público alvo são os desenvolvedores, avaliadores e usuários de sistemas e produtos de TI que requerem segurança. O padrão está dividido em três partes (ISO, 2005):

- Introdução e modelo geral - onde são definidos os conceitos e princípios seguidos pelo modelo, além de uma nomenclatura e uma diagramação, baseada na orientação de objetos específicos para a formulação de objetivos de segurança, para selecionar e definir seus requisitos e para especificações de altos níveis de produtos e sistemas;
- Requisitos funcionais de segurança - estabelecendo um conjunto de elementos funcionais para a padronização dos requisitos divididos em classes, como gestão de segurança, privacidade e comunicação.
- Requisitos da garantia de segurança - estabelecendo um conjunto de elementos para a padronização da garantia da segurança divididos ao longo do ciclo de desenvolvimento dos produtos ou sistemas.

2.1.4 ISO/IEC 13335

Publicada em 1998, descreve técnicas de gestão de segurança para a área de tecnologia da informação. Pode ser utilizada para trabalhar em conjunto com a BS 7799-2, que sugere quais os processos devem ser implantados para conduzir a gestão de segurança, enquanto a ISO/IEC 13335 descreve as técnicas (SIEWERT, 2006).

A Norma ISO/IEC 13335 (2004) faz parte de uma série de normas que lidam com os aspectos de gestão de planejamento, implementação e operação, incluindo manutenção, tecnologia da informação e comunicação (TIC) de segurança.

A norma consiste em 5 partes, sob o título geral de tecnologia da informação (SIEWERT, 2006):

Parte 1: conceitos e modelos para segurança em TI.

Parte 2: gerenciamento e planejamento da segurança TI.

Parte 3: técnicas para o gerenciamento de segurança em TI.

Parte 4: seleção de proteção.

Parte 5: proteção para conexões externas.

A norma provê diretrizes no gerenciamento da segurança em TI. Deve ser adequada às necessidades específicas de cada organização.

Governo e organizações comerciais dependem muito do uso da informação para realizar suas atividades empresariais. Comprometimento de confidencialidade, integridade, disponibilidade, não repúdio, autenticidade da responsabilidade e da confiabilidade dos bens de uma organização podem ter impactos adversos. Conseqüentemente, há uma necessidade crítica para proteger informações e para gerenciar a segurança dos sistemas TICs dentro das organizações. Esta obrigação de proteger a informação é particularmente importante no ambiente atual, já que muitas organizações estão conectadas internamente e externamente por redes de sistemas de TIC não necessariamente controlado pela própria organização (ISO, 2004).

2.2 Requisitos de segurança de software

Os requisitos de segurança de software necessitam absorver as necessidades de segurança da organização estabelecidas em suas políticas de alto nível, sob pena de comprometer a sustentabilidade associada ao negócio. Observa-se como ponto chave na especificação dos requisitos de segurança o reconhecimento das ameaças a que o software está submetido, considerando, consequentemente, políticas de alto nível para determinação da pertinência de cada uma das ameaças levantadas (TONDEL; JAATUM; MELAND, 2008).

Para definir os requisitos, engenheiros de sistemas podem, em conjunto com os usuários, executar análises *top-down* e *bottom-up* de possíveis falhas de segurança que poderia causar risco para a organização, bem como definir os requisitos para solucionar vulnerabilidades (GOERTZEL, 2007).

Braz (2009) em sua tese define requisitos de segurança como as necessidades do software para que ele atenda as políticas regulatórias e institucionais do seu negócio. Portanto, o papel dos seus requisitos de segurança é de fornecer informações sobre a real necessidade do sistema ou aplicação de forma a alcançar seus objetivos de negócios.

Segundo a ISO/IEC 27001, segurança da informação implica na preservação da confiabilidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade e não repúdio podem também estar envolvidas.

Ainda conforme a norma ISO/IEC 27001 é essencial que uma organização identifique os seus requisitos de segurança da informação. Existem três fontes principais de requisitos de segurança da informação.

1. Uma fonte é obtida a partir da análise/avaliação de riscos para a organização, levando em conta os objetivos e as estratégias globais de negócio. Por meio da analise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
2. Outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviços têm que atender, além do seu ambiente sociocultural.
3. A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Ameaça, vulnerabilidade e impactos são considerados conceitos importantes quando se fala em segurança e são definidos pelos seguintes conceitos:

- Ameaça é uma causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ISO, 2009), ou ainda, ameaça é um agente externo ao ativo de informação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por esse ativo (CAMPOS, 2007).

- Vulnerabilidade é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças NBR ISO/IEC 27002 (2009).
- Impactos de incidentes referem-se aos potenciais prejuízos causados ao negócio por esse incidente. Tais prejuízos podem significar perdas financeiras, desgaste da imagem na organização perante o mercado ou perda de recursos e colaboradores (CAMPOS, 2007).

A norma ISO/IEC 27001 (2009) diz que os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação. Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, bem como a implementação dos controles selecionados para a proteção contra estes riscos. Esta análise/avaliação deve ser repetida periodicamente para contemplar quaisquer mudanças.

Sommerville (2007) trata de confiança, disponibilidade e segurança em sistemas. Em relação à confiança no sistema define que o grau de confiança dos usuários em que o sistema irá operar conforme sua expectativa e que não irá ‘falhar’ durante seu uso normal. Alguns sistemas como, por exemplo, um processador de texto não tem como principal preocupação a confiabilidade, então é necessário o bom senso do usuário em tomar algumas medidas de precauções, como salvar o trabalho frequentemente, para que não tenha maiores problemas.

Ainda, Ferreira e Araújo (2008) em seu livro que contém um guia prático para elaboração e implementação recomenda que seja estabelecido na política corporativa um capítulo destinado ao detalhamento e à explicação dos seguintes conceitos:

- **Confidencialidade**: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- **Integridade**: garantia de que a informação está correta, é verdadeira e não está corrompida.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Auditabilidade**: o acesso e o uso das informações devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

- **Legalidade**: o acesso e o uso da informação devem estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;
- **Não repúdio de autoria**: o usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Tais conceitos são considerados os principais requisitos de segurança, porém podem desdobrar-se em conceitos mais detalhados facilitando assim seu entendimento e implementação.

Em seguida é mostrado detalhamentos e conceitos sobre cada requisito especificado.

- **Autenticação**: capacidade de garantir que um usuário, sistema ou informação é mesmo quem alega ser.
- **Privacidade**: capacidade de um sistema de manter incógnito um usuário, impossibilitando a ligação direta da identidade do usuário com as ações por este realizadas.
- **Controle de registros -** Registros devem ser estabelecidos e mantidos para fornecer evidências de conformidade.
- **Processo de autorização para os recursos de processamento da informação** - Deve ser definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.
- **Controle contra códigos maliciosos** - Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos.
- **Registro de usuário** - Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.
- **Gerenciamento de privilégios** - A concessão e o uso de privilégios devem ser restritos e controlados.
- **Restrição de acesso à informação** - O acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte deve ser restrito de acordo com o definido na política de controle de acesso.
- **Gerenciamento de senha do usuário** - A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.
- **Sistema de gerenciamento de senha** - Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.

- **Identificação e autenticação de usuário** - Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.
- **Autenticação dos dados** - permite a uma entidade a aceitar a responsabilidade pela autenticidade das informações (por exemplo, digitalmente assinado). Fornecer uma garantia da validade de uma unidade específica de dados que podem ser posteriormente utilizados para verificar se o conteúdo da informação não tenha sido forjada ou fraudulentamente modificado.
- **Uso aceitável dos ativos** – Devem ser identificadas, documentadas e implementadas regras que permitam o uso de informações e de ativos associados aos recursos de processamento da informação.
- **Registros de auditoria** - Registros *(log)* de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
- **Monitoramento do uso do sistema** - Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.
- **Proteção das informações dos registros (*log*)** - *R*ecursos e informações de registros (*log*) sejam protegidos contra falsificação e acesso não autorizado.
- **Registros (*log*) de administrador e operador** - Convém que as atividades dos administradores e operadores do sistema sejam registradas.

Os requisitos de segurança acima apresentados demonstram apenas exemplos. De acordo com Mead (2003), McGraw (2006) e Moffett, Haley, Nuseibeh (2004) a arte de identificar e manter requisitos de segurança é um complexo empreendimento que merece amplo tratamento. Através de tal definição neste trabalho busca-se apenas exemplificar requisitos de segurança que podem ser necessários para algum sistema. Novos requisitos surgem a cada nova vulnerabilidade, ameaça etc. encontrada em projetos.

Campos (2007) em seu livro diz que problemas de segurança acontecem em ativos de informações que sofrem com fraquezas que podem ser intencionais ou não, resultando assim na quebra de um ou mais princípios de segurança da informação, essas fraquezas são

intituladas vulnerabilidades e podem vir a ocorrem através de: Tecnologias - como, por exemplo, computadores, CDs, portas USBs, acesso a rede local ou internet, aparelhos de fax, impressoras, etc.; Pessoas - pessoas mudam de emprego, ficam doentes; Processos - contratações, relações entre colaboradores; Ambiente - são suscetíveis a incêndios, enchentes, terremotos, acesso de pessoas não autorizadas.

Medidas de segurança também são imprescindíveis para o sucesso da segurança da informação. Sêmola (2003) define medidas de segurança como práticas, procedimentos e mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades. Medidas de segurança são consideradas controles que podem ter as seguintes medidas:

- Preventiva: tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança da instituição.
- Detectáveis: visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades.
- Corretivas: ações voltadas à correção de uma estrutura tecnológica e humana para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição.

Além de todos esses conceitos que devem ser levados em conta no momento da definição de requisitos de segurança do sistema também é necessário que o usuário esteja consciente da importância da segurança no sistema, para que ele possa auxiliar na implementação da política da segurança da informação tomando medidas preventivas e evitando maus hábitos em relação à segurança.

De acordo com a norma ISO (2009), deve-se garantir que os usuários estejam cientes das ameaças e das preocupações de segurança da informação e estejam equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho.

Os autores Halfiz, Adamczyk e Johnson (2007) afirmam que a criação de sistemas seguros é difícil, porém a adaptação dos sistemas existentes para introduzir a segurança é ainda mais difícil. Atacantes sempre desvendam novas vulnerabilidades de segurança, arquitetos de segurança têm dificuldade em prever novos ataques antecipadamente. Confiabilidade, integridade e disponibilidade são consideradas padrões de segurança.

A segurança do software é uma idéia da Engenharia de Software e busca que um produto desenvolvido continue funcionando corretamente diante de ataques maliciosos (MCGRAW, 2004). Segundo Tovar et al. (2006), por traz de cada problema de segurança em um

computador e de cada ataque malicioso há um inimigo em comum: a baixa qualidade de software.

Algumas vezes a Segurança do Software é confundida com a Segurança do Sistema, neste trabalho trataremos apenas de processo para desenvolvimento de produtos com segurança e não a verificação e ajustes em problemas atuais de segurança existentes no software.

3. PROCESSOS DE SOFTWARE

A utilização de processos de software tem sido apontada como um fator primordial para o sucesso de empresas de desenvolvimento de software (MACORATTI, 2005).

Um processo de software é um conjunto de atividades que leva à produção de um produto de software. Essas atividades podem envolver o desenvolvimento de software propriamente dito. No entanto, cada vez mais, novos softwares são desenvolvidos com a aplicação e a modificação de sistemas existentes e de configuração e integração de softwares comerciais ou componentes de sistema. Embora existam muitos processos de software diferentes, algumas atividades como: especificação de software, projeto e implementação de software, validação de software e evolução de software, são comuns a todos eles (SOMMERVILLE, 2007).

Diversas razões podem ser definidas para a utilização de um processo de software padrão, como: redução dos problemas relacionados a treinamento, revisões e suporte à ferramentas; experiências adquiridas nos projetos são incorporadas ao processo padrão e contribuem para melhorias em todos os processos definidos; economia de tempo e esforço na definição de novos processos adequados a projetos (MACORATTI, 2005). A razão pela qual utiliza-se processos de software nesta dissertação é que através dos processos de software existente na organização busca-se incorporar novas atividades a este processo, gerando assim um processo adaptado.

Este capítulo introduz processos de software tradicionais e ágeis, já que os dois modelos de processos são utilizados por empresas atualmente.

3.1 Processos Tradicionais

Fowler (2010) diz que um dos objetivos das metodologias tradicionais é desenvolver um processo onde as pessoas envolvidas são partes substituíveis. Com esse processo você pode tratar as pessoas em vários tipos. Você tem um analista, alguns programadores, alguns testadores e um gerente. Os indivíduos não são tão importantes, apenas os papéis são importantes. Dessa forma, se você planeja um projeto, não importa qual analista e testadores que você conseguiu, apenas que você sabe quanto você tem para você saber como o número de recursos afeta o seu plano.

3.1.1 RUP

O *Rational Unified Process* (RUP) é um *framework* de processo para desenvolvimento de software iterativo e incremental bem sucedido (IBM, 2007). RUP fornece uma abordagem disciplinada para atribuir tarefas e responsabilidades dentro de uma organização de software. Seu objetivo é garantir a produção de software de alta qualidade que atenda às necessidades de seus usuários finais dentro de um cronograma e um orçamentos previsíveis (SHUJA, 2008).

O RUP mostra como uma equipe de software pode aplicar abordagens comercialmente comprovadas de desenvolvimento de software (IBM, 2007). RUP concentra-se em seis princípios básicos de engenharia de software, que são conhecidos como “Melhores Práticas”. Esses princípios constituem o fundamento do RUP, e são: adaptar processos; equilibrar as

prioridades das partes interessadas; colaboração entre equipes; demonstrar valor iterativamente; elevar o nível de abstração; focar na qualidade contínua (IBM, 2007).

O desenvolvimento iterativo no RUP promove e organiza o desenvolvimento de software em quatro fases, cada qual composta por uma ou mais iterações, como pode ser observado na Figura 3.1. Disciplinas têm um importante papel no projeto das iterações executadas dentro de cada fase. Disciplina é definida como uma categorização de atividades baseada em similaridade e esforço de cooperação. Dependendo da fase em que o projeto está, cada iteração é formada por um conjunto de disciplinas cuja ênfase varia. Observando-se a Figura 3.1 pode-se perceber que o gráfico associado às disciplinas varia de intensidade de acordo com a fase.

Cada fase tem objetivos bem definidos que são verificados ao final da fase nos chamados marcos de acompanhamento. A fase de *Iniciação* tem como objetivo principal definir os objetivos do ciclo de vida do projeto (escopo do software); a de *Elaboração* planejar o projeto, especificar recursos, definir e validar a arquitetura; a de *Construção* construir o produto; e a de *Transição* implantar o software (IBM, 2007).

Uma disciplina é uma coleção de atividades que estão relacionadas a uma área de concentração ou campo de estudo. Cada atividade é decomposta em subatividades ou tarefas. O RUP propõe nove disciplinas, que são divididas em seis disciplinas relacionadas diretamente à engenharia de software, também chamadas de disciplinas núcleo e três disciplinas de suporte. As disciplinas núcleo são: Modelagem de Negócios, Requisitos, Análise e Projeto, Implementação, Teste e Implantação. As disciplinas de suporte são: Gerenciamento de Configuração e Mudança, Gerenciamento de Projetos de Software e Ambiente (RATIONAL, 1998).

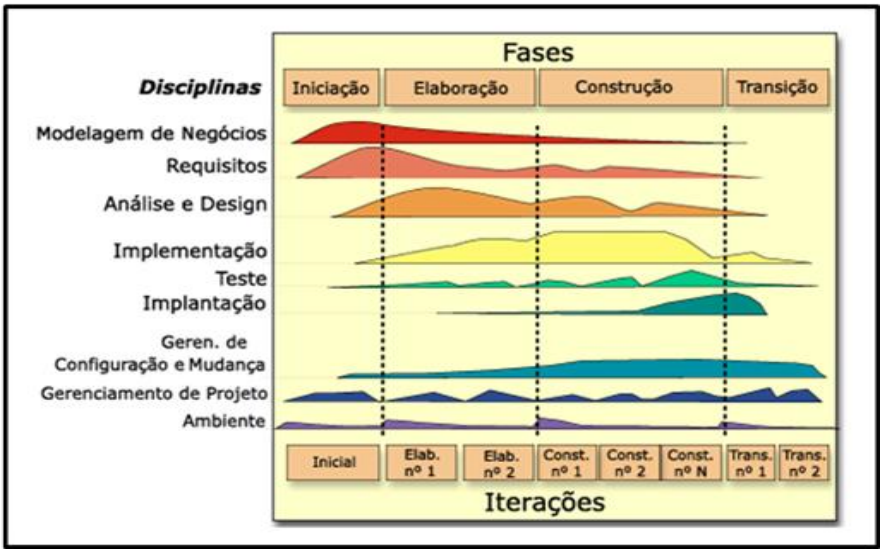


Figura 3.1 - Visão geral do RUP (adaptado de (RATIONAL, 1998).

O RUP utiliza três principais elementos para descrição de métodos que são: papel, tarefa e artefato (SHUJA, 2008). O *papel* define o comportamento e as responsabilidades de um indivíduo, ou um conjunto de indivíduos trabalhando em uma equipe, dentro do contexto de uma organização de software. O *papel* representa um cargo executado por indivíduos em um projeto e define como eles devem realizar o trabalho. Uma *tarefa* é uma unidade de trabalho que um indivíduo que representa um *papel* é encarregado de executar. Uma *tarefa* tem uma finalidade clara, usualmente expressa em termos de criação ou atualização de algum *artefato*, como um modelo, uma classe ou um plano. *Tarefas* têm *artefatos* como entrada e saída. Um *artefato* é um produto de trabalho do processo.

3.1.2 RUP Estendido para Segurança

O RUP é largamente utilizado em grandes projetos, podendo ser adaptado também a pequenos e médios, ou customizado para atender às necessidades específicas de determinado projeto de software (SHUJA, 2008). No artigo “Extensão de um *framework* de processo para adaptação à segurança em aplicações Web” publicado no WebMedia em 2010 por Wagner, Fontoura e Nunes (2010) utiliza-se o SSE-CMM para adaptar o RUP de acordo com as

recomendações de segurança deste modelo. Este trabalho vem de encontro a esta dissertação no sentido de adaptação de processos e de inclusão de uma disciplina de segurança em processos de software.

O artigo (WAGNER; FONTOURA; NUNES, 2010) difere desta dissertação no sentido de que não permite a adaptação de processos dinamicamente, além de ser uma adaptação realizada apenas para a base do RUP.

3.2 Métodos Ágeis

Em fevereiro de 2001, vários metodologistas se reuniram em Utah, nos Estados Unidos, para discutir as similaridades entre suas abordagens, que foram por eles denominadas de métodos ágeis. Métodos ágeis podem ser caracterizados por (FOWLER, 2002): Desenvolvimento Iterativo; Envolvimento do Cliente; Equipe com boa qualificação técnica; Desenvolvedores devem tomar decisões técnicas; Processo Adaptável; Mudanças nos Requisitos; Projetos Simples.

Como exemplos de métodos ágeis citam-se: *Scrum* (SCHWABER, 2001), *Extreme Programming* (XP) (BECK, 2004), *Feature Driven Development* (FDD) (BECK, 2003), *Adaptative Software Development* (ASD) (HIGHSMITH, 2004), entre outros.

3.2.1 *Extreme Programming*

XP foi proposto por Kent Bech, com base em seus vários anos de prática como desenvolvedor de software orientado a objetos. É uma metodologia leve para times de tamanho pequeno a médio, que desenvolvem software com requisitos vagos e que se modificam rapidamente (BECK 2004).

O desenvolvimento é realizado de forma iterativa e incremental. No início de cada ciclo, o cliente identifica as funcionalidades mais importantes, isto é, as que trarão maior valor para seu negócio. Essas funcionalidades são construídas e constituem versões do software. A

cada iteração, novas funcionalidades são agregadas e adicionam mais valor ao software (TELES 2004).

