Alexandre Balesteros Alves

Software Seguro:
Processo para Desenvolvimento de Requisitos de Segurança

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia de Software.

São Paulo
2016

Alexandre Balesteros Alves

Software Seguro:
Processo para Desenvolvimento de Requisitos de Segurança

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia de Software.

Área de Concentração: Tecnologia de Software

Orientador: Profª. MSc. Sarah Kohan

São Paulo
2016

Catalogação-na-publicação

Alves, Alexandre Balesteros
Software Seguro: Processo para Desenvolvimento de Requisitos de Segurança / A. B. Alves -- São Paulo, 2016.
79 p.

Monografia (MBA em Tecnologia de Software) - Escola Politécnica da Universidade de São Paulo. PECE – Programa de Educação Continuada em Engenharia.

1.Segurança 2.Processos 3.Requisitos 4.Análise de Riscos I.Universidade de São Paulo. Escola Politécnica. PECE – Programa de Educação Continuada em Engenharia II.t.

DEDICATÓRIA

Dedico este trabalho a minha esposa Gisele e aos meus filhos Leonardo e Sophia.

AGRADECIMENTOS

Agradeço ao PECE – Programa de Educação Continuada em Engenharia pela estrutura e qualidade do curso que proporcionou essa grande oportunidade de crescimento profissional e acadêmico.

Agradeço a minha orientadora, Professora MSc. Sarah Kohan, por todo apoio e ensinamentos durante todo o processo de elaboração desse trabalho.

A toda minha família, em especial aos meus pais pelo caráter e dedicação ao longo de toda a minha vida.

RESUMO

O objetivo dos processos de desenvolvimento de software seguro é garantir a qualidade e segurança do produto através de uma sequência de atividades aplicadas ao longo de todo o ciclo de desenvolvimento.

A vivencia no ambiente de desenvolvimento de software nos mostra que usualmente as empresas não dão a devida importância para a segurança e geralmente quando ocorrem, são aplicadas somente nas fases finais do desenvolvimento.

A única forma de se produzir um software que seja seguro é aplicando os conceitos de segurança desde as primeiras tarefas do projeto, desde quando as ideias começam a ser organizadas para o início dos trabalhos.

Este trabalho concentra-se nas fases iniciais do projeto, mais precisamente na etapa de elaboração de requisitos de segurança, onde comprovadamente a maioria das vulnerabilidades de um software nascem, muitas vezes devido a negligência, falta de conhecimento ou de tempo.

ABSTRACT

The purpose of the secure software development process is to ensure the quality and safety of the product through a sequence of activities applied throughout the development lifecycle.

The experiences in the software development environment shows that companies usually do not give due importance to the safety and usually when they occur, are applied only in the final stages of development.

The unic way to produce software that is secure is applying safety concepts from the first project tasks, from when the ideas begin to be arranged for the start of work.

This work focuses on the early stages of the project, more precisely in the preparation stage of security requirements, which proved most vulnerabilities of software are born, often due to neglect, lack of knowledge or time.

LISTA DE ILUSTRAÇÕES

Pág.

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

IF	Instituição Financeira
ATM	Caixa Eletrônico (Automatic Teller Machine)
API	Application Programming Interface
PDV	Ponto de Venda Terminal remoto para meio de pagamento
NIST	National Institute of Standards and Technology
SQUARE	Security Quality Requirements Engineering
SERA	Security Engineering Risk Analysis

SUMÁRIO

1. INTRODUÇÃO

Este capítulo apresenta as motivações, objetivos e justificativas que inspiraram o estudo que levou ao desenvolvimento deste trabalho.

1.1 Motivações

Nos dias atuais, o uso de sistemas de software é fundamental para empresas, governos e cidadãos. Dia após dia, esses sistemas de software vêm se tornado mais complexos e intrínsecos à vida de todos nós.

Informações confidenciais são processadas, transmitidas e armazenadas por esses sistemas o tempo todo. Desta forma, os sistemas de software vêm se tornando alvo de ações criminosas crescentes com o objetivo de obter informações confidenciais para uso em operações ilícitas.

É uma questão essencial para as empresas que desenvolvem e utilizam software, melhorar constantemente a segurança dos seus sistemas frente a essas novas ameaças para proteger seus ativos e os ativos dos seus clientes.