3.2.1.1 Valores do XP

Valores, em XP, são conceitos básicos que orientam a metodologia a ser seguida. Os valores resumem a filosofia de trabalho e a orientação a ser utilizada na tomada de decisão. Kent Beck definiu quatro valores-chave para XP, que são (BECK, 2004):

• **Comunicação**: o objetivo da comunicação é prover um lugar onde as pessoas podem livremente discutir o projeto sem medo ou represália;

• **Simplicidade**: escolha o projeto, tecnologia, algoritmos e técnicas mais simples para satisfazer as necessidades do cliente para a iteração atual do projeto;

• ***Feedback***: obtido por meio de teste de código, *User Stories*, entregas freqüentes/pequenas iterações, programação por pares/revisões constantes de código e outros métodos;

• **Coragem**: seja corajoso o suficiente para fazer o que é certo. Teste de regressão é chave para atingir esse valor.

3.2.1.2 Práticas do XP

O XP baseia-se nas seguintes práticas (TELES, 2004):

- Cliente Presente: O cliente junta-se a equipe de desenvolvimento durante todo o projeto. O trabalho do cliente é para escrever e priorizar as tarefas, auxiliar no teste de aceitação e estar à disposição para responder perguntas da equipe de desenvolvimento que possam surgir.
- Jogo do Planejamento: Onde são definidas estimativas de prazo para cada tarefa e as prioridades: quais as tarefas mais importantes.

- *Stand Up Meeting*: A equipe de desenvolvimento se reúne a cada manhã para avaliar o trabalho que foi executado no dia anterior e priorizar aquilo que será implementado no dia que se inicia. Trata-se de uma reunião rápida que recebe o nome de *stand up meeting*, que em inglês significa reunião em pé.
- Programação em Par: A programação em pares significa que todo o código é produzido por duas pessoas em uma programação de tarefas em uma estação de trabalho. Um programador tem controle sobre a estação de trabalho e está preocupado principalmente sobre a codificação o outro está revisando o código continuamente.
- Desenvolvimento Guiado por Testes: O XP é destinado à construção de sistemas com alta qualidade, o que leva à necessidade de diversos mecanismos de validação para assegurar que o software está correto. Um destes mecanismos é a programação em par, tal como foi citado anteriormente. Além dela, o XP também utiliza a técnica de desenvolvimento guiado por testes.
- *Refactoring*, Código Coletivo: Para que o sistema possa evoluir de forma incremental, a equipe deve fazer com que ele expresse os seus objetivos facilmente e esteja sempre claro e fácil de compreender. Freqüentemente, isso levará a equipe a modificar partes do sistema que estejam funcionando para facilitar a sua manutenção.
- Código Padronizado: No XP o sistema não é segmentado em partes, de modo que cada desenvolvedor fique responsável por uma delas. Os desenvolvedores têm acesso a todas as partes do código e podem alterar aquilo que julgarem importante sem a necessidade de pedir autorização de outra pessoa, pois o código é coletivo.
- *Desing* Simples: Para que o cliente possa obter *feedback* logo, a equipe precisa ser ágil no desenvolvimento, o que a leva a optar pela simplicidade do design. Ao invés de criar generalizações dentro do código, de modo a prepará-lo para possíveis necessidades futuras, a equipe deve sempre optar por um código que seja suficiente para atender às necessidades da funcionalidade que está implementando. Os desenvolvedores se baseiam na premissa de que serão capazes de incorporar qualquer necessidade futura quando e se ela surgir. Para isso, eles contam com o *refactoring*, os testes e as demais práticas do XP para apoiá-los.
- Metáfora: A metáfora descreve o sistema de conceitos simples. Os conceitos podem ser literal ou Figurado, dependendo da clareza do sistema real.
- Ritmo Sustentável: A qualidade do design, do código, das metáforas e do sistema é determinada diretamente pela qualidade dos desenvolvedores e a capacidade que

eles têm de se manter atentos, criativos e dispostos a solucionar problemas. Para garantir que a equipe tenha sempre o máximo de rendimento e produza software com melhor qualidade possível, o XP recomenda que os desenvolvedores trabalhem apenas oito horas por dia e evitem fazer horas-extras, visto que é essencial estar descansado a cada manhã, de modo a utilizar a mente na sua plenitude ao longo do dia.

- Integração Contínua: Quando uma nova funcionalidade é incorporada ao sistema, ela pode afetar outras que já estavam implementadas. Para assegurar que todo o sistema esteja sempre funcionando de forma harmoniosa, a equipe pratica a integração contínua que leva os pares a integrarem seus códigos com o restante do sistema diversas vezes ao dia. Cada vez que um par faz isso, ele executa todos os testes para assegurar que a integração tenha ocorrido de forma satisfatória.
- Releases Curtos: uma série de iterações, cada uma com duração de 2 a 4 semanas.

3.2.2 SCRUM

O Scrum é um processo de desenvolvimento iterativo e incremental para gerenciamento de projetos e desenvolvimento ágil de software.

O *framework* Scrum consiste em um conjunto formado por Times e Scrum e seus papéis associados, Eventos com Duração Fixa (*Time- Boxes*), Artefatos e Regras. Times Scrum são projetados para otimizar flexibilidade e produtividade. Para esse fim, eles são auto-organizáveis, interdisciplinares e trabalham em iterações. Cada Time Scrum possui três papéis: 1) o ScrumMaster, que é responsável por garantir que o processo seja compreendido e seguido; 2) o Product Owner, que é responsável por maximizar o valor do trabalho que o Time Scrum faz; e 3) o Time, que executa o trabalho propriamente dito. O Time consiste em desenvolvedores com todas as habilidades necessárias para transformar os requisitos do Product Owner em um pedaço potencialmente entregável do produto ao final da *Sprint* (SCHWABER; SUTHERLAND, 2009).

Apesar de Scrum ter sido destinado para gerenciamento de projetos de software, ele pode ser utilizado em equipes de manutenção de software ou como uma abordagem geral de gerenciamento de projetos/programas (SCHWABER; SUTHERLAND, 2009).

4 PADRÕES DE SEGURANÇA

Os padrões de segurança representam um conjunto de boas práticas aplicadas pela indústria para limitar ataques (SCHUMACHER et al., 2006). O principal objetivo de um padrão de segurança é fornecer uma solução para um problema. Os padrões capturam a experiência de indivíduos especialistas em segurança e fornecem soluções para problemas relacionados com a segurança, que podem ser aplicados por indivíduos não especialistas. A solução proposta pelo padrão pode ser implementada com a ajuda de outros padrões os quais resolvem subproblemas de um problema original (YOSHIOKA; HONIDEN; FINKELSTEIN, 2004).

Os padrões de segurança fornecem uma estrutura na qual descrevem uma informação particular sobre um determinado contexto para qual é aplicado o padrão. Eles materializam mecanismos básicos ou abordagens do processo que fornecem meios de proteger a confidencialidade, integridade e disponibilidade das informações (SCHUMACHER et al., 2006). Os padrões de segurança também guiam o desenvolvimento de software seguro de um modelo de análise para um modelo mais completo que satisfaz os requisitos funcionais (SOLINAS; FERNANDEZ; ANTONELLI, 2009).

Nesse sentido, observa-se que os padrões também podem ser úteis para satisfazer requisitos de segurança. A utilização de padrões de segurança para elaboração de processos de software confiáveis tem como objetivo reusar experiências bem-sucedidas para desenvolvimento de software seguro, facilitando a adaptação de processos. Nessa dissertação, padrões são usados para implementar requisitos de segurança do sistema.

Padrões geralmente são organizados no seguinte formato (ROSADO, 2006):

i) Objetivo: Ele descreve o que o padrão faz, qual a sua lógica e seu objetivo.

ii) Contexto: Descreve o contexto do problema.

iii) Problema: Explica qual problema esse padrão resolve.

iv) Descrição: Um cenário que ilustra o problema de *design*.

v) Solução: Indica como resolver o problema.

vi) Consequências: Descreve os resultados da utilização do padrão.

vii) Conhecimentos utilizados: Exemplos de padrões encontrados em sistemas reais viii) Padrões relacionados: Lista de outros padrões relacionados que utilizam este padrão como referência.

Padrões são úteis para desenvolvedores e arquitetos pois (TROWBRICGE, 2003):

- Documentam mecanismos simples que funcionam.
- Fornecem vocabulário e taxonomia comum para desenvolvedores e arquitetos.
- Permitem que soluções sejam descritas resumidamente através da combinações de padrões.
- Permitem o reuso da arquitetura, do design e de decisões de implementações.

4.1. Principais autores de Padrões de Segurança

Alguns autores destacam-se pela criação de padrões de segurança. Nestas subsecções serão apresentados alguns destes autores.

Padrões de segurança representam uma forma de sintetizar o conhecimento acumulado sobre o design de sistemas de segurança. Os padrões de segurança também são destinados a ser utilizados e compreendidos por desenvolvedores que não são profissionais de segurança (ROSADO et al., 2006).

4.1.1 Schumacher

Schumacher et al. (2005) em seu livro "*Security Patterns*" destacam-se dentre os demais autores. Citações a respeito deste livro são constantes em trabalhos e artigos sendo publicados atualmente (KROLL et al., 2010), (BRAZ, 2009), (WASSERMANN, 2004).

Padrões comprovaram seu sucesso em várias áreas do desenvolvimento do software. Algumas vantagens da utilização de padrões de segurança são (SCHUMACHER et al., 2006):

- Padrões codificam basicamente conhecimentos de segurança em um caminho estruturado e compreensível.
- A representação dos padrões é familiar para os desenvolvedores de software e engenheiros de sistemas.
- Padrões são utilizados para capturar conhecimentos em organizações. A utilização de padrões para capturar conhecimentos de segurança auxilia na integração dos sistemas a empresa.
- O foco da segurança na implementação de muitos sistemas é em baixo nível. Um foco de padrões de segurança é a garantia de alto nível de arquitetura e garantias à empresa. A utilização de uma abordagem padrão em todos os níveis, ajuda na integração de altos e baixos níveis.

Como exemplo de padrões de segurança propostos por Schumaher et al. (2006) pode-se citar o *Threat Assesment*, *Controlled Process Creator, Access Control Requirements, Role Rights Definition, Role-Based Access Control, Risk Determination, Vulnerability Assessment*.

4.1.2 Rosado

O autor Rosado (2006) é conhecido como um dos principais autores de padrões de segurança e diz que padrões de segurança são propostos como um meio de diminuir a lacuna entre desenvolvedores e especialistas em segurança.

Alguns dos padrões apresentados pelo autor são (ROSADO, 2006): *Authorization Pattern, RBAC, Multilevel Pattern, Reference Monitor Pattern, Virtual Address Space, Access Control, Execution Domain Pattern, SAP Pattern, Check Point Pattern*.

4.1.3 Romanoski

Uma boa estratégia de segurança requer primeiramente um alto nível de reconhecimento dos princípios gerais de segurança. Eles são demonstrações simples,

geralmente preparadas pelo chefe do escritório de informações que endereça conceitos gerais de segurança. Após, políticas de segurança são criadas por profissionais de segurança. Políticas de segurança destinam-se a tratar de problemas relacionados à execução de requisitos de segurança em negócios (ROMANOSKY, 2002).

Uma vez que as políticas gerais são definidas, os padrões de segurança podem ajudar a identificar e formular práticas e procedimentos de segurança que são relevantes para um ambiente empresarial (ROMANOSKY, 2002).

Os padrões de segurança definidos por este autor são explicados através de um alias, da motivação, do problema, das forças, da solução, de consequências, de conhecimentos utilizados e de padrões relacionados. Alguns dos padrões definidos por Romanosky são: *Authoritative Source of Data*, *Risk Assessment and Management*, *Enterprise Partner Communication*, *The Security Provider*. Conceitos e explicações a respeito dos padrões citados e outros padrões podem ser obtidos através de (ROMANOSKY, 2003).

4.1.4 Trowbridge

As melhores soluções são aquelas compostas por uma série de mecanismos pequenos e simples que resolvem problemas com segurança e efetividade. Durante o processo de construção de grandes e complexos sistemas, estes mecanismos simples combinam e envolvem um grande sistema. Conhecimentos a respeito destes mecanismos simples não vêm facilmente. Estes geralmente estão em mentes de experientes desenvolvedores e arquitetos e são partes importantes do conhecimento tácito que é trazido para o projeto (TROWBRIDGE, 2003).

Este autor divide os padrões de segurança em: Padrões para a *Web*, padrões para sistemas distribuídos, padrões de desenvolvimento, padrões de organização.

4.1.5 Kienzle

Há uma grande desconexão entre os profissionais de segurança e desenvolvedores de sistema. Profissionais de segurança estão preocupados principalmente com a segurança do sistema, enquanto desenvolvedores estão preocupados principalmente em construir um sistema que funcione. Enquanto segurança está entre as metas de requisitos não-funcionais que desenvolvedores precisam estar preocupados, este é apenas um de muitos. E enquanto profissionais de segurança queixam-se que desenvolvedores não levam a segurança a sério, desenvolvedores estão frustrados com profissionais de segurança que não entendem que segurança não é sua única preocupação (KIEZLE, 2002).

Padrões de segurança são propostos com o sentido de criar uma ponte nesta lacuna. Padrões de segurança são projetados para capturar soluções para problemas de segurança. Padrões de segurança também são desenvolvidos no sentido de serem utilizados e entendidos por desenvolvedores que não são profissionais de segurança. Enquanto sua ênfase está na segurança, estes padrões capturam os pontos fortes e deficiências de cada abordagem diferente, com o intuito de permitir que desenvolvedores tomem decisões a respeito da segurança e outras metas a serem atingidas (KIEZLE, 2002).

A forma de apresentação de padrões de segurança deste autor consiste basicamente na forma de apresentação dos autores citados anteriormente.

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

Padrões de segurança podem ser usados para implementar normas, uma vez que são descritos mais detalhadamente. Esta seção apresenta um artigo publicado no SBSI em 2010, intitulado “Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008” por Kroll et al. (2010) e que está

diretamente relacionado a esta dissertação. Este artigo apresenta 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.

Este artigo (KROLL et al., 2010) faz associação dos padrões às PAs. Essa associação originou as regras sugeridas pela ferramenta, porém no artigo não é tratada a questão da adaptação dos processos mas sim da dinamicidade entre os projetos da empresa.

4.2.1 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:

Tabela 4.1 – PA's relacionadas à padrões de segurança.

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);
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.

5. METODOLOGIA PARA ADAPTAÇÃO DE PROCESSOS DE SOFTWARE CONFIÁVEIS

Este capítulo descreve a metodologia proposta para adaptação de processos seguros. Essa metodologia utiliza como base o *framework* PRiMA-F, construído a partir do *Rational Unified Process* e de regras de associação de padrões de processo e organizacionais aos riscos identificados e mensurados para o projeto. Nesse trabalho é proposto uma extensão de PRiMA-F, chamado de SMT-*Framework*, para adaptar o processo com base nas áreas de processo do SSE-CMM, ao invés de riscos de projeto. Outra diferença é que no PRiMA-F são utilizados padrões de processo e organizacionais e no SMT-*Framework* são utilizados padrões de segurança. Os processos obtidos a partir do *framework* estendido visam o desenvolvimento de software confiável.

5.1 PRiMA (*Project Risk Management Approach*)

PRiMA consiste em uma abordagem sistemática para gerencia de riscos em projetos de software. Tem como objetivo permitir a elaboração de um processo específico para um dado projeto, visando minimizar a exposição do projeto aos riscos, identificados e mensurados de acordo com o contexto do projeto.

A adaptação de processos em PRiMA é baseada em um *framework* PRiMA-F que foi definido segundo o metamodelo PRiMA-M (FONTOURA, 2006). O PRiMA-M representa os conceitos usados na definição de processos de software, isto é, a partir dos conceitos descritos no metamodelo são instanciados elementos de processo (atividades, papéis, artefatos, ferramentas, etc.) que são usados na construção de modelos de processo. O metamodelo define a linguagem para expressar processos de software; descreve os conceitos e suas relações com a finalidade de construir e interpretar modelos de processo (FONTOURA, 2006).

5.2 Metodologia SMT

Para agregar segurança a um processo de software este trabalho propõe uma metodologia de adaptação de processos de software. Esta tem por objetivo permitir a elaboração de um processo de desenvolvimento de software para um projeto específico, considerando práticas de segurança descritas no SSE-CMM.

A adaptação de processos, neste trabalho, considera que existe um processo padrão da organização (PSPO) que descreve os elementos de processo que devem existir em todos os projetos da organização, e consiste em alterá-lo para satisfazer as necessidades do projeto, especialmente em relação à segurança e tem como resultado o processo específico para o projeto (PEP). A Figura 5.1 apresenta a metodologia proposta.

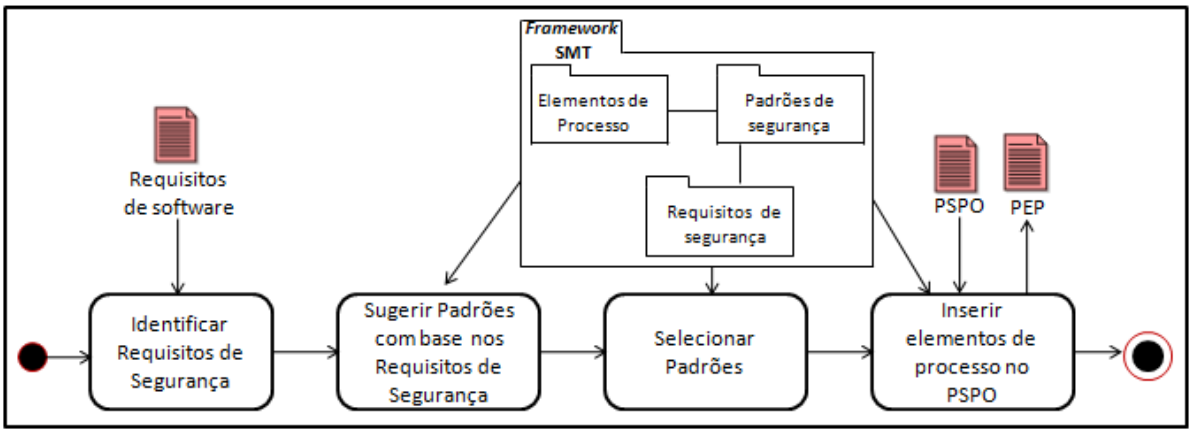


Figura 5.1 – Metodologia para Adaptação de Processos de Software Confiáveis

Com base nos requisitos de segurança identificados para o projeto, o engenheiro de segurança, auxiliado pelo gerente do projeto, seleciona um conjunto de áreas de processo do SSE-CMM que devem ser incorporadas ao projeto. Nessa seleção, além dos requisitos de segurança definidos para o projeto, deve ser considerada a opinião de especialidades e dos *stakeholders*.

Com base nas regras de associação definidas no *framework SMT*, são selecionados os padrões que visam satisfazer as PAs selecionadas na etapa anterior. O engenheiro de processo seleciona da lista sugerida os padrões que deseja incorporar ao PSPO. Após selecionar os padrões de segurança, os elementos de processo associados à implementação destes são incorporados ao PSPO originando o PEP.

A seguir será explicado cada item da metodologia, iniciando pelos artefatos:

- **Requisitos de software:** Requisitos são propriedades desejáveis para um sistema de software. Um requisito pode ser mensurável (ex., tempo médio de atendimento de requisições), ou avaliado subjetivamente (ex., qualidade da documentação).

- **Processo de Software Padrão da Organização (PSPO):** Assume-se que cada organização desenvolvedora de software tenha um processo padrão que é seguido durante o desenvolvimento de um projeto de software. Este processo padrão é utilizado como base, para que nele sejam inclusos elementos de processos.

- **Processo Específico para o Projeto (PEP):** Após a inclusão dos elementos de processos propostos pelos padrões de segurança no PSPO, este passa a ser o Projeto Específico para o Projeto, pois possui características e elementos de processos definidos exclusivamente para o projeto em desenvolvimento.

As atividades presentes na metodologia são:

- **Identificar requisitos de segurança:** Através dos requisitos de software verificar quais são os requisitos de segurança que serão necessários para que o projeto em desenvolvimento possa ser considerado confiável.

A utilização de PA’s deu-se por estas possuírem uma lista de objetivos que indicam os resultados esperados após sua implementação e uma lista de BPs (*Base Practices*) que auxiliam no cumprimento dos objetivos. Considera-se neste trabalho que PA’s são requisitos de segurança.

- **Sugerir padrões com base nos requisitos de segurança**: A associação de PAs aos padrões se dá por meio de regras de associação. Como exemplo de regras elaboradas pode se

citar o uso dos padrões *Asset Valuation* (SCHUMACHER et al., 2006); *Threat Assessment* (SCHUMACHER et al., 2006); *Vulnerability Assessment* (SCHUMACHER et al., 2006) e *Risk Determination* (SCHUMACHER et al., 2006) para implementação da PA03 – Avaliação dos Riscos de Segurança.

Essa PA tem o propósito de identificar os riscos de segurança envolvidos com o sistema em um ambiente definido. Os riscos devem ser avaliados 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.

O padrão *Risk Determination* (SCHUMACHER et al., 2006) pode ser usado para determinação dos riscos de segurança. *Risk Determination* necessita de outros padrões que fornecem os dados necessários (ativos, ameaças e vulnerabilidades) para avaliação dos riscos, que são: padrão *Asset Valuation* (SCHUMACHER et al., 2006) auxilia na determinação da importância dos ativos da Organização, padrão *Threat Assessment* (SCHUMACHER et al., 2006) identifica as ameaças e sua probabilidade de ocorrência, e o padrão *Vulnerability Assessment* (SCHUMACHER et al., 2006) trata da identificação das vulnerabilidades que podem ser exploradas por ameaças. Desta forma, por meio da aplicação destes quatro padrões os objetivos da PA03 são atendidos. A organização pode definir suas próprias regras de associação. As associações utilizadas neste trabalho são apresentadas na seção 4.2.1, Tabela 4.1.

As regras de associação de padrões a áreas de processo, bem como de elemento de processo a padrões são sugestões, elaboradas por meio da literatura e podem ser alteradas pela organização por meio de análises de projetos passados, sessões de retrospectivas, entre outros.

- **Selecionar padrões:** O gerente de segurança seleciona os padrões de segurança de acordo com a lista de padrões que foram previamente cadastrados na ferramenta.

- **Inserir elementos de processo no PSPO**: Os elementos de processos definidos no *framework* são incorporados ao processo de desenvolvimento de software padrão da organização.

5.2.1 *Framework* SMT

O *framework* (Figura 5.2) visa auxiliar na execução da metodologia através de um pré cadastro que é realizado na ferramenta de elementos de processo, padrões de segurança e requisitos de segurança.

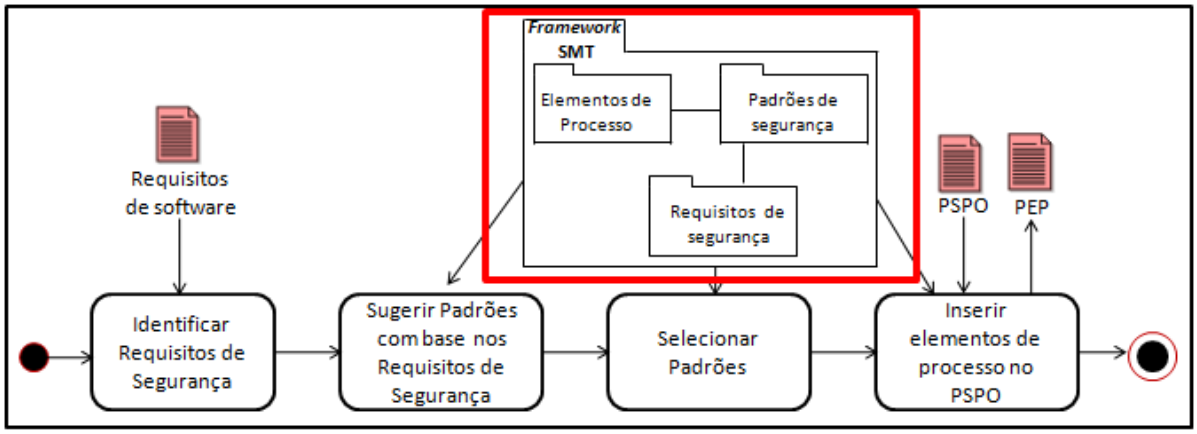


Figura 5.2 Destaque para o *framework* no contexto da metodologia

Os artefatos presentes no *framework* são:

- Elementos de Processo – Elementos de processos são necessários para a adaptação do processo uma vez que estes são os "blocos para construção" de novos processos e representação de padrões de segurança, definindo atividades, artefatos e papéis as tarefas.

- Padrões de Segurança - Padrões de segurança fornecem soluções efetivas para problemas recorrentes de segurança da informação.

- Requisitos de Segurança – Requisitos de segurança são, da mesma forma que requisitos de software, condições que devem ser englobadas no processo de desenvolvimento de software para que a segurança prevista seja alcançada.

O *framework* proposto para adaptação de processos foi construído a partir do *Rational Unified Process* e de regras de associação de padrões de segurança às áreas de processo do SSE-CMM. O diagrama UML da Figura 5.3 mostra as tarefas que devem ser seguidas para adaptação de processos.

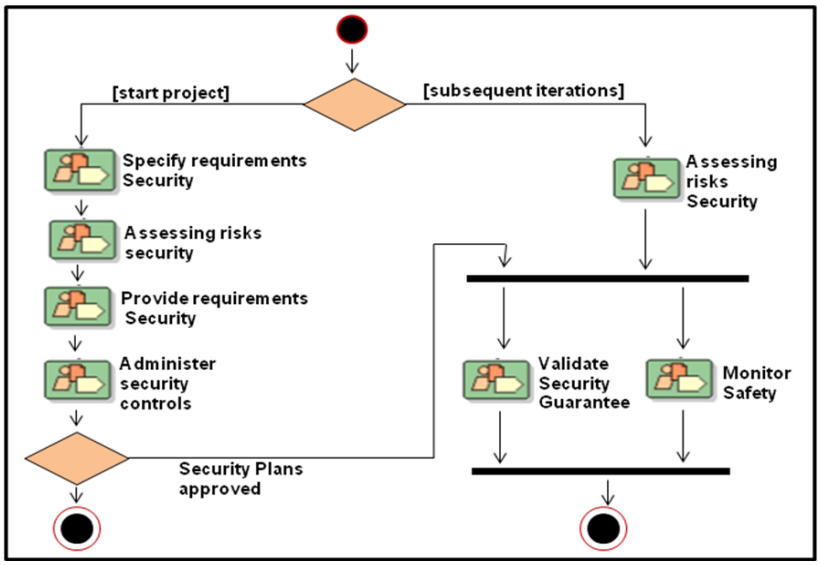


Figura 5.3 Detalhamento da disciplina de segurança

Considerando que, o Modelo SSE-CMM descreve várias recomendações que devem ser seguidas para o desenvolvimento de software seguro, e que bases de processos visam normalmente agrupar coleções de atividades relacionadas a uma área de concentração, identifica-se que a melhor solução é agrupar as atividades propostas para adicionar segurança em uma única disciplina de segurança.

No artigo "Extensão de um *framework* de processo para adaptação à segurança em aplicações Web" publicado por Wagner, Fontoura e Nunes, (2010) realizou-se uma incorporação de atividades relacionadas a segurança nas disciplinas já existentes no Processo Unificado, por exemplo, "Especificar Necessidades de Segurança" poderia ser incorporada a disciplina de Requisitos. Várias disciplinas teriam seus diagramas de atividades alterados, dificultando a compreensão e implementação do processo. Outra vantagem de se ter uma disciplina separada para tratar de questões de segurança é a facilidade que terão empresas que

desejam estender seus processos com base nesse trabalho. Essa disciplina foi elaborada de acordo com as orientações para adaptação do RUP (RUI, HAO, ZHIQING, 2009), e deverá ser executada em todas as fases, porém, com mais intensidade na fase de iniciação e elaboração. Essa disciplina é uma disciplina de suporte porque se preocupa com gerenciamento de segurança dentro do projeto.

5.3 Incorporação de Padrões ao *Framework SMT*

Para que padrões de segurança possam ser incorporados em processos de software é necessário que eles estejam descritos por meio de conceitos que serão usados na modelagem dos processos. Metamodelos são utilizados para descrever elementos que podem ser usados para a elaboração de modelos. No caso deste trabalho optou-se por utilizar o metamodelo PRiMA-M (*Project Risk Management Approach – Metamodel*) elaborado (FONTOURA, 2006). PRiMA-M representa um conjunto de conceitos que são usados na modelagem de processos de software. Elementos de processo, instanciados a partir de PRiMA-M, podem ser usados na definição de processos planejados, ágeis ou híbridos. A Figura 5.4 mostra os elementos que compõem o PRiMA-M.

O *Ciclo de Vida* de um processo é uma agregação de *Fases*, que por sua vez são associadas a *Atividades*. Uma *Disciplina* identifica um conjunto de *Papéis* que participa na *Disciplina* e define um conjunto de *Atividades* que compõem a disciplina. Uma *Atividade* especifica uma colaboração específica dentro de uma *Disciplina* e representam agrupamento de *Tarefas*, sendo que um *Papel* é responsável por cada *Tarefa*. *Artefatos* são produtos gerados durante a execução de *Tarefas*, e podem ser modelos, planos, versões do software, relatórios, etc. *Papéis* representam os cargos executados por indivíduos em um projeto. *Ferramentas* são usadas para auxiliar a realização de atividades. *Mentores de Ferramentas* descrevem como executar uma *Tarefa*, usando determinada *Ferramenta*.

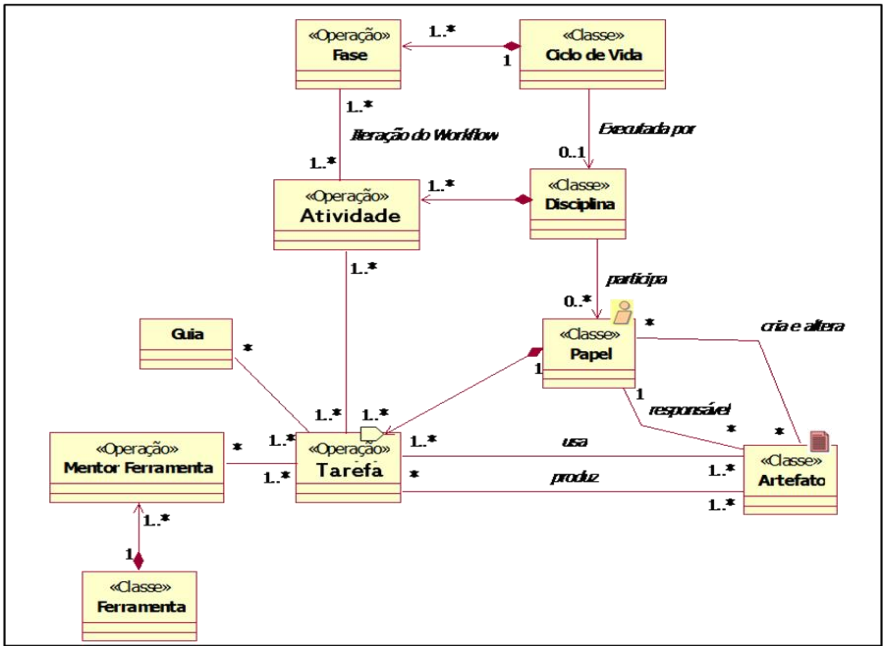


Figura 5.4 – PRiMA – Metamodelo adaptado de (FONTOURA, 2006)

PRiMA–M foi adaptado para que fosse possível compatibilizar com a versão 7 do RUP. Alterações foram realizadas nos nomes das classes. Na versão 7 do RUP o "*Workflow Detail*" passou a ser chamado de "Atividade" e "Atividade" passou a ser chamada de "Tarefa".

Para exemplificar como padrões de segurança podem ser descritos por meio de elementos de processo, instanciados a partir do PRiMA, na Figura 5.5 são descritos os elementos necessários à implantação do padrão *Asset Valuation*.

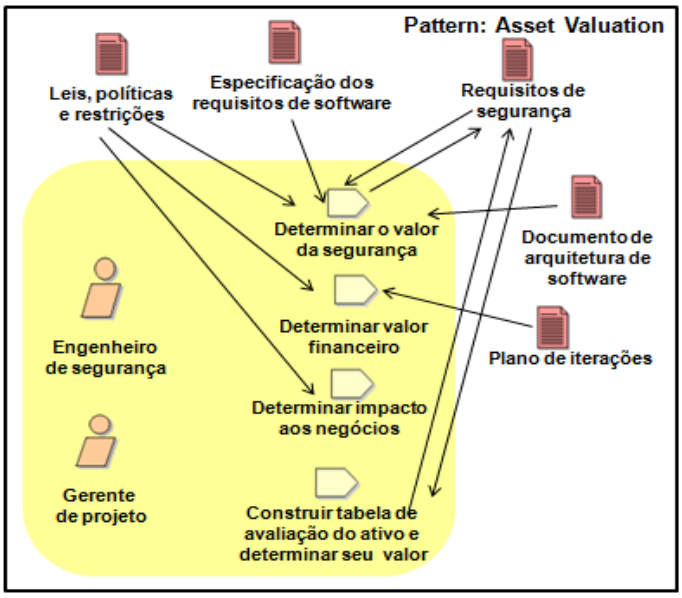


Figura 5.5 - Padrão *Asset Valuation*

Considerando que o padrão *Asset Valuation* ajuda a determinar a importância global dos ativos que a empresa detém e controla, e avaliar o impacto que perdas de ativos podem resultar em prejuízos financeiros é necessário incluir as seguintes tarefas no processo para implantar esse padrão:

- *Determinar o valor da segurança*, que tem como objetivo determinar o valor da segurança do ativo com base na importância dada pela empresa em garantir os requisitos de segurança da informação confidencialidade, integridade, disponibilidade e responsabilidade.
- *Determinar o valor financeiro* do ativo para a empresa com base no custo de reparar ou substituir como também o custo para manter e operar o ativo.
- *Determinar impacto aos negócios* tem como objetivo determinar o valor do ativo em relação ao impacto que o ativo pode ter em relação aos processos de negócio da organização.
- *Construir tabela de avaliação do ativo e determinar seu valor*, tem como objetivo combinar os resultados das avaliações de valor de segurança, valor financeiro e impacto de negócio em uma tabela de avaliação do ativo.

O engenheiro de segurança executa essas tarefas auxiliado pelo gerente de projeto. O principal artefato elaborado durante essas atividades é o documento *Requisitos de Segurança*

que descreve os ativos, juntamente com o valor de segurança, o valor financeiro e o impacto que o ativo pode ter no negócio, bem como as tabelas de avaliação elaboradas.

No RUP, um diagrama de atividade é proposto para cada disciplina para organizar as atividades possíveis de serem executadas nos processos de software instanciados a partir deste. As atividades propostas para implantação de padrões foram incluídas nos diagramas de atividades existentes no RUP, identificando-se desta forma, a sequência de execução das mesmas.

Cada *atividade*, proposta para implementação de padrões, foi analisada para definir a seqüência de execução da atividade. Essa seqüência foi definida a partir de uma análise de artefatos necessários à execução de atividade e de artefatos gerados por atividades. As atividades seqüenciadas foram organizadas em diagramas de atividades, por disciplina.

A fim de exemplificação demonstra-se aqui apenas um padrão, porém os demais associados às áreas de processo podem ser visualizados no anexo B.

A Figura 5.6 é especificada a base de conhecimento utilizada pelo *framework*. Através das tabelas é possível verificar a integração dos dados. A base de conhecimento inclui informações da ferramenta PMT-Tool, PRiMA –Tool e SMT- Tool (que serão explicadas no próximo capítulo). As tabelas específicas da ferramenta SMT estão destacadas, e correspondem a:

- *processarea_sse*: cadastro das 11 áreas de processo relacionadas a segurança do SSE-CMM.
- *projectpa*: cadastro dos projetos relacionados as áreas de processo.
- *selectionrulesprocessarea*: cadastro da associação dos padrões às áreas de processo.

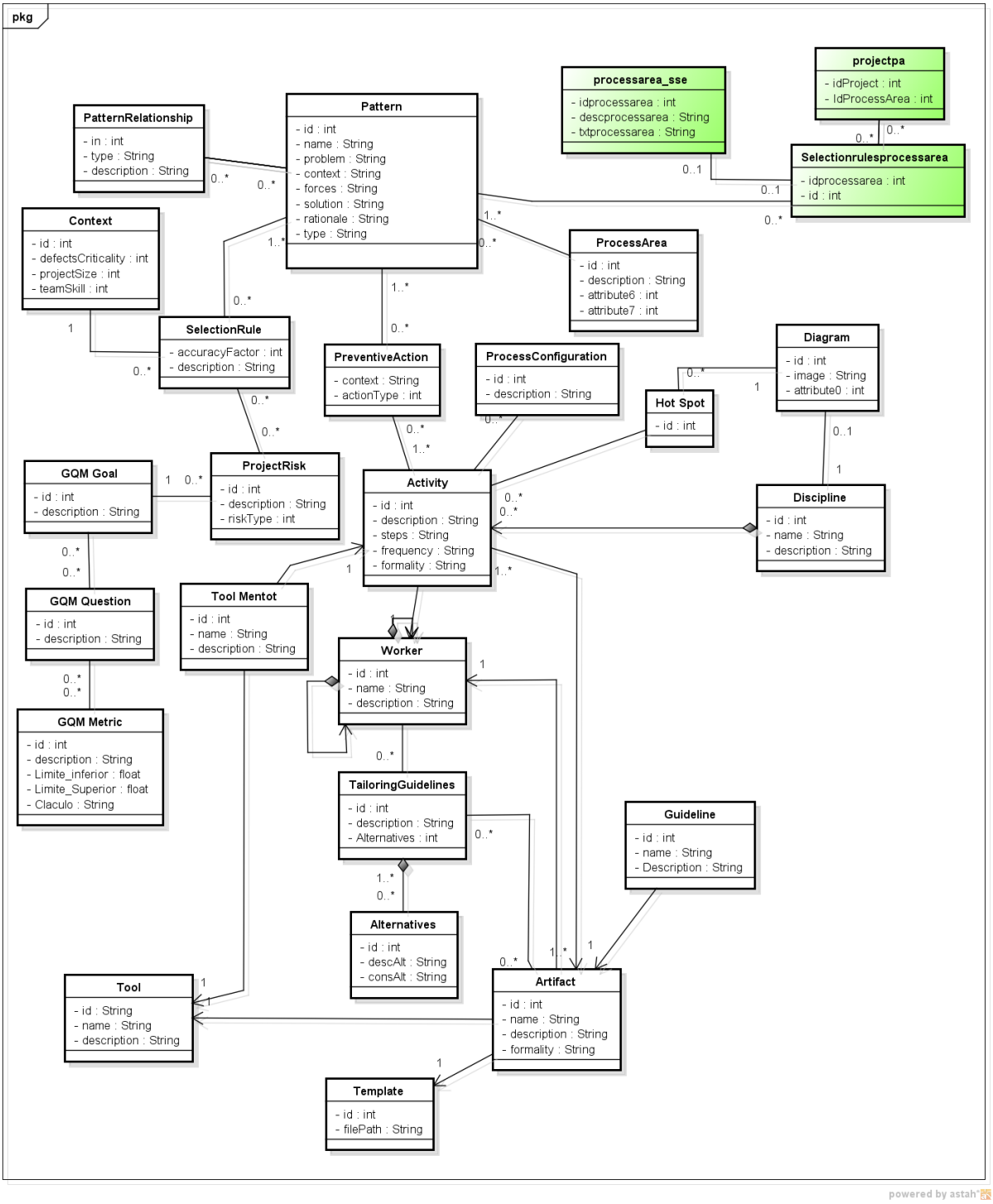


Figura 5.6 - Base de conhecimento

6. SMT – TOOL AMBIENTE EXPERIMENTAL PARA ADAPTAÇÃO DE PROCESSOS DE SEGURANÇA EM PROJETOS

Um ambiente experimental para adaptação de processos com base em requisitos de segurança é composto pelas ferramentas: *Security based Methodology Tailoring* (SMT-Tool), *Project Risk Management Approach* (PRIMA-Tool) e *Pattern-Based Methodology Tailoring* (PMT-Tool). PMT-Tool é responsável pela catalogação de padrões de segurança. O módulo PRiMA-Tool é responsável pela elaboração do processo de projeto de software, desde a adaptação dos processos padrões da organização inseridos nos padrões selecionados para a prevenção de riscos em projetos até a elaboração do Website, onde constam as atividades que devem ser realizadas na execução da adaptação. A partir de tais ferramentas sentiu-se a necessidade de extensão destas para contemplar segurança, o que gerou a ferramenta SMT-Tool, correspondente ao PRiMA adaptado à segurança. A extensão utilizou vários dos recursos que já estavam disponíveis na *suíte*. As metas de segurança inseridas na ferramenta SMT-Tool foram baseadas no modelo SSE-CMM.