Problemas de segurança de software afetam diretamente a confidencialidade, integridade e disponibilidade. Segurança não pode ser vista como uma funcionalidade, mas sim como uma propriedade do software que deve ser levada em consideração sobre todo o processo de desenvolvimento do sistema Yasar, Preuveneers, Berbers e Batthi (2008).

Este trabalho, tem como foco o processo de desenvolvimento de requisitos de segurança, pois trata-se da atividade inicial do ciclo de desenvolvimento ou manutenção de um software sendo o ponto inicial para abordar as questões de segurança.

1.2 Objetivo

O objetivo deste trabalho é apresentar uma proposta para um processo de desenvolvimento de requisitos de segurança para a construção e manutenção

software seguro e resiliente, para que empresas possam incorporá-lo ao seu ciclo de desenvolvimento.

1.3 Justificativas

Atualmente os ataques a sistemas com o intuito de obter informações sigilosas tem aumentado drasticamente e o principal alvo são as mensagens trocadas entre os componentes que integram os sistemas.

Segundo Wincor Nixdorf (2015), o número de fraudes contra ATMs aumentou 32% entre os anos de 2009 e 2013 na Europa onde identificou-se o crescimento de ocorrências de Ataques Lógicos contra ATMs, somente nos Estados Unidos o setor de serviços financeiros registrou perdas de US$23,6 milhões com ataques lógicos no ano de 2013, representando um aumento de 43,9% em comparação com o ano de 2012.

A dependência da tecnologia da informação faz da segurança do software um elemento chave para a solidez dos negócios de uma empresa em relação a continuidade dos seus serviços, recuperação de desastres, confiabilidade dos consumidores e propriedade intelectual.

Na era atual, os serviços e processos oferecidos pelas empresas são totalmente dependentes de sistemas de software que processam, armazenam e transmitem informações críticas para os seus negócios, essas informações compreendem dados sensíveis, relevantes e privados da empresa e de seus clientes.

* ATM – Authomatic Teller Machines, conhecidos no Brasil como Caixas Eletrônicos, são dispositivos eletromecânicos automatizados dotados de submódulos como dispensadores de cédulas, teclados e leitores de cartão magnético. Esses submódulos são controlados por interface de comunicação e software de aplicação bancária embarcadas em uma unidade CPU.

Sendo assim, os sistemas de software são foco constantes de ataques de cyberterroristas, crime organizado e diversos outros tipos de criminosos que visam acessá-los para obter dados valiosos. A grande maioria desses sistemas de software não são resistentes aos ataques.

O processo de desenvolvimento de requisitos de segurança para software seguro tem como principal objetivo cobrir as deficiências de segurança encontradas ao longo do ciclo de desenvolvimento tradicional, adicionando atividades específicas de análise de riscos no processo de desenvolvimento de requisitos.

Falhas de segurança afetam diretamente a resiliência de um sistema frente a ataques, expondo-o a possíveis quebras de segurança, a adoção do processo de desenvolvimento de requisitos de segurança é o primeiro passo para reduzir de forma significante o número de falhas e vulnerabilidades no produto final.

O processo proposto neste trabalho busca a correção de vulnerabilidades potenciais o mais cedo possível, através da adoção de um processo de desenvolvimento de requisitos de segurança baseado no modelo SQUARE proposto por Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nacy R. Mead, (2008), com foco em análise de riscos de segurança.

1.4 Estrutura do Trabalho

Para a elaboração do trabalho foi seguida a seguinte estrutura:

O Capítulo 1 – INTRODUÇÃO, apresenta as motivações, o objetivo, as justificativas e a estrutura do trabalho.

O Capítulo 2 - REVISÃO BIBLIOGRÁFICA, apresenta um panorama geral da literatura pesquisada, apresentando os pontos de vista verificados nos artigos e livros utilizados como base para a elaboração deste trabalho.

O Capítulo 3 - DESENVOLVIMENTO, apresenta a proposta do processo de desenvolvimento de requisitos de segurança com análise de riscos e modelagem de ameaças.

O Capítulo 4 - ANÁLISE DOS RESULTADOS, apresenta os resultados verificados durante a aplicação do processo elaborado e apresentado no capítulo 3, apresentando os prós e contras da sua aplicação.