6.1. PRIMA – TOOL

A ferramenta PRiMA foi criada com a intenção de gerenciar riscos em projetos de software, o pode ser uma tarefa complexa e trabalhosa em qualquer organização se executada de maneira manual. Por isso, é desejável a implementação de um ambiente que apóie a adaptação do processo da organização e a gerência de riscos. Tal implementação tem como finalidade possibilitar uma experimentação prática do uso da abordagem proposta (FONTOURA, 2006). A adaptação de processos existente no PRiMA, foi amplamente utilizada para o desenvolvimento da SMT.

O ambiente experimental elaborado é composto por dois módulos principais, que são: *Pattern-based Methodology Tailoring* (PMT-Tool) e *Project Risk Management Approach* (PRiMA-Tool).

O módulo *Pattern-based Methodology Tailoring* (PMT-Tool) (HARTMANN, 2005) foi desenvolvido por Júlio Hartmann, como dissertação de mestrado. PMT é responsável por catalogar os padrões de processo e associá-los aos riscos de software por meio de regras, bem como selecionar os padrões para prevenir riscos priorizados para determinado projeto. Maiores informações sobre PMT podem ser obtidas em (HARTMANN, 2005).

O módulo *Project Risk Management Approach* (PRiMA-Tool) foi desenvolvido por Lisandra Manzoni Fontoura como parte da tese de doutorado (FONTOURA, 2006).

6.2. SMT – Tool

Essa ferramenta foi desenvolvida com o objetivo de apoiar o desenvolvimento da metodologia proposta no capítulo anterior.

A Figura 6.1 mostra a tela principal da SMT-Tool. No menu à esquerda são exibidas as funcionalidades da ferramenta.

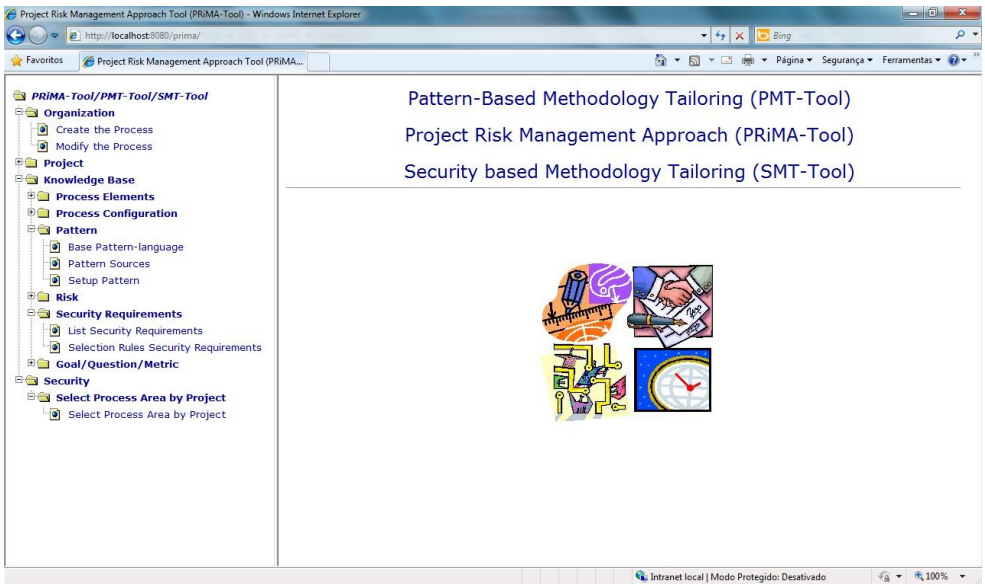


Figura 6.1 - Formulário Principal da *Suíte*

Para que a ferramenta possa auxiliar no processo de adaptação de processos, é necessário que alguns dados sejam previamente cadastrados. A seguir as atividades que devem ser realizadas são detalhadas.

As atividades que devem ser seguidas para configurar a ferramenta SMT-Tool são:

- Criação da organização ao qual serão adicionadas os projetos a serem adaptados;

- Criação do projeto;

- Criação dos elementos de processo: a disciplina, os papéis, os artefatos e as atividades;

- Cadastro de padrões;

- Seleção de atividades necessárias para implementar os padrões;

- Cadastro de requisitos de segurança;

- Cadastro das regras de associação de requisitos de segurança a padrões;

- Seleção de requisitos de segurança para um projeto específico;

- Realização da adaptação do processo: seleção da organização e da base de processo;

- Elaboração do *Website* para a visualização das atividades necessárias para adaptação do processo.

Os passos para a configuração da ferramenta estão descritos acima, a seguir serão demonstradas as respectivas imagens.

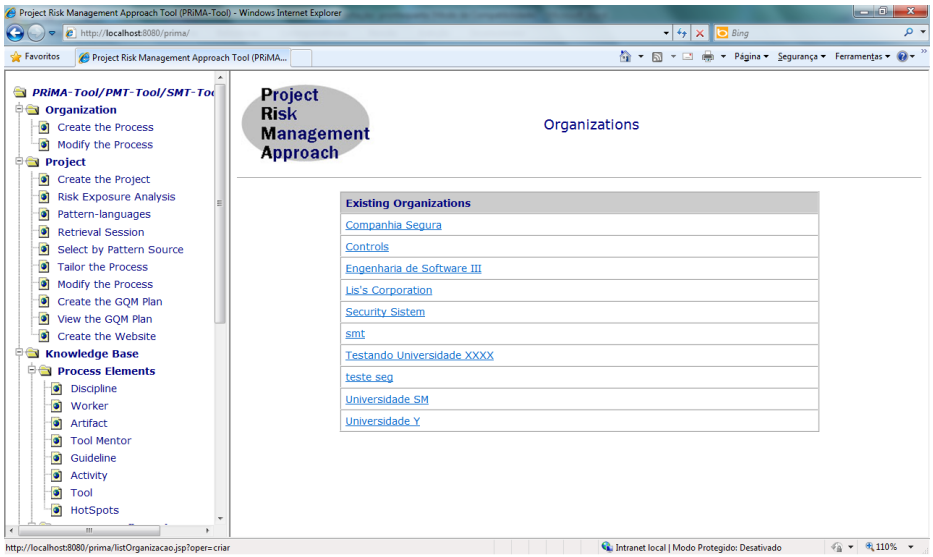


Figura 6.2 – Formulário para cadastro do processo padrão da organização

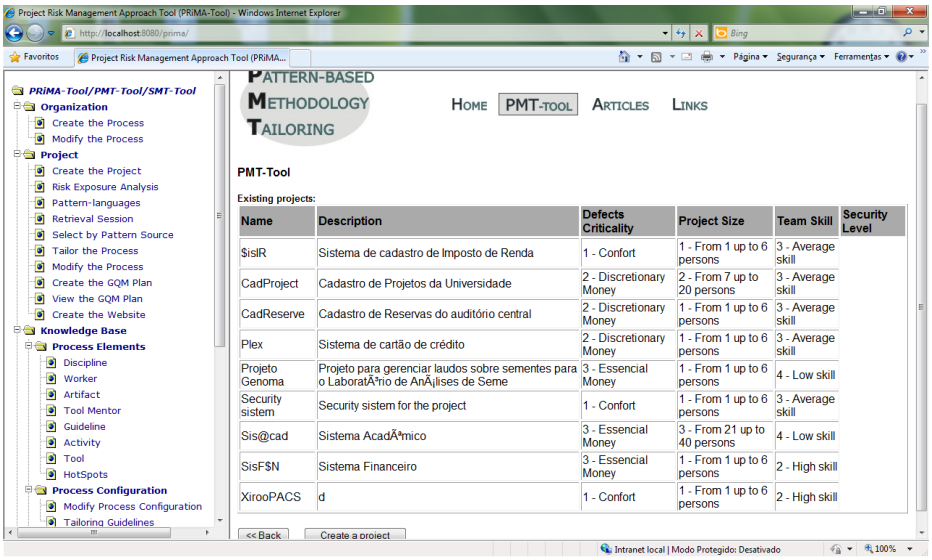


Figura 6.3 - Formulário de cadastro do projeto.

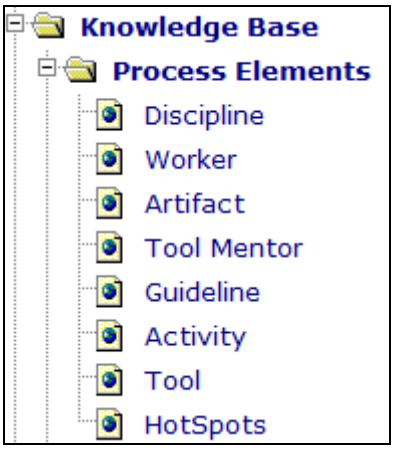


Figura 6.4. - Atalho de acesso aos elementos de processos.

A Figura 6.4 demonstra os elementos de processo que precisam ser cadastrados para que seja possível a adaptação de processos. Esse é um modulo da ferramenta PRiMA – Tool e para a ferramenta SMT – Tool precisam ser cadastrados apenas a *discipline*, o *worker*, os *artifacts* e as *activities*.

O cadastro de padrões é realizado na ferramenta PMT – Tool, conforme Figura 6.5.

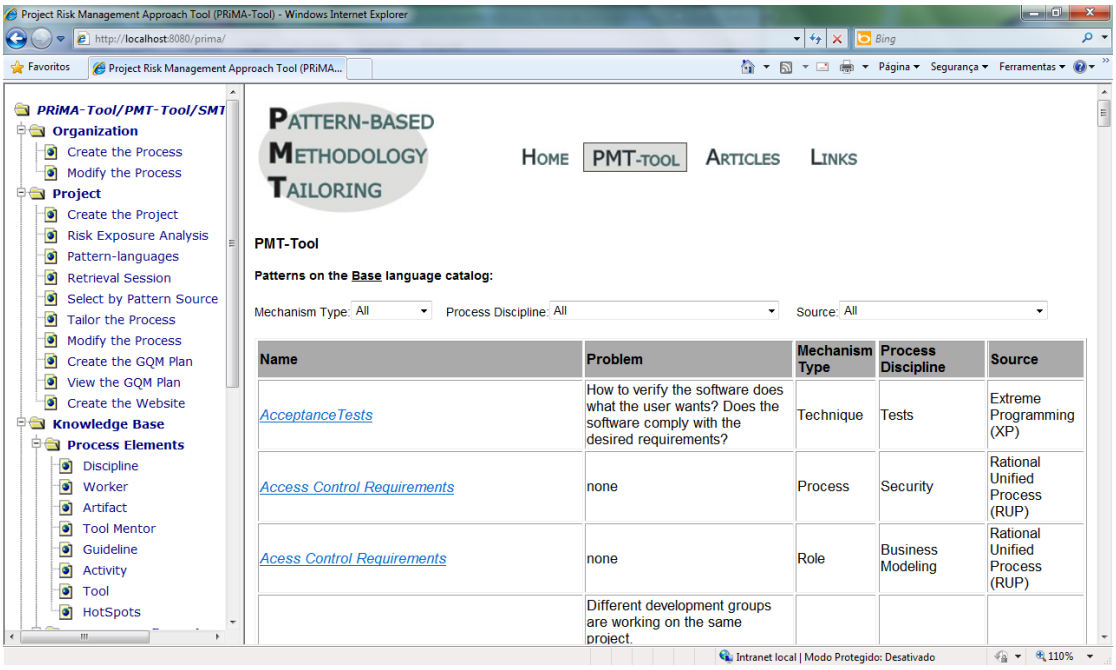


Figura 6.5 - Formulário para cadastro de padrões

O cadastro de requisitos de segurança é específico do SMT –Tool, uma vez que este é o modulo responsável pela segurança. O formulário está demonstrado na Figura 6.6.

Figura 6.6 - Formulário para cadastro dos Requisitos de Segurança

A definição das regras é realizada através do ícone "*Security Requirement*", que está dividido em dois sub-itens, "*List Security Requirement*", onde é possível cadastrar, editar e deletar requisitos de segurança, e "*Selection Rules Security Requirement*", onde são cadastradas as regras de associação de requisitos de segurança à padrões. A Figura 6.7 mostra o formulário para associação.

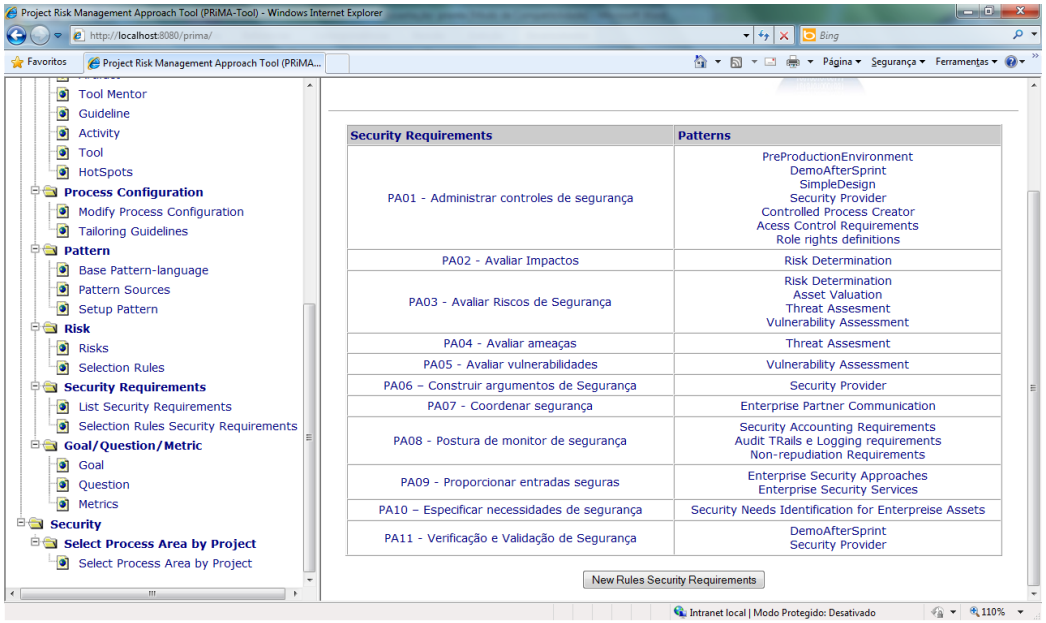


Figura 6.7 - Formulário para associação de requisitos de segurança a padrões.

Através do item "*Security*" – "*Select Process Area by Project*" é possível que o projeto em desenvolvimento seja associado as áreas de processo ou requisitos de segurança que foram cadastrado anteriormente.

Conforme a Figura 6.8 o usuário seleciona o projeto em desenvolvimento.

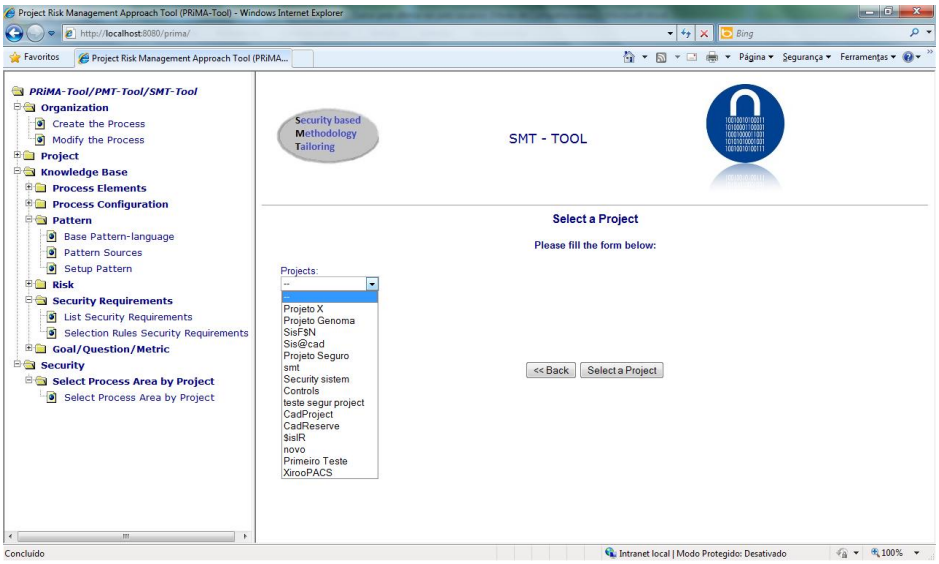


Figura 6.8 - Formulário de seleção do projeto para o qual será criado o processo

Após selecionar o projeto, o usuário deverá selecionar as PA's que devem ser inclusas para garantir a segurança esperada para o projeto. Conforme Figura 6.9.

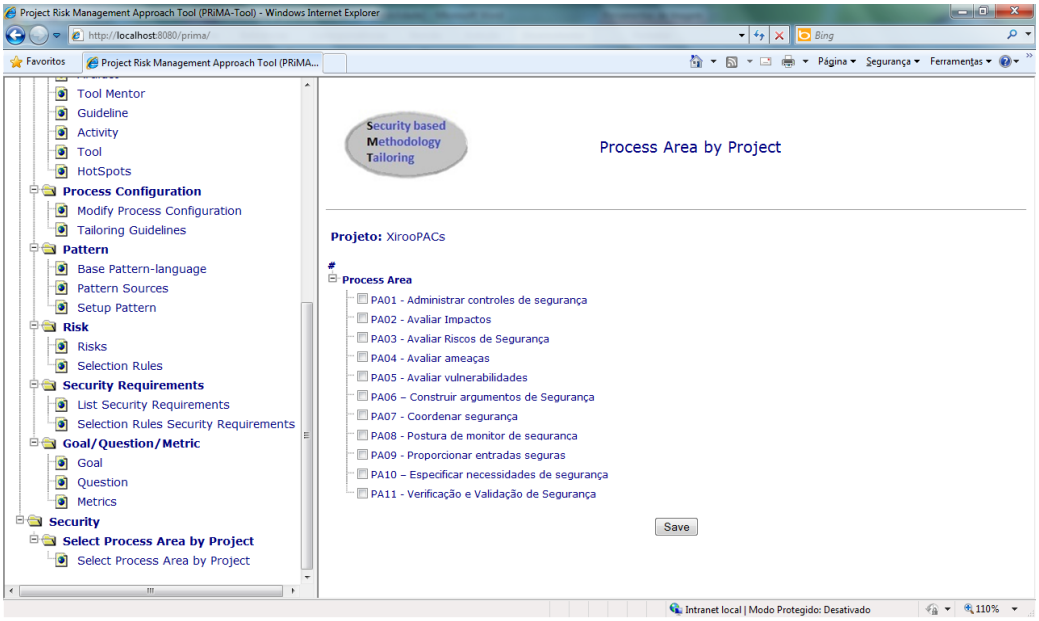


Figura 6.9 - Formulário de seleção das PA's que serão associadas ao projeto.

Após selecionadas as áreas de processo o usuário clica no botão “*Save*” e o sistema SMT direciona o processo para a ferramenta PMT, que vai apresentar os padrões de acordo com as PA’s selecionadas e as associações realizadas entre padrões e PA’s.

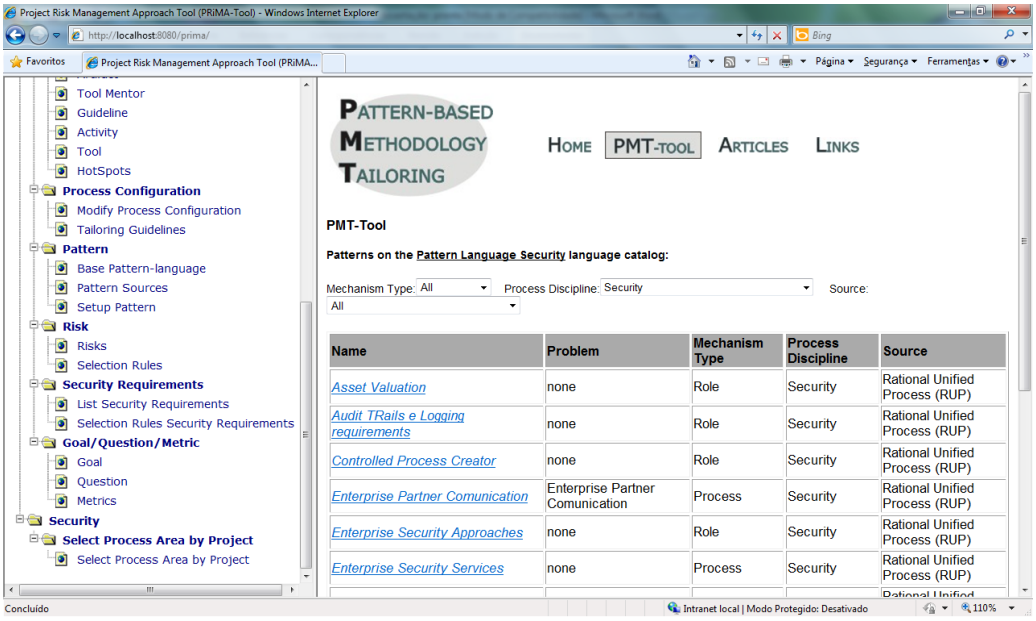


Figura 6.10 - Formulário com a lista de padrões selecionados para o projeto.

Para que seja possível realizar a adaptação do processo é necessário que o usuário acesse a opção “*Tailor the Process*” no menu de opções. Neste momento o usuário vai selecionar novamente o projeto no qual está trabalhando. A adaptação é responsável por inserir no processo padrão da organização os elementos de processo que implementam os padrões selecionados.

O próximo passo consiste em selecionar o processo da organização e a base de processos que serão utilizadas na adaptação dos processos.

Base de processos consiste no modelo que a organização utiliza para desenvolvimento dos seus projetos. Na SMT-Tool é possível cadastrar base de processos conforme necessário.

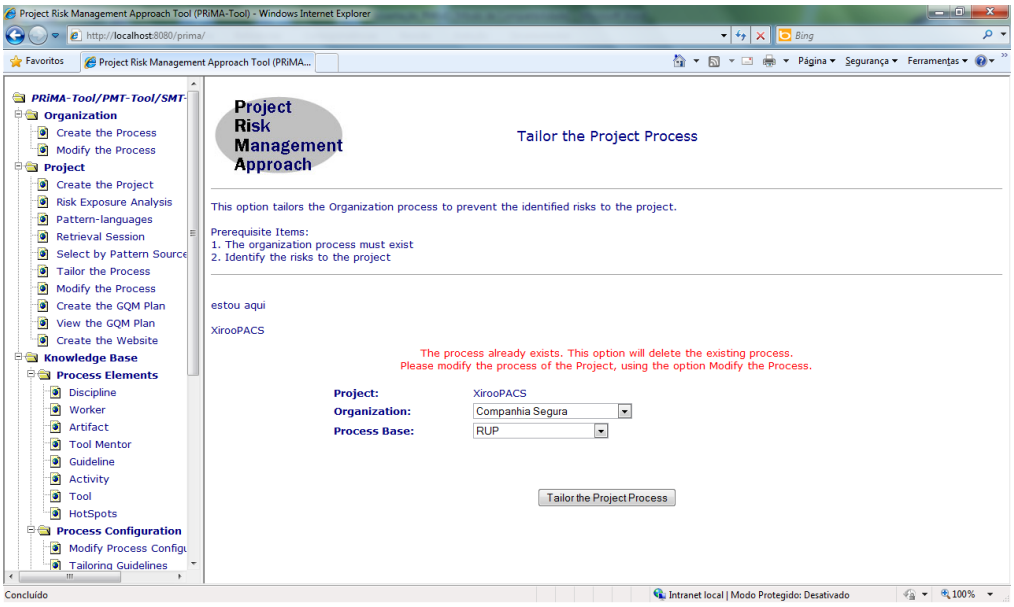


Figura 6.11 - Formulário de seleção para adaptação de processos.

O usuário irá visualizar as atividades que serão necessárias para que o projeto seja adaptado contemplando segurança para o projeto, conforme Figura 6.12. Após verificar as atividades o usuário deve clicar em “Save”, onde irá salvar as configurações determinadas para aquele projeto.

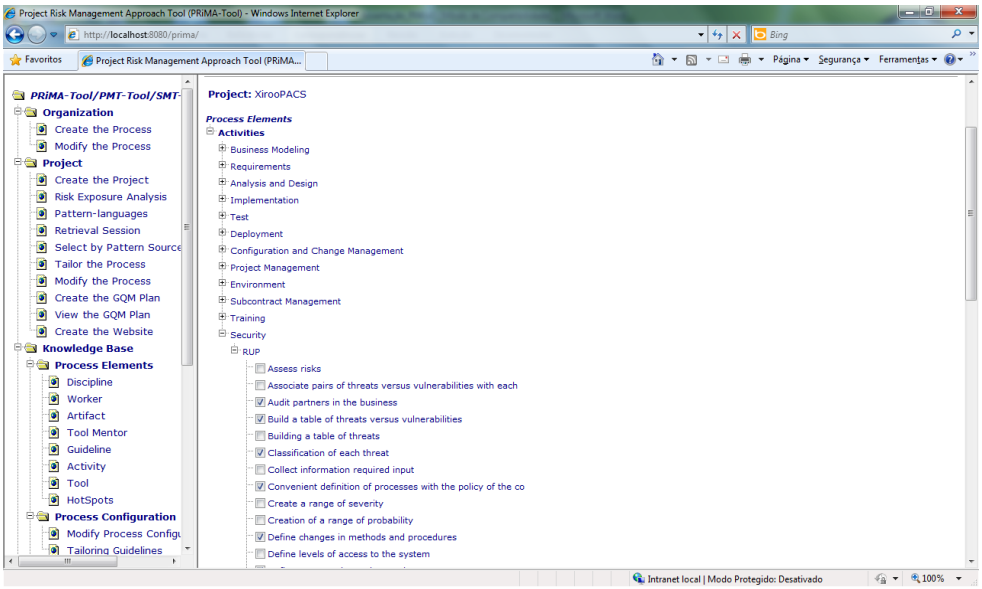


Figura 6.12 - Formulário de seleção de atividades para adaptação de processos confiáveis.

O último passo é a visualização da adaptação que deve ser realizada no projeto. O usuário deve gerar o *Website* através "*Create the Website*" .

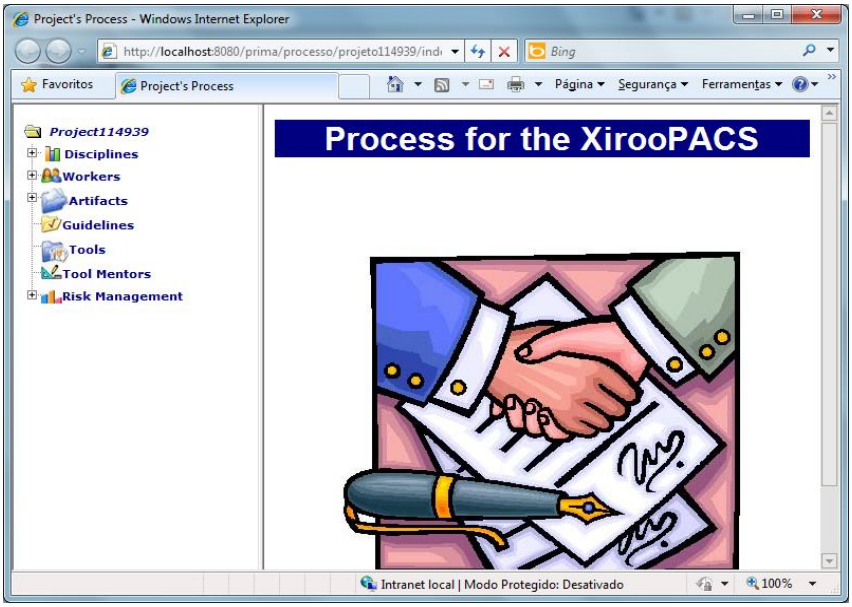


Figura 6.13 - Tela inicial do *Website*

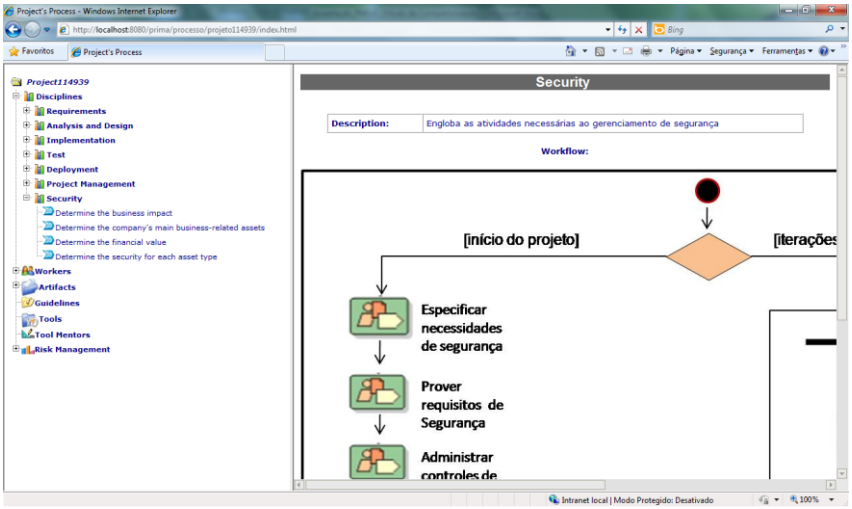


Figura 6.14 – Diagrama de atividades com atividades propostas para segurança.

7. ESTUDOS DE CASO

Este capítulo descreve dois estudos de caso realizados para validar a sistemática apresentada. Os estudos de caso foram realizados com o auxílio das ferramentas apresentadas no capítulo anterior.

Cada um dos estudos de caso foi realizado em um sistema e empresa diferente. Um dos sistemas selecionados possibilita a consulta e visualização de exames pelo médico e pelo paciente. O outro sistema selecionado é uma administradora de cartões de crédito. A partir das características básicas destes sistemas é possível perceber que o nível de segurança demandado é alto, motivo pelo qual foram selecionados para realização dos estudos de caso desta dissertação.

7.1 Metodologia do Estudo de Caso

Para o desenvolvimento dos sistemas propostos nestes estudos de caso o gerente do projeto, juntamente com o engenheiro de segurança realizaram um levantamento da priorização e quantificação dos requisitos de segurança (áreas de processo) propostos pelo Modelo SSE-CMM. Um questionário contendo todas as especificações necessárias para o entendimento das áreas de processo foi aplicado. O modelo do questionário está no Anexo C deste trabalho. Os níveis de relevância apresentados foram: altíssimo, alto, médio, baixo e não relevante. O gerente de projeto atribuiu um nível a cada um dos requisitos de segurança apresentados.

Após a realização do nivelamento (nível importância para o projeto – baixo, média, alta e altíssima) das áreas de processo pelo engenheiro de segurança e sua equipe realizou-se, previamente em Kroll et al. (2010), a associação de padrões necessários (as regras já estavam cadastradas no banco de dados) para a implantação de cada uma das áreas de processo. Os

padrões selecionados estão apresentados na Tabela 4.1. Estes padrões visam satisfazer a implementação da segurança das áreas de processo selecionadas.

7.2 Estudo de Caso I – XirooPACS

O primeiro estudo de caso se refere ao desenvolvimento do sistema XirooPACS desenvolvido na empresa Animati. A Animati Computação Aplicada é uma empresa brasileira que atualmente está instalada na Incubadora Tecnológica da UFSM e desenvolve software para área médica. Jean Carlo Albierto Berni é o gerente de projetos que foi o responsável pelas informações repassadas e por responder o questionário.

7.2.1 Descrição do Sistema

O sistema Xiroo PACS é um Sistema de Arquivamento e Comunicação de Imagens Médicas. Neste sistema radiologistas têm à sua disposição ferramentas de organização de exames. É possível marcar os exames que já foram laudados, ou criar rótulos personalizados para separar exames por categorias, ou também destacar aqueles que podem servir como casos de estudo. Casos de estudos são exames selecionados para realização de alguma análise ou estudo referente a aquela situação/doença.

Agendamento de exames, cadastro de pacientes e entrega de laudos pela internet a pacientes e médicos solicitantes são as características principais deste sistema.

A análise do sistema foi realizada considerando principalmente a questão de visualização de exames no sistema Web por pacientes e médicos, o que faz com que este sistema necessite de um alto índice de segurança.

7.2.2 Priorização das Áreas de Processo

A importância atribuída a cada área de processo pelo gerente do projeto juntamente com sua equipe foi:

Tabela 7.1 - Tabulação da importância associada a cada área de processo.

Áreas de Processo	**Importância para o Projeto**
PA01 – Administração dos controles de segurança	Alta
PA02 – Avaliação do Impacto	Alta
PA03 - Avaliação dos Riscos de segurança	Alta
PA04- Avaliação de Ameaças	Média
PA05- Avaliação de Vulnerabilidades	Média
PA06 – Construção de argumentos de garantia	Baixa
PA07 – Coordenação da segurança	Média
PA08 – Monitoração da postura da segurança	Média
PA09 – Fornecer a entrada segurança	Alta
PA10 – Especificar as necessidades de segurança	Altíssima
PA11 – Verificação e validação da segurança	Alta

Um acordo entre o engenheiro de processos e o gerente de segurança definiu que para o projeto em desenvolvimento seriam tratados as áreas de processo aos quais foi atribuído nível de relevância altíssimo ou alto.

7.2.3 Padrões Selecionados

Os padrões selecionados para cada uma das áreas de processos específicas foram:

Tabela 7.2 – Padrões associados as áreas de processo selecionadas.

Áreas de Processos	**Padrões de Segurança**
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* (SCHUMACHER et al. 2006); *Multilevel Security Pattern* (SCHUMACHER et al. 2006);
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);
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**	*Check Point Pattern* (ROSADO 2006); *Task Process Pattern* (AMBLER 1998); *Whitehat, Hack Thyself* (ROMANOSKY 2003);

Através do estudo detalhado de cada um destes padrões percebe-se que existe uma ligação entre vários deles, porém estes não descrevem soluções excludentes e sim soluções complementares. Alguns padrões dependem da implementação de outros, o que faz com que não sejam repetitivos.

7.2.4 Processo Específico para o Projeto

Um processo específico para o projeto foi gerado com base nos diferentes padrões selecionados por meio da inserção de diversas atividades, artefatos e papéis que estão implementando os padrões selecionados da ferramenta. No *WebSite* constam todas as atividades que devem ser desenvolvidas durante o desenvolvimento do projeto.

Este trabalho foca em segurança e por isso os padrões selecionados descrevem atividades relacionadas à segurança, porém, padrões complementares a atividades de

segurança podem estar envolvidos no processo e serem incorporados em outras disciplinas, conforme a visão de cada equipe de projeto.

Tabela 7.3 – Atividades do Processo Específico para o projeto XirooPACS

PROCESSO PARA XIROOPACS
Atividades
Add or delete authorization rules as necessary
Assessing risks
Associate pairs of threats versus vulnerabilities with each asset separately
Build table for valuation of assets and determine their value
Collect necessary input information
Construction of table of threats
Contemplating authorization rules in the diagram
Convenient to define processes with company policy
Create a severity scale
Define the importance of each specific security requirements
Determine for each asset type which types of security are need
Determine the business impact
Determine the financial value
Determine the value of security
Determine which approaches to use for each asset type
Determine which assets relate to which business factors
Establish the domain to which the service access control is needed
Generate consolidated reports
Identify attacks that can provide processes
Identify business factors that influence the security protection needs of assets, both external and internal to the enterprise
Identify security risk criteria that influence approaches
Identify the business assets of the enterprise
Identify the threatened
Identify vulnerabilities
Identify what types of security may be needed
Perform threat assessment
Promote authentication, authorization and management of security
Release restricted
Revisit approaches for each asset type as circunstances change
Select policies for access controls to the particular system
Specify a set of factors that affect the specification and the importance of requirements
Specify actions to be taken in case of data breach
Specify the level of granularity to which access control should be applied
Artefatos
UML diagram covering security requirements
Authorization rules of the company
UML Diagram
Presentation of results
Value of users who will be allowed access to the system
Regulation of access
Access policy of the company
Processes within the company
Report access levels and risks posed if there
Access control policy
Level of granularity of the company
Check the impact of each safety requirement
Access control
Description of the main causes of vulnerabilities in systems
Table of severity vulnerabilities relating to the threatened
Security Requirements
Plan risk Security

Laws, policies and restrictions Software architecture document List of events that can cause damage to assets Description of the main causes of vulnerabilities in systems Incident analysis and feedback Security Approaches Enterprise Assets
Papéis
Engineer Security Project Manager Analyst Business

As áreas de processo do modelo SSE-CMM que foram incorporadas ao processo são implementadas através da realização das atividades citadas na Tabela 7.3.

As atividades "*Associate pairs of threats versus vulnerabilities*", "*Build table for valuation of assets and determine their value*", "*Construction of table of threats*", "*Contemplating authorization rules in the diagram*", "*Determine the business impact"*, "*Determine the financial value", "Determine the value of security"* estão associadas as áreas de processos PA01-Administração dos Controles de Segurança, PA02- Avaliação do Impacto, PA03-Avaliação os riscos de segurança, pois implementam ações relacionadas a controles de riscos e segurança de acesso.

"*Collect necessary input information*", "*Identify security risk criteria that influence approaches*", "*Revisit approaches for each asset type as circunstances change*", "*Identify the business assets of the enterprise*", "*Identify what types of security may be needed*" estão associadas as áreas de processos PA09- Fornecer entrada de segurança, PA10- Especificar necessidades de segurança, PA11- Verificação e validação da segurança.

O processo específico para o projeto gerado apresenta características de um projeto que demanda da segurança que está presente em algumas áreas de processo específicas do SSE-CMM.

O anexo B demonstra todas as atividades associadas a cada padrão e a cada área de processo.

7.2.5 Análise dos Resultados

O gerente de projeto foi consultado sobre a validação do resultado. Após a apresentação dos resultados (Tabela 7.3), realizou-se a seguinte questão: "Você concorda com

a literatura? Se as atividades da Tabela 7.3 forem implementadas o sistema Xiroo PACS terá um nível de segurança satisfatório? Por quê?”

Jean Carlos Berni, gerente de projetos da empresa Animati, responsável pelo projeto Xiroo PACS, respondeu:

> Acredita-se que a implementação das atividades que foram relacionadas garantiria um nível de segurança satisfatório para o processo de desenvolvimento do sistema Xiroo PACS. Pontos principais como controle de acesso de usuários por cargos e funções e as possibilidades de verificação de quais atividades estão relacionadas aos atores envolvidos fornecem um nível elevado de confiabilidade ao processo de desenvolvimento. Ainda podem-se perceber atividades de controle de riscos associados ao processo, favorecendo o planejamento dos aspectos de negócios do projeto.

7.3 Estudo de Caso II – Plex

O segundo estudo de caso teve como finalidade demonstrar as características e resultados do estudo de caso realizado através do sistema Plex desenvolvido pela empresa Elevata, uma empresa brasileira que está localizada na cidade de Santa Maria. Marcio Puntel é o gerente de projetos que foi o responsável pelas informações repassadas e por responder o questionário.

7.3.1 Descrição do Sistema

Plex é um sistema de cartão de crédito que visa possibilitar que as empresas tenham seu próprio cartão de crédito. Este sistema integra serviços de administração de cartões, incluindo serviços de vendas monitoradas e risco avaliado.

O acesso ao sistema Plex é feito via *web*. Cada lojista utiliza o software de forma independente. Os dados não são compartilhados, quer dizer, o banco de dados do lojista A não é acessado ou compartilhado pelo lojista B e vice-versa.

A análise do risco do cliente para avaliação de crédito será fornecida pela Solução PLEX, considerando dados cadastrais e comportamento de compra do usuário. A partir desse

momento, o lojista conhece o potencial de compra do cliente e o risco envolvido de acordo com o montante de crédito oferecido (valor de compra, prazo de pagamento, endividamento na loja ou em outras, etc).

Visto que a base de dados deste sistema ira envolver dados de muitos clientes e de várias empresas, que o mesmo cliente pode ter cartões de duas empresas e as cobranças e cadastros precisam ser separados, e ainda que falhas podem acarretar em grande perda de valor para as empresas, pode-se afirmar que este é um sistema que necessita de um alto índice de segurança envolvido no processo.