O Capítulo 5 - CONSIDERAÇÕES FINAIS, descreve um panorama geral do trabalho, apresentando as conclusões obtidas e propostas de trabalhos futuros.

2. REVISÃO BIBLIOGRÁFICA

Este capítulo apresenta os estudos relevantes realizados para o tema escolhido

2.1 Introdução

O desenvolvimento de requisitos de segurança requer que a corporação adote uma série de processos que encadeiam técnicas específicas, habilidades e experiências CMMI Institute, Siemens AG Corporate (2013).

Quando um software é desenvolvido sob a ótica de segurança, ele torna-se mais resistente a ataques e falhas não intencionais McGraw, Allen, Mead, Ellison e Barnum, (2013).

Segundo Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nacy R. Mead, (2008) as propriedades fundamentais que caracterizam um software como seguro são: Confidencialidade, Integridade e Disponibilidade.

2.1.1 Confidencialidade

Para um software ser considerado seguro o mesmo deverá ser construído de tal forma que suas características funcionais, seus ativos e o seu conteúdo estejam esta devidamente protegidos de acessos indevidos por parte de usuários ou entidades não autorizadas. Esta propriedade é válida mesmo para softwares de código aberto, onde estas caracteristicas estão disponíveis, porém o software deve manter a confidencialidade dos seus dados geridos.

2.1.2 Integridade

O software e os ativos sob sua gestão devem ser resiliente a adulteração ou modificações, mesmo que ocorram ações não autorizadas ao seu código fonte, configurações ou comportamento. As adulterações dos ativos incluem ações como a substituição, corrupção, destruição, inserção lógica (intencional e não intencional) ou eliminação. A integridade deve ser preservada durante o desenvolvimento e durante sua execução.

2.1.3 Disponibilidade

O software deve permanecer operacional e acessível aos seus usuários autorizados (sejam eles humanos ou outros sistemas de software) sempre que necessário, ao mesmo tempo que, o mesmo, deve permanecer inacessível para usuários não autorizados (sejam eles humanos ou outros sistemas de software).

Segundo Yasar, Preuverneers, Berbers e Bhatti (2008), problemas de segurança de software afetam diretamente as três características fundamentais. Segurança não pode ser vista como uma funcionalidade, mas sim como uma propriedade do software que deve ser levada em consideração sobre todo o seu processo de desenvolvimento.

2.2 Processo de Desenvolvimento de Software

Segundo Sommerville (2007) um processo de software caracteriza-se por uma sequência de atividades estruturadas de tal forma que permita a produção de um produto de Software.

As atividades consideradas como fundamentais para o ciclo de desenvolvimento de software e o ciclo de vida do produto são apresentadas a seguir;

- **Definição de Requisitos;**
  Definições e objetivos do software são definidos nessa fase através de consulta aos *stakeholders* do sistema. Nesta fase, os requisitos são levantados e a especificação do sistema é gerada.
- **Projeto de Sistema de Software;**
  Definição da arquitetura do sistema, identificação de componentes e estabelecimento de suas relações.
- **Implementação e testes unitários;**
  Nesta fase, os componentes estabelecidos são codificados de forma independente, os testes unitários verificam se os componentes atendem as especificações definidas.
- **Integração e testes de sistema;**

Esta fase consiste em integrar os componentes que foram construídos de forma independente, formando o sistema como um todo. Os testes avaliam o funcionamento completo e se o software construído atende ao uso pretendido.

- **Operação e Manutenção;**
  Fase mais longa do ciclo de vida do produto, é a fase onde o sistema é instalado em ambiente operacional, a manutenção do software consiste em correções de erros que não foram identificadas nas fases anteriores do projeto.

2.3 Processo de Desenvolvimento de Software Seguro

O processo de desenvolvimento de software seguro, consiste em agregar atividades específicas ao longo do ciclo de desenvolvimento padrão, para que segurança seja adotada desde o princípio do ciclo de desenvolvimento do produto, Noopur, Davis (2006) define processos como “uma sequência de passos executados para um determinado propósito”, ou seja, desta forma um processo de desenvolvimento de software seguro pode ser especificado como uma série de atividades, que não são necessariamente sequenciais, mas que tem como objetivo desenvolver, executar e manter uma solução de software segura.