A análise do sistema foi realizada considerando principalmente a base de dados e a integração com cobranças e cadastros dos clientes.

7.3.2 Priorização das Áreas de Processo

O nível de importância associado a cada área de processo no sistema Plex foi o seguinte:

Tabela 7.4 – Tabulação da importância associada a cada área de processo.

PA01 – Administração dos controles de segurança	Altíssima
PA02 – Avaliação do Impacto	Altíssima
PA03 - Avaliação dos Riscos de segurança	Altíssima
PA04- Avaliação de Ameaças	Alta
PA05- Avaliação de Vulnerabilidades	Altíssima
PA06 – Construção de argumentos de garantia	Altíssima
PA07 – Coordenação da segurança	Alta
PA08 – Monitoração da postura da segurança	Altíssima
PA09 – Fornecer a entrada segurança	Alta
PA10 – Especificar as necessidades de segurança	Alta
PA11 – Verificação e validação da segurança	Altíssima

Um acordo entre o engenheiro de processos e o gerente de segurança definiu que para o projeto em desenvolvimento seriam tratados as áreas de processo aos quais foi atribuído nível de relevância altíssimo ou alto, o que neste caso implica na implementação de todas as PA's.

7.3.3 Padrões Selecionados

Os padrões associados, de acordo com a definição da seção anterior, foram:

Tabela 7.5 – Padrões associados às áreas de processo selecionadas.

Áreas de Processos	**Padrões de Segurança**
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* (SCHUMACHER et al., 2006); *Multilevel Security Pattern* (SCHUMACHER et al., 2006);
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	*Document the Security Goals* (KIENZLE, 2002);

segurança	*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	*Check Point Pattern* (ROSADO, 2006); *Task Process Pattern* (AMBLER, 1998); *Whitehat, Hack Thyself* (ROMANOSKY, 2003);

7.3.4 Processo Específico para o Projeto

Da mesma forma do sistema XIROOPACS, através da inserção de diversas atividades, artefatos e papéis para contemplar a implementação dos padrões solicitados para o projeto, é possível gerar através da ferramenta o WebSite, onde constam todas as atividades que devem ser desenvolvidas durante o desenvolvimento do projeto. Como esta dissertação está focada em segurança o interesse principal está na disciplina de segurança que foi inclusa no processo de desenvolvimento do projeto e, para este estudo de caso, apresenta as atividades que devem ser realizadas para que a segurança esperada para o projeto realmente seja integrada, conforme Tabela 7.6.

Tabela 7.6 – Atividades do Processo Específico para o projeto Plex

PROCESSO PARA O SISTEMA PLEX
Atividades
Add or delete authorization rules as necessary
Assessing risks
Associate pairs of threats versus vulnerabilities with each asset separately
Audit partners in the business
Build table for valuation of assets and determine their values
Collect necessary input information
Construction of table of threats
Contemplating authorization rules in the diagram
Convenient to define processes with company policy
Create a severity scale
Define changes in methods and procedures
Define scope and security requirements
Define the importance of each specific security requirements
Define the relative importance of specific requirements
Determine for each asset type which types of security are need
Determine the business impact
Determine the company's main business-related assets

Determine the financial value
Determine the security for each asset type
Determine the value of security
Determine which approaches to use for each asset type
Determine which assets relate to which business factors
Establish the domain for which the accounting service is need
Establish the domain for which the non-repudiation service is needed
Establish the domain to which the service access control is needed
Generate consolidated reports
Identify and protect communication channels
Identify attacks that can provide processes
Identify business factors that influence the security protection needs of assets, both external and internal to the enterprise
Identify security risk criteria that influence approaches
Identify the business assets of the enterprise
Identify the main business of the company
Identify the threatened
Identify vulnerabilities
Identify what types of security may be needed
Implement secure connections
Perform threat assessment
Present results
Processes under control
Promote authentication, authorization and management of security
Release restricted
Revisit approaches for each asset type as circumstances change
Run termination services activity
Select policies for access controls to the particular system
Specify a set of factors that affect the specialization and importance of requirements
Specify accounting requirements for the target accounting domain
Specify actions to be taken in case of data breach
Specify non-repudiation requirements for the target domain
Specify the level of granularity to which access control should be applied
Artefatos
Provision of company data
Provide details of partners
Identify secure communication and channels
Release channels of communication for research
Security Requirements
Plan risk Security
Laws, policies and restrictions
Software architecture document
Plan iteration
Value of users who will be allowed access to the system
Reports of access control
Access policy of the company
Processes within the company
Regulation of access
Report access levels and risks posed if there
Level of granularity of the company
Access control policy
Check the impact of each safety requirement
UML Diagram
Authorization rules of the company
Critical assets of the company
Basic security needs of each asset
List of events that can cause damage to assets
Description of the main causes of vulnerabilities in systems
Table of severity vulnerabilities relating to the threatened
Company assets
Description of the main causes of vulnerabilities in systems
Table of severity vulnerabilities relating to the threatened
Presentation of results
Services Business
Determine levels services and information
Information, data financial and personal Physical assets
Laws, regulations, mission, goals, business processes, midwives, etc..

Reliability, integrity and availability of enterprise data Access control Incident analysis and feedback Security Approaches Enterprise Assets UML diagram covering safety requirements
Papéis
Engineer Security Project Manager Analyst Business

Como a importância atribuída a cada uma das áreas de processo foi alta ou altíssima, os padrões associados consideram todos os propósitos propostos pelo Modelo SSE-CMM.

Na seção 7.1.4 já foi descrita a relação entre as áreas de processo 01, 02, 03, 09, 10 e 11 com os padrões e as atividades que as implementam.

As áreas de processo 04 - Avaliação de Ameaças e 05- Avaliação de Vulnerabilidades são implementadas através do mesmo conjunto de atividades da área de processo 03 - Avaliação os riscos de segurança. As atividades são "*Associate pairs of threats versus vulnerabilities*", "*Build table for valuation of assets and determine their value*", "*Construction of table of threats*", "*Contemplating authorization rules in the diagram*", "*Determine the business impact*", "*Determine the financial value*", "*Determine the value of security*".

"*Audit partners in the business*", "*Define scope and security requirements*", "*Identify and protect communication channel*s", "*Establish the domain for which the accounting service is need*", "*Specify a set of factors that affect the specification and target domain*", "*Define the relative importance of specific requirements*" são algumas das atividades que implementam a PA07 e PA08, que estão relacionadas a monitoração e coordenação da postura de segurança.

O processo específico para o projeto gerado apresenta características de um projeto que demanda da segurança total do modelo SSE-CMM.

O anexo B demonstra todas as atividades associadas a cada padrão e a cada área de processo.

7.3.5 Análise dos Resultados

Através da análise da Tabela 7.6 percebe-se que várias atividades precisam ser incorporadas no processo de desenvolvimento de software atual para que um nível razoável de segurança seja incorporada ao projeto.

O gerente de projeto foi consultado sobre a validação do resultado. Após a apresentação dos resultados (Tabela 7.6), realizou-se a seguinte questão: "Você concorda com a literatura? Se as atividades da Tabela 7.6 forem implementadas o sistema Plex terá um nível de segurança satisfatório? Por quê?"

Márcio Puntel, gerente de projetos da empresa Elevata, responsável pelo projeto Plex, respondeu:

> "Sim, concordo. Porque existem várias atividades que podem ser flexíveis o suficiente para buscar ações proativas para o maior risco: pessoas e suas ações. No contexto de sistema e hardware existem atividades claras e precisas para garantir a segurança."

7.4 Análise dos Estudos de Caso

Os estudos de caso foram realizados com projetos de características bastante distintas, porém os dois necessitam de um alto índice de segurança e por isso geram processos específicos similares. No primeiro estudo de caso algumas áreas de processo não foram necessárias para a segurança do projeto, já no segundo estudo de caso todas as áreas de processo foram consideradas de relevância alta ou altíssima para o projeto. Os dois sistemas envolvem um nível de segurança bastante alto, para que suas funcionalidades sejam garantidas e os dados devidamente protegidos.

A verificação de quais atividades são realmente de alta importância para o projeto não é uma tarefa fácil, uma vez que a consideração de requisitos adicionais, que não sejam realmente necessários, pode adicionar custos extras e desnecessários para o projeto. A base dos processos padrões das organizações consideradas para os estudos de caso foi o RUP.

Nesta dissertação são sugeridas regras de associação de requisitos de segurança a padrões, mas a organização é quem deve definir suas próprias regras, de acordo com as suas necessidades. Somente o uso das regras definidas para adaptação de processos e avaliações nos resultados obtidos nos projetos permitirão a organização ajustar a base de conhecimento às suas necessidades.

Através dos dois estudos de caso realizados foi possível verificar que o segundo projeto demanda de mais segurança, pois as áreas de processo as quais foi atribuída importância alta ou altíssima pelos engenheiros de segurança e gerente do projeto foram mais expressivas. No segundo estudo de caso foram reveladas mais preocupações relacionadas a ameaças, vulnerabilidades e gerenciamento de garantia de segurança, que correspondem às áreas de processo que não foram implementadas no primeiro estudo de caso.

8. CONSIDERAÇÕES FINAIS

O processo de software e consequentemente o desenvolvimento de sistemas tem se mostrado cada vez mais importante para a organização, para os desenvolvedores e para seus usuários.

Este trabalho propôs uma metodologia para adaptação de processo de desenvolvimento de software, que visa facilitar a tarefa de adaptação. A eficácia dos processos elaborados a partir do *framework* vai depender das regras de associação de padrões às PA's. Um *framework* inicial foi elaborado a partir dos processos SCRUM, RUP e XP; e de padrões de segurança propostos por (SCHUMACHER et al., 2006) e (YODER; BARCALOW, 1998). Não é objetivo desse trabalho propor um *framework* definitivo. Esse trabalho propõe uma forma de organização desses diferentes elementos, mas a organização deve definir os padrões e regras de associação adequadas a sua realidade, e avaliar essas regras constantemente, melhorando-as.

No sentido de apoiar a metodologia desenvolveu-se uma ferramenta *intitulada Security Methodology Tailoring* – SMT. Esta visa elaborar processos confiáveis, por meio da inserção de padrões ao processo de software padrão da organização, de acordo com os requisitos de segurança priorizados para projetos de software.

Essa sistemática provê instrumentos para facilitar a identificação dos requisitos de segurança que devem ser implementados no projeto.

8.1. Trabalhos relacionados

O desenvolvimento de software confiável já vem sendo discutido em muitos trabalhos que buscam maneiras para aumentar as garantias de proteção de um projeto ou de um processo de software. Alguns trabalhos relacionados são apresentados a seguir.

Mellado, Mediana e Piattini (2008) consideram requisitos de segurança desde a fase inicial do desenvolvimento de linhas de produção, através de um processo iterativo e

incremental no qual podem ser adicionadas tarefas, conforme necessidade. Através desta incorporação de tarefas estes autores buscam facilitar a conformidade com as normas segurança e gerenciar possíveis variabilidades que podem acontecer entre requisitos de segurança. Os autores não exemplificam como requisitos de seguranças, abstraídos de normas de segurança, podem ser desdobrados em tarefas. Neste sentido, o presente trabalho visa facilitar a definição de tarefas a partir da associação de padrões, os quais, normalmente, são amplamente explicados, ou até mesmo sugerem as tarefas a serem realizadas para satisfazer o requisito associado.

Paes e Hirata (2007) propõem uma extensão ao RUP com a inclusão de uma disciplina chamada “Segurança”. A disciplina é baseada em boas-práticas e na experiência dos autores (PAES; HIRATA,2007), mas não considera normas ou modelos de segurança. Nesse trabalho não é descrito como o processo definido pode ser adaptado às necessidades dos projetos. Considera-se importante a definição de um modelo ou norma de segurança a ser seguido, uma vez que este possui requisitos bem definidos, como é o caso do modelo SSE-CMM, no qual são definidas Áreas de Processo para serem implementadas e desta forma garantir a segurança da organização.

Hafiz, Adamczyk e Johnson (2007) focam na utilização de padrões para o atendimento de critérios de segurança de software. No entanto, os autores relatam que existe uma grande quantidade de padrões de segurança disponível e é difícil escolher qual o padrão é mais indicado para cada caso, bem como organizá-los para uso em um projeto.

Este trabalho difere dos demais por propor uma adaptação de processos de software por meio de padrões de segurança e por elaborar um *framework* para facilitar a instanciação de processos seguros. A utilização das práticas preconizadas pelo modelo SSE-CMM e de padrões de segurança visa utilizar práticas já consolidadas para desenvolvimento de software confiável.

8.2. Contribuições

8.2.1 Associação de padrões as áreas de processo do SSE-CMM

A associação de padrões as áreas de processo do Modelo SSE-CMM é uma forma de garantir a implementação dos requisitos de segurança previstos no SSE-CMM.

Conforme explicado na seção 4.2 desta dissertação, padrões possuem atividades que devem ser implementadas. Estas atividades são descritas claramente, o que faz com que padrões implementem requisitos de segurança com mais facilidade e eficácia.

A associação de padrões de segurança às áreas de processo do SSE-CMM possibilita que a organização reuse soluções bem sucedidas em vários projetos de software, pois essas regras são cadastradas em um banco de dados constituindo uma base de conhecimento da organização que pode avaliar e atualizar essas informações conforme o desenvolvimentos de projetos futuros.

8.2.2 Adaptação de Processos

A metodologia proposta para realização da adaptação de processos visa auxiliar, através da utilização de elementos de processo (atividades, papéis, artefatos, ferramentas, etc.), a criação de processos que estejam de acordo com a segurança esperada para o projeto.

Uma base de conhecimento existente foi alterada para contemplar dados necessários para a realização da adaptação. Entende-se como base de conhecimento um conjunto de dados que serão utilizados com alguma finalidade específica.

8.2.3 Ferramenta SMT-Tool

SMT-Tool foi elaborada para apoiar o uso da sistemática proposta para gerenciar requisitos de segurança em projetos de software. Conclui-se que uma vez definida a base de conhecimento da organização na ferramenta, a adaptação de processos de software torna-se uma tarefa fácil.

8.2.4 Estudos de Caso

A partir dos estudos de caso realizados conclui-se que podem ser gerados diferentes processos a partir de um mesmo processo padrão, de acordo com as características do projeto.

O objetivo da realização dos estudos de caso foi validar a metodologia e da ferramenta proposta nesta dissertação.

A metodologia foi aplicada em dois projetos reais, o que possibilitou a validação.

8.3. Perspectivas Futuras

A principal perspectiva futura deste trabalho é a criação de níveis de segurança conforme a necessidade de cada projeto específico, levando em consideração requisitos como tamanho do projeto, nível de habilidade da equipe e criticidade do projeto. Um trabalho com a idéia inicial foi publicado sobre o assunto (WAGNER; MACHADO, 2010).

Outra perspectiva futura deste trabalho é estender a abrangência deste trabalho para outros requisitos de segurança, que estejam além de um único modelo, como o SSE-CMM.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799** – Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 21827:2008**. Information technology. Security techniques. Systems Security Engineering. Capability Maturity Model (SSE-CMM).Published in Switzerland. 2nd edition, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006**. Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Associação Brasileira de Normas. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. NBR ISO/IEC 27002:2009**. Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Associação Brasileira de Normas. Rio de Janeiro, 2009.

_____. **ISO/IEC TR 13335-1**. Guidelines for the Management of IT Security(GMITS) - Techniques for the management of IT Security. 1st Edition. Switzerland, 2004.

_____. **ISO/IEC TR 13335-2**. Guidelines for the Management of IT Security (GMITS): Part 2— Managing and Planning IT Security. International Organisation for Standardisation, Switzerland, 1997.

_____.**ISO/IEC 15408-1. Information technology — Security techniques — Evaluation criteria for IT security —** International Organisation for Standardisation , Genebra, 2005.

AIRMIC, IRM "**A structured approach to Enterprise Risk Management (ERM)and the requirements of ISO 31000***"* . Ed. Alarm. Londres, Reino Unido, 2010.

BECK, K. **Programação Extrema (XP) Explicada: Acolha as Mudanças**. Ed. Bookman: Porto Alegre. 2004.

BECK, K.; **Test Driven Development: By Example** Ed., Pearson Education, United States. 2003

BRAZ, F. Instrumentação da análise e projeto de software seguro baseada em ameaças e padrões. Tese (Doutorado em Engenharia Elétrica) - Faculdade de tecnologia, Brasília, Brasil, 2009.

BYERS, D., SHAHMEHRI, N. **Design of a Process for Software Security.** Second International Conference on Availability, Reliability and Security (ARES'07), v.2, p.301-309,Viena, Austria. 2007.

CAMPOS A., **Sistema de segurança da informação –** Controlando os riscos. Visual Books: Santa Catarina, 2007.

COMPAGNA L. et al. **How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns**. In: Artificial Intelligence and Law v. 17, n. 1, p. 1-30, New York, EUA.

ERNST & YOUNG. (2008). **Global Information Security Survey.** Reino Unido, 2008. Disponível em:< http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf>. Acesso em 10 de fev. de 2010.

FERNANDES E. et al. Using security patterns to build secure systems. Workshop on Software Patterns and Quality (SPAQu'07), Nagoya, Japan, 2007.

FERREIRA F. N. F., ARAÚJO T. M., **Política de Segurança da Informação**. Rio de Janeiro: Ciência Moderna. 2008.

FONTES E. "**Segurança da Informação – O usuário faz a diferença**". São Paulo: Saraiva. 2008.

FONTOURA, M. L. "***PRiMA: Project Risk Management Approach***". Tese (Doutorado em Ciência da Computação). Universidade Federal do Rio Grande do Sul – UFRGS. Porto Alegre, Brasil. 2006.

FOWLER, M. **The New Methodology**. Disponível em: <http://www.martinfowler.com/articles/newMethodology.html>. Acesso em: ago. 2010.

FONTES, E. **Segurança da Informação:** O usuário faz a diferença. São Paulo: Saraiva, 2006.

GOERTZEL, K. M., **Software Security Assurance.** State-of-the-Art Report (SOAR). 2007

HALFIZ M., ADAMCZYK P. and JOHNSON R. **Organizing Security Patterns**. IEEE Software (vol. 24 no. 4) p. 52-60. Illinois, EUA 2007.

HARTMANN, J. **Utilizando Padrões Organizacionais e Avaliação de Risco para Adaptar a Metodologia de Desenvolvimento de Software**. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre. 2005.

HE R., WANG H., LIN Z., **A Software Process Tailoring Approach Using a Unified Lifecycle Template**. Em: Computational Intelligence and Software Engineering, 2009. CiSE 2009.

HIGHSMITH, J.: **Agile Project Management: Creating Innovative Products** Ed., Pearson Education/Addison-Wesley, United States. 2004.

HUMPHREY, WATTS. S. ***Managing the software process***. Addison-Wesley, 1989.

IBM Corporation.**IBM Rational Unified Process v7.0**. 2007.

LACHAPELLE E., **White Paper : Control Objectives for Information and related Technology**, Montreal, Canada, 2007.

LAUREANO, M. A. P.; **Gestão de Segurança da Informação**. PUCPR –PPGIA, 2005.

KAJAVA, Jorma. et al. **Information Security Standards and Global Business**. ICIT 2006. IEEE International Conference. Industrial Technology, 2006.

KHAN, A., ZULKERNINE U., MOHAMMAD A. **Activity and Artifact Views of a Secure Software Development Process.** International Conference on Computational Science and Engineering. , pp. 339- 404, 2009.

KHAN M. U. A., ZULKERNINE, M. **Quantifying Security in Secure Software Development Phases** Annual IEEE International Computer Software and Applications Conference, v.3 p. 905-960 Washington, USA, 2008.

KRAUSE, M; TIPTON, H. F. **Handbook of Information Security Management**. Auerbach Publications, 1999.

KROLL, J., FONTOURA M. L., WAGNER, R., (2010) **Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008**. Em: Simpósio Brasileiro de Sistemas de Informação, Marabá, Pará.

KROLL J., FONTOURA L. M., D'ORNELLAS M. C., WAGNER R., **Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008**. SBSI – Simpósio Brasileiro de Sistemas de Informação. 2010.

KRUCHTEN P. ***The Rational Unified Process – An Introduction***. Ed., Reading, Mass.: Addison-Wesley. 2000.

MEAD, NANCY R., LINGER R., MCHUGH J., LIPSON H., **Managing Software Development for Survivable Systems**, *Annals Software Eng.*, vol. 11, no. 1, pp. 45–78, 2001.

MEAD NANCY R., MCGRAW GARY, **A Portal for Software Security**, IEEE SECURITY & PRIVACY, pp. 75-79, USA. 2005.

MELLADO D., MEDINA, F. E., PIATTINI M., 2008 ***Security Requirements Variability for Software Product Lines*** Em: IEEE. University of Castilla La-Mancha – Espanha.

NUNES F. J. B., BELCHIOR A. D., ALBUQUERQUE A. B., **A knowledge Management Aproach to Support a Secure Software Development** Universidade de Fortaleza – Fortaleza. Brasil.

MEAD N., **Requirements Engineering for Survivable Systems**. Carnegie Mellon University EUA, 2003.

MCAFEE. **Cybercrime cost $1 trillion last year.** Disponível em: http://news.zdnet.com/2100-9595_22-264762.html Acesso em 8 de jul. de 2010. 2009.

MCGRAW, G.; **Software Security**, IEEE Security & Privacity. v.2, p.32- 36. EUA. 2004

MCGRAW G,. **Software Security**: Build Security In. Addison-Wesley Software Security Series, EUA, 2006.

MOFFETT J,. HALEY C,. NUSEIBEH B,. **Core Security Requirements Artefacts** Security Requirements Group, Reino Unido, 2004.

NUNES, F. **PASS - Processo de Apoio à Segurança de Software**, Fundação Edson Queiroz Universidade De Fortaleza, Fortaleza, 2007.

PAES, C. E. B. e HIRATA, C. M. 2007. ***RUP extension for the development of secure systems.*** In: Portal ACM, Pontifícia Universidade Católica de São Paulo - Instituto Tecnológico de Aeronáutica – São Paulo, Brasil.

QUINTELLA M,. CÔRTES R,. **Estudo Comparativo da Compatibilidade entre IRM e ITIL na Gestão de Ativos de TI (Estudo de Caso)**. UFF – FGV-EAESP VIII SIMPOI, 2005.

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.

RATIONAL Software Corporation, **Rational Unified Process Best Practices for Software Development Teams**. In: IBM Rational Software. Disponível em: <http://www.rational.com/media/whitepapers/rup_bestpractices.pdf.> Acesso em: nov. de 2009. 1998.

ROBERTSON K,. **Detecting and Preventing Attacks Against Web Applications**. Tese (Doutorado em Ciência da Computação). Universidade da Califórnia, Santa Barbara, EUA. 2009

ROSADO D. et al. **A Study of Security Architectural Patterns.** In: Proceedings of the First International Conference on Availability, Reliability and Security, Washington, USA. 2006.

RUI H., HAO W., ZHIQING L., **A Software Process Tailoring Approach Using a Unified Lifecycle Template** Em: Computational Intelligence and Software Engineering. Beijing, China. p. 1 – 7, DEC. 2009.

SAHIBUDIN, S.; SHARIFI, M.; AYAT, M. **Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations**, University Teknologi Malaysia, p. 749 - 753 2008.

SCHUMACHER M, et al. **Security Patterns**. J.Wiley & Sons, 2006.

SCHWABER K., SUTHERLAND J.,**Guia do Srum**. *ScrumAlliance.* Nov. 2009

SÊMOLA M., **Gestão da Segurança da Informação – Uma visão executiva** Rio de Janeiro: Elsevier. 2003

SEMOLA M,. **Gestão Da Segurança Da Informação**. Ed Campus, 2009.

SOFTWARE ENGINEERING INSTITUTE **Capability Maturity Model,** 2009.

SHIMADA,L. M.; JUNIOR, M. V. C. **Aplicação do ITIL e ISO/IEC 20000 na Gestão de Serviços de Suporte em Microinformática**.UNIFIEO – revista da Pós-Graduação 2008.

SIEWERT. V., **Resumo da Norma ISO/IEC 13335-3**. Disponível em: < http://www.vivaolinux.com.br/artigos/impressora.php?codigo=5072>. Acesso em 7 de julho de 2010. 2006.

SOMMERVILLE I. **Engenharia de software** São Paulo: Pearson Addison – Wesley

SHUJA, A. **Welcome to the IBM Rational Unified Process and Certification**. Em: IBM Rational Software. Disponível em: <http://www.ibmpressbooks.com/bookstore/product.asp?isbn=0131562924 > Acesso em jan. de 2010, 2008.

SOFTWARE ENGINEERING INSTITUTE. **Systems Security Engineering-Capability Maturity Model Group (SSE-CMM) – Model Description Document**. Version 3.0,

International Systems Security Engineering Association. Disponível em: <http://www.sse-cmm.org/docs/ssecmmv3final.pdf > Acesso em nov. de 2009. 2003.

SORTICA E.A.; CLEMENTI, S.; CARVALHO B.; **Governança de TI: Comparativo entre COBIT e ITIL**. FGV-EAESP – CATI 2004 – Anais do Congresso Anual de Tecnologia da Informação 2004 .

TELES V., M., **Extreme Programming: Aprenda a encantar seus usuários desenvolvendo software com agilidade e alta qualidade.** Editora Novatec. São Paulo, Brasil. 2004.

TONDEL, I. A.; JAATUM, M.G.; MELAND P.H.; **Security Requirements for the rest of us: A survey.** IEEE Software. IEEE Computing Society. Loa Alamitos. CA. USA, v. 25, n.1, p. 20-27. 2008. ISSN 0740-7459.

TOVAR, E.; CARRILLO J.; VEJA V.; GASCA G. **Desarrollo de productos de Software seguros en sintonía con los Modelos SSE-CMM, COBIT e ITIL.** Universidad Católica del Norte - Universidad Politécnica de Madrid. Madrid. Disponível em : <http://www.aemes.org/rpm/descargar.php?volumen=3&numero=2#page=2> Acesso em 30 de junho de 2009. 2006.

TROWBRICGE D., **Enterprise Solution Patterns Using Microsoft .NET**, Microsoft Corporation. 2003

UM kit de ferramentas para a excelência de TI Disponível em: <http://www.efagundes.com/Artigos/COBIT.htm> 2009

WAGNER R., FONTOURA L., KROL J., **Análise dos Critérios de Segurança do COBIT baseado no Modelo SSE-CMM**. In: XXXVI Conferência Latino-americana de Informática (XXXVI CLEI) Assunção, Paraguai. 2010

WAGNER R., FONTOURA L., NUNES R., **Extensão de um framework de processo para adaptação à segurança em aplicações Web**. In: Simpósio Brasileiro de Sistemas Multimídia e Web (WebMedia 2010) Minas Gerais, Brasil, 2010.

WAGNER R., MACHADO A., **Níveis de segurança para processos de desenvolvimento de software seguro**. In: Simpósio de Informática da Região Centro, Santa Maria, 2010.

WASSERMANN R., **Using Security Patterns to Model and Analyze Security Requirements**, 2004.

WEISS M,. MOURATIDIS H,. **Selecting Security Patterns that Fulfill Security Requirements**, In: 16th IEEE International Requirements Engineering Conference pages 169–172. IEEE Computer Society. 2008.

ANEXOS

ANEXO A - PUBLICAÇÕES E PESQUISAS RELACIONADAS À DISSERTAÇÃO

Durante o desenvolvimento da dissertação, foram realizadas as seguintes publicações.

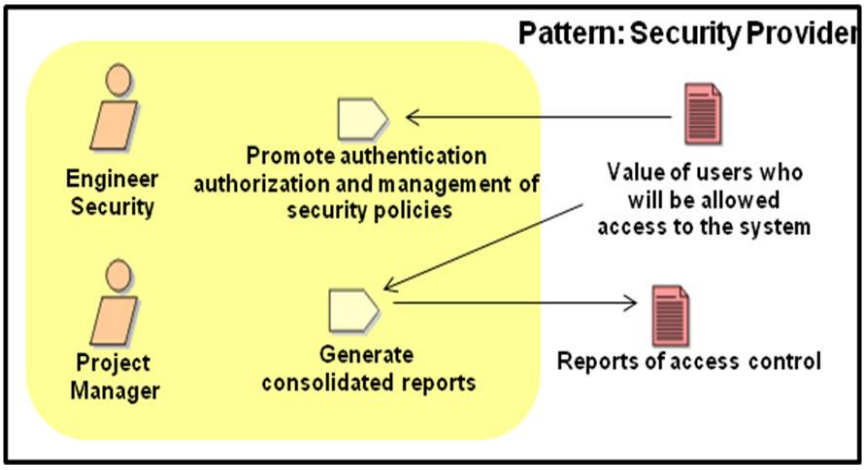
Tabela A1 – Publicações relacionadas à dissertação.

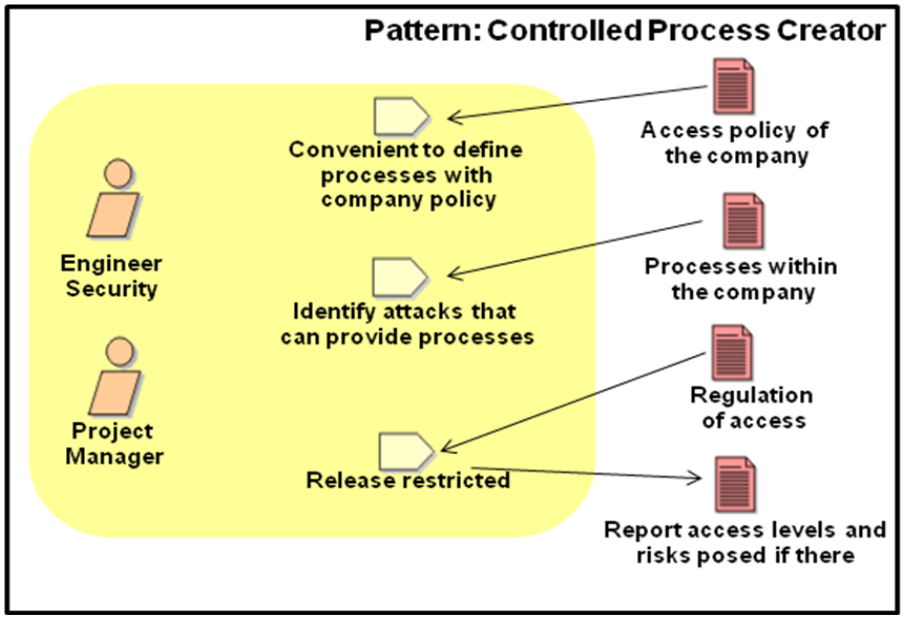
LOCAL	TITULO	AUTORES
SBSI 2010 - Simpósio Brasileiro de Sistemas de Informação	Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008	Josiane Kroll, Lisandra M. Fontoura, Rosana Wagner e Marcos C. D'Ornellas
WTES/SBES 2010 - Workshop de Teses e Dissertações do Simpósio Brasileiro de Engenharia de Software	Processos de Desenvolvimento de Software Confiável Baseados em Padrões de Segurança	Rosana Wagner e Lisandra M. Fontoura
CLEI 2010 – Conferência Latino Americana de Informática	Análise dos Critérios de Segurança do COBIT baseado no Modelo SSE-CMM	Rosana Wagner, Lisandra M. Fontoura e Josiane Kroll
WebMedia 2010 – Simpósio Brasileiro de Sistemas Multimídia e Web (Forma de Pôster)	Extensão de um *framework* de processo para adaptação à segurança em aplicações Web	Rosana Wagner, Lisandra M. Fontoura e Raul Ceretta Nunes
SIRC 2010 – Simpósio de Informática da Região Centro	Níveis de segurança para processos de desenvolvimento de software seguro	Rosana Wagner e Alencar Machado
CIbSE 2011 – Congresso Ibero-Americano em Engenharia de Software (Aceito para publicação como *short paper*)	Metodologia para a Adaptação de Processos de Software baseada no Modelo SSE-CMM	Rosana Wagner e Lisandra M. Fontoura

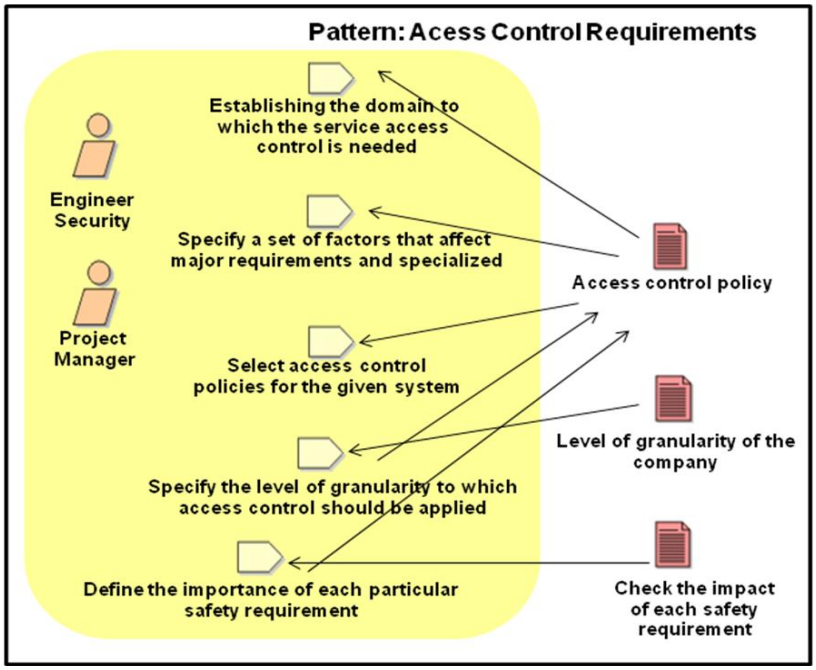
ANEXO B – ARTEFATOS, ATIVIDADES E PAPÉIS UTILIZADOS PARA A ADAPTAÇÃO DO PROCESSO

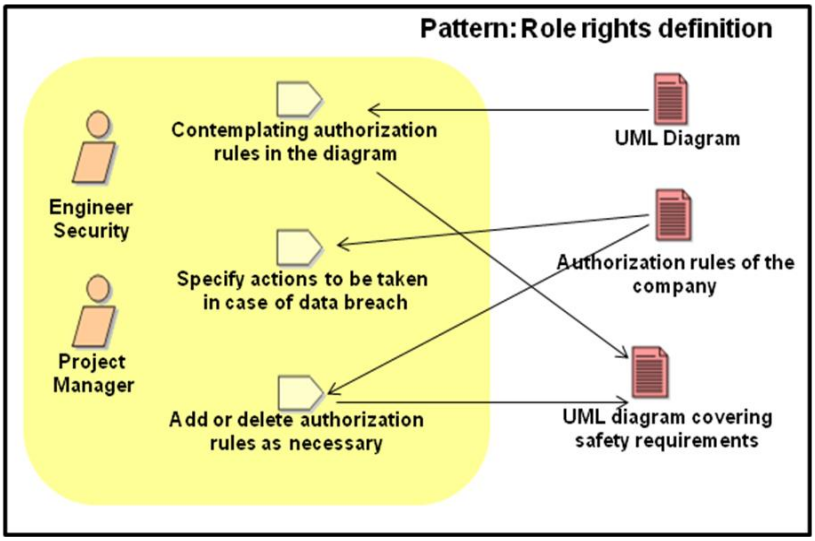
PA01 - Administração dos controles de segurança

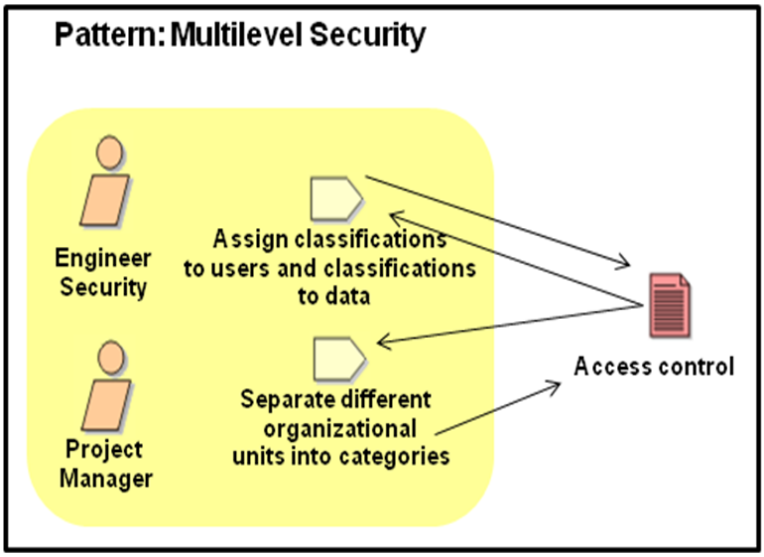
- Security Provider (ROMANOSKY, 2002);
- Controlled Process Creator (SCHUMACHER et al., 2006);
- Access Control Requirements (SCHUMACHER et al., 2006);
- Role Rights Definition (SCHUMACHER et al., 2006);
- Role-Based Access Control (SCHUMACHER et al., 2006); (Segundo Schumacher este padrão é implementado pelo Role Rights Definition (SCHUMACHER et al., 2006);)
- Authorization Pattern (SCHUMACHER et al., 2006); (implementado pelo Multilevel Security Patterns)
- Multilevel Security Pattern (SCHUMACHER et al., 2006);





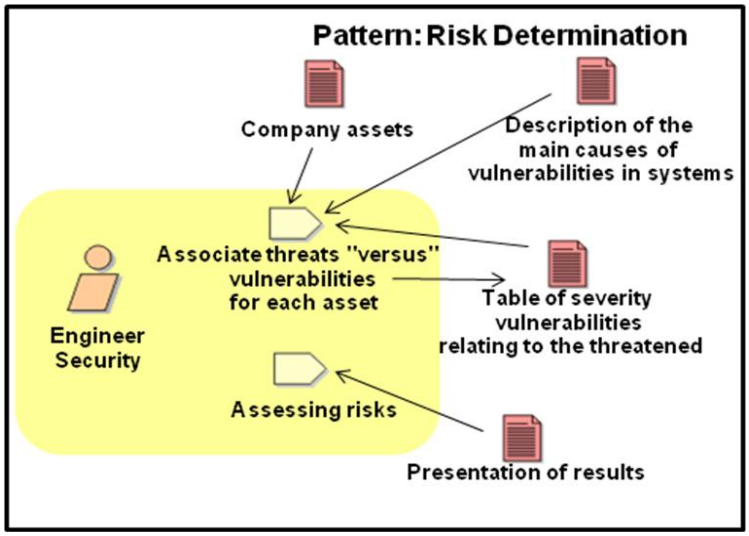

Pattern: Acess Control Requirements
Establishing the domain to which the service access control is needed
Engineer Security
Specify a set of factors that affect major requirements and specialized
Access control policy
Project Manager
Select access control policies for the given system
Level of granularity of the company
Specify the level of granularity to which access control should be applied
Define the importance of each particular safety requirement
Check the impact of each safety requirement


Pattern: Role rights definition
Contemplating authorization rules in the diagram
UML Diagram
Engineer Security
Specify actions to be taken in case of data breach
Authorization rules of the company
Project Manager
Add or delete authorization rules as necessary
UML diagram covering safety requirements


Pattern: Multilevel Security
Engineer Security
Assign classifications to users and classifications to data
Access control
Project Manager
Separate different organizational units into categories