A adoção de um processo de desenvolvimento de software seguro deve cobrir as deficiências de segurança encontradas no processo padrão de desenvolvimento, adicionando atividades específicas de análise de riscos, práticas e verificações durante todo o ciclo de vida, reduzindo o número de falhas e vulnerabilidades no software entregue.

2.4 Desenvolvimento de Software Seguro com CMMI

Esta sessão é baseada nos tópicos apresentados por CMMI Institute Siemens AG Corporate (2013), aborda quatro áreas específicas de engenharia:

- **Preparação organizacional para desenvolvimento de software seguro:**
  Tem como objetivo estabelecer e manter padrões corporativos para o desenvolvimento de software seguro e também prover ações em casos de identificação de vulnerabilidades.
- **Gerenciamento de software seguro em projetos:**

O objetivo dessa área de processo é estabelecer, planejar e gerenciar atividades e riscos de segurança durante o ciclo de vida do projeto.

- **Requisitos e solução técnica para desenvolvimento de software seguro:**
  Tem como proposta estabelecer os requisitos de segurança e adoção de técnicas de implementação voltadas a segurança do software, assegurando-se que o desenvolvimento atenda às necessidades de segurança estabelecidas.
- **Validação e Verificação de software seguro:**
  O objetivo dessa área de processo é assegurar que o produto desenvolvido seja aderente com a especificação de segurança, demonstrando que o software atende as expectativas estabelecidas quando o mesmo é posto no seu ambiente operacional.

Com a adoção desses processos, a corporação estabelece a produção e manutenção de software seguro com abrangência em todo o ciclo de desenvolvimento, ao invés da adoção de ações pontuais reativas ao descobrimento de vulnerabilidades ao longo do processo. Sendo assim, a corporação estaria apta a desenvolver software seguro por concepção e construção que atendam às necessidades de segurança estabelecidas pelo seu mercado de atuação.

A maioria das empresas adotam ações de segurança em seus produtos de forma ineficaz, como por exemplo adotando guias de codificação ou testes de penetração em fases já avançadas do processo, levando a detecção de problemas de forma tardia. As detecções de problemas em fases avançadas do desenvolvimento usualmente são onerosas devido a necessidade de retrabalhos na arquitetura do produto ou em sua concepção de *design*, essas atividades isoladas podem culminar na entrega de um produto com riscos severos de segurança.

A tabela 1 apresenta a Estrutura de Segurança no Desenvolvimento de Software Seguro, baseado no guia de desenvolvimento seguro do CMMI.

Tabela 1 - Detalhamento de atividades de segurança

CMMI DEV Área	Área de Processo de Segurança	Objetivos
Gerenciamento de Projetos	Preparação Organizacional para Desenvolvimento Seguro	Estabelecer a capacidade organizacional para desenvolver produtos seguros
	Gerenciamento de Segurança em Projetos	Preparar e gerenciar atividades para segurança
		Gerenciar Riscos de Segurança do Produto
Engenharia	Requisitos e Solução Técnica de Segurança	Desenvolver requisitos de Segurança do cliente, Arquitetura e Design de Segurança
		Implementar Design de Segurança
	Validação e Verificação de Segurança	Efetuar verificações de Segurança
		Efetuar validações de Segurança

Fonte: CMMI Institute Siemens AG Corporate (2013)

Para que o processo se torne eficaz, uma série de atividades e características em nível organizacional são necessárias, essas atividades devem ser incorporadas aos processos de desenvolvimento da empresa de tal forma que eles se tornem parte integral das atividades diárias da corporação, o que requer forte patrocínio e comprometimento da alta gerência para que todos os níveis se adequem.

Para que o desenvolvimento de software seguro seja adotado, os ambientes de desenvolvimento demandam requisitos especiais, tais como ferramentas específicas e alto nível de proteção contra acessos indevidos, desta forma a segurança da informação torna-se mais do que nunca uma questão crítica para a preparação da corporação.

Os processos de desenvolvimento de software seguro devem ser adequados e inseridos aos planos de melhoria de processos da empresa, sendo implementados de

forma gradativa ao longo de implantações de melhorias dos processos da organização de acordo com suas prioridades.

2.4.