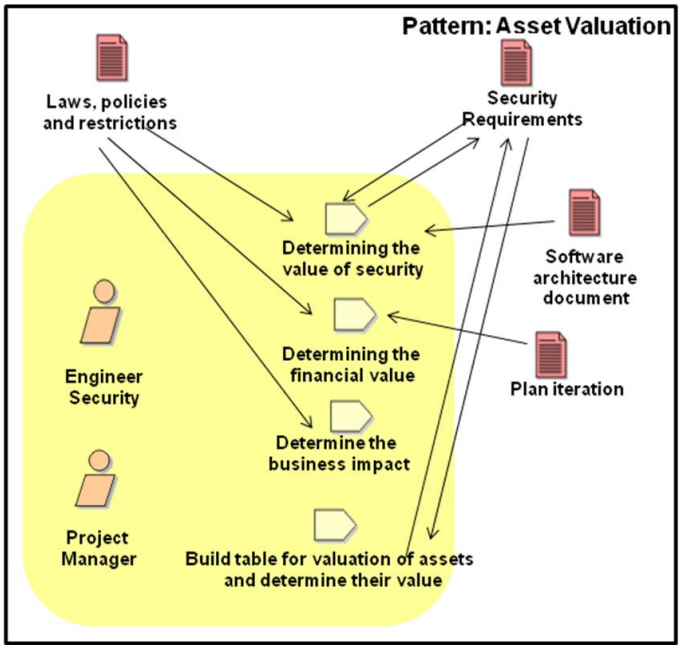
PA02- Avaliação do impacto

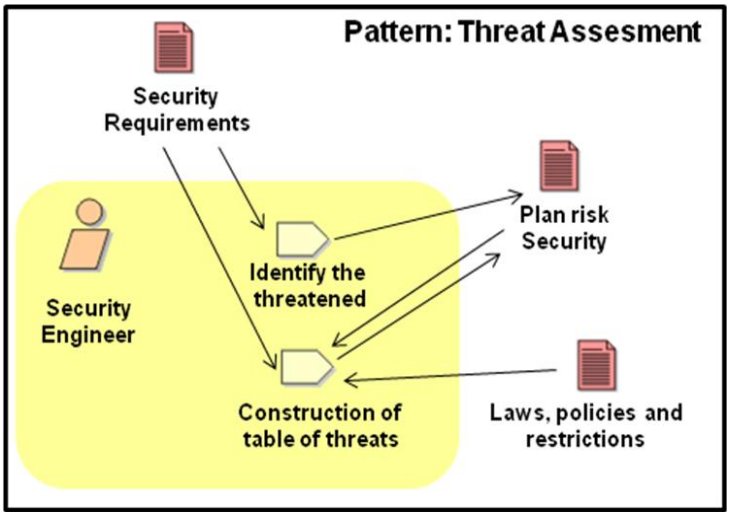
- Risk Determination (SCHUMACHER et al., 2006);

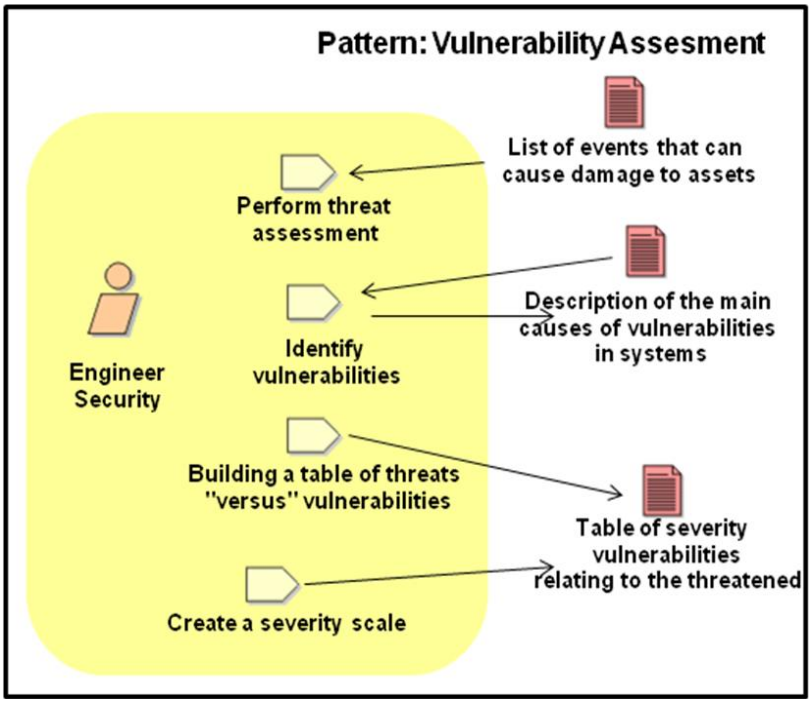


PA03- Avaliação dos Riscos de segurança

- 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);

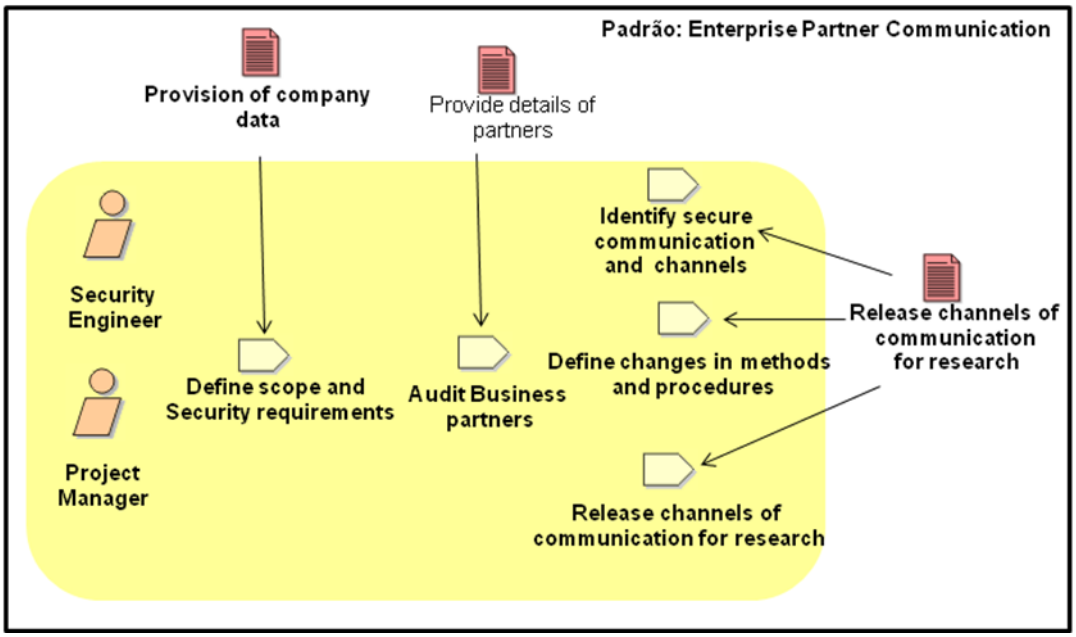
PA05- Avaliação de Vulnerabilidades
 Vulnerability Assessment (SCHUMACHER et al., 2006);

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);

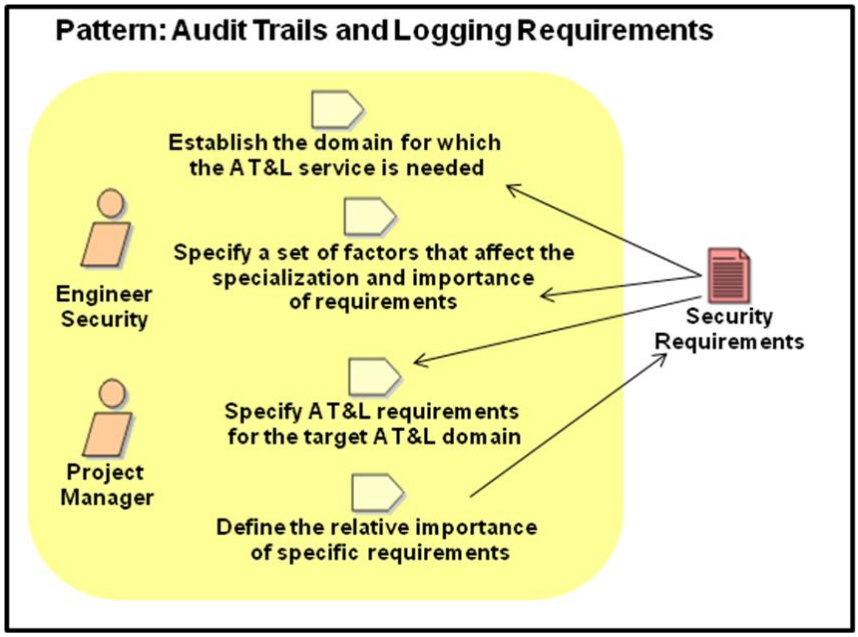
PA07 – Coordenação da segurança

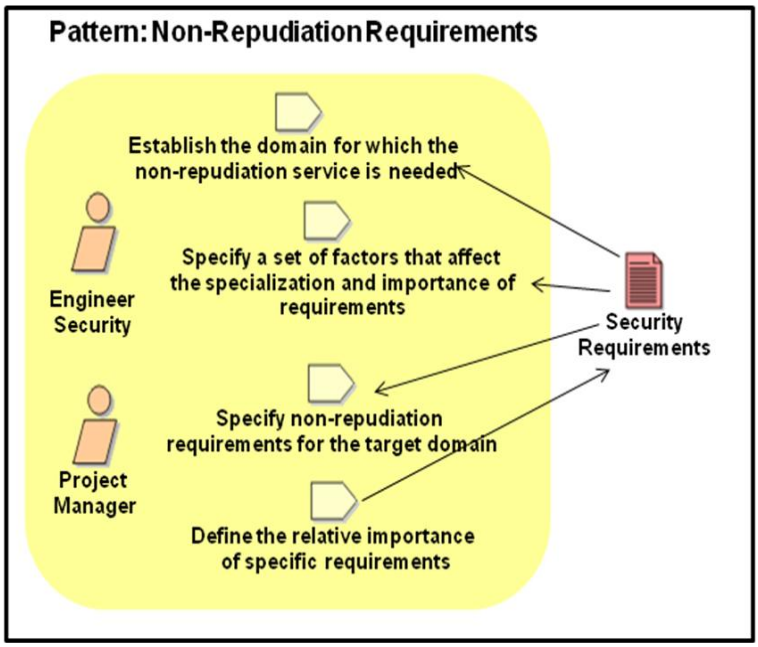
 Enterprise Partner Communication (SCHUMACHER et al., 2006);
 Share Responsibility for Security (KIENZLE, 2002);
 Gatekeeper (COPLIEN, 1999);
 Buffalo Mountain (organizational) (COPLIEN, 1999);

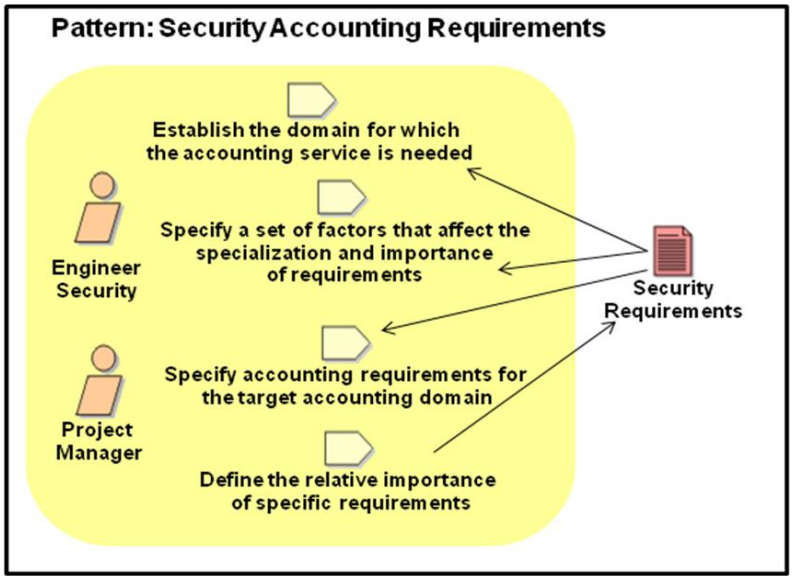


PA08 – Monitoração da postura da segurança

 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);

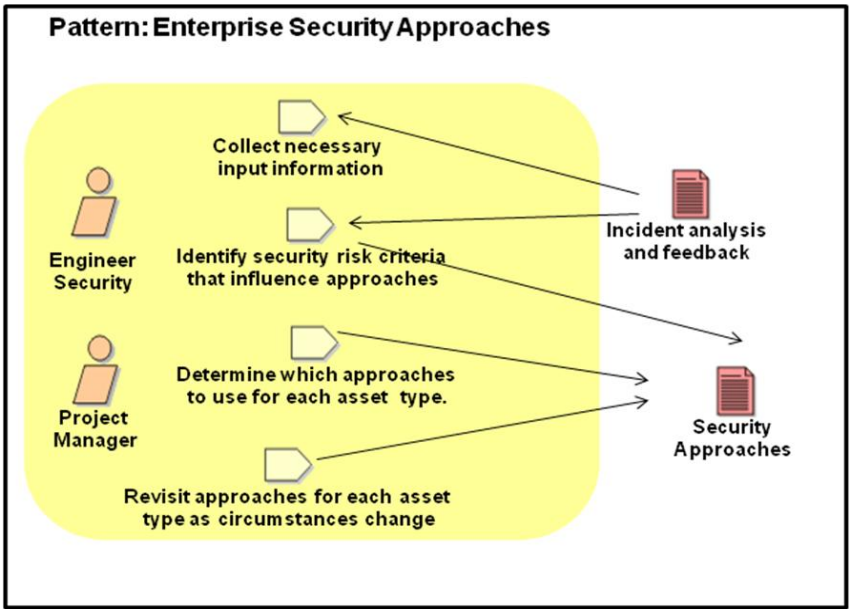

Pattern: Audit Trails and Logging Requirements
Establish the domain for which the AT&L service is needed
Specify a set of factors that affect the specialization and importance of requirements
Engineer Security
Security Requirements
Specify AT&L requirements for the target AT&L domain
Project Manager
Define the relative importance of specific requirements

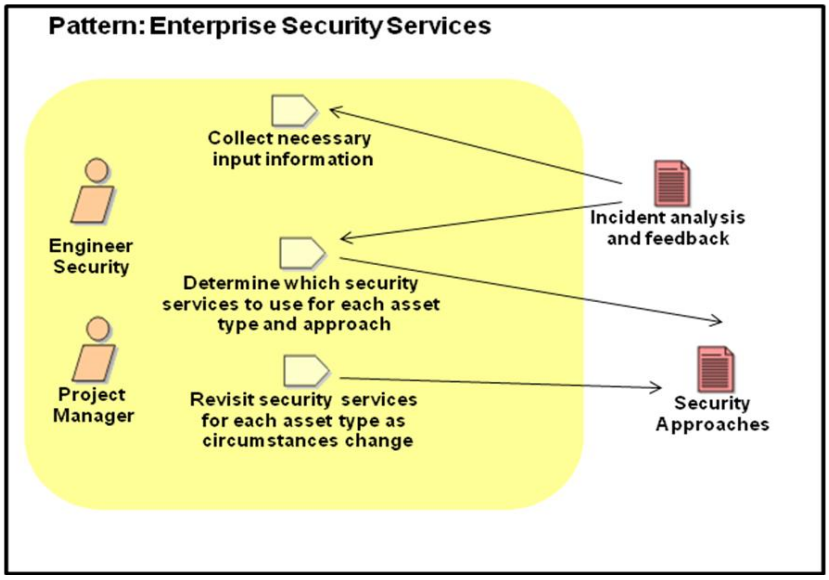

Pattern: Non-Repudiation Requirements
Establish the domain for which the non-repudiation service is needed
Specify a set of factors that affect the specialization and importance of requirements
Engineer Security
Security Requirements
Specify non-repudiation requirements for the target domain
Project Manager
Define the relative importance of specific requirements



PA09 – Fornecer a entrada segurança

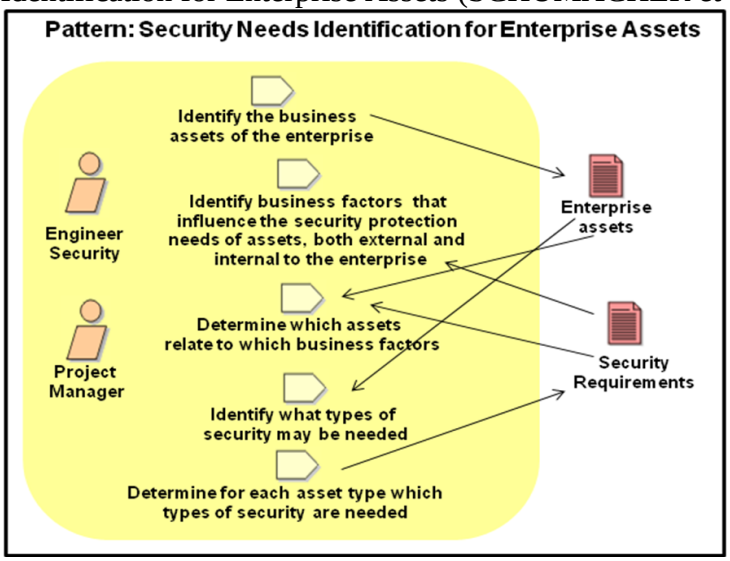
- Document the Security Goals (KIENZLE, 2002);
- Document the Server ConFiguration (KIENZLE, 2002);
- Enterprise Security Approaches (SCHUMACHER et al., 2006);
- Enterprise Security Services (SCHUMACHER et al., 2006);





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).

ANEXO C – QUESTIONÁRIO ENVIADO AS EMPRESAS

	Questionário para Identificação dos Requisitos de Segurança Relevantes para um Software

IDENTIFICAÇÃO	
NOME:	
EMPRESA:	
SOFTWARE:	
DATA:	

Instruções para preenchimento:

- Nome: é o nome da pessoa que está respondendo o questionário.
- Cargo: é o cargo ocupado pela pessoa.
- Empresa: nome da empresa desenvolvedora do software.
- Software: nome do software para o qual os requisitos estão sendo identificados

Este questionário visa identificar quais áreas de processo, propostas pelo SSE-CMM são desejáveis ao software sendo desenvolvido. As áreas de processo foram extraídas de:
SSE-CMM. Systems Security Engineering-Capability Maturity Model Group (SSE-CMM) – Model Description Document. Version 3.0, International Systems Security Engineering Association. Disponível em: <http://www.sse-cmm.org/docs/ssecmmv3final.pdf > Acesso em nov. de 2009. 2003.

Observações:

- Indiferentemente do motivo, caso a pessoa que está respondendo o questionário, não se sinta confortável em responder alguma questão, pode não o fazê-lo;
- Os dados coletados serão utilizados para a seleção de padrões de segurança relevantes ao processo de software;
- Comprometemos, Rosana Wagner e Lisandra Manzoni Fontoura, a SOMENTE divulgar as informações que forem autorizadas pelas empresas que participarem desta pesquisa e também a divulgar as conclusões obtidas no estudo.

DEFINIÇÃO DE TERMOS
Ativos: é qualquer coisa de valor que deve ser protegido de danos. Um ativo pode exigir proteção, porque é o potencial alvo de ataque. Os bens podem ser pessoas, propriedades (ex. dados, hardware, software e instalações) e serviços.
Ataque: (violação de segurança) é a tentativa não autorizada de um atacante de causar dano a um ativo (ou seja, violar a segurança do sistema, ignorar os mecanismos de segurança). Um ataque pode ser bem sucedido ou não.
Atacante: é um agente (por exemplo, os seres humanos, programas, processos, dispositivos ou outros sistemas) que provoca um ataque devido ao desejo de causar danos a um ativo.
Dano: é um impacto negativo associado a um ativo, devido a um ataque.
Ameaça: é uma condição geral, situação ou estado (geralmente correspondente a motivação dos invasores em potencial) que pode resultar em um ou mais ataques relacionados.

	Identificação de Áreas de Processo

Instruções para preenchimento: assinale o nível de relevância de cada área de processo abaixo relacionada para o projeto de software. Justifique sua resposta caso seja necessário.

MODELO SSE-CMM
PA01(Process Area) - Administração dos controles de segurança - Assegurar que a segurança destinada para o sistema é integrada dentro do projeto do sistema e é de fato realizada pelo sistema resultante em seu estado operacional. Níveis de relevância da área de processo: ☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante Comentário:
PA02- Avaliação do 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 imateriais, como a perda de reputação. Níveis de relevância da área de processo: ☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante Comentário:

PA03- Avaliação dos 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA04- Avaliação de ameaças - Identificar as ameaças de segurança, suas características e propriedades.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA05- Avaliação de 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA06 – Construção de argumentos de garantia - Transmitir claramente que as necessidades de segurança do cliente são cumpridas.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA07 – Coordenação da 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA08 – Monitoração da 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA09 – Fornecer a entrada 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA10 – Especificar as 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário:

PA11 – Verificação e validação da 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.

Níveis de relevância da área de processo:
☐ Altíssima ☐ Alta ☐ Média ☐ Baixa ☐ Não relevante

Comentário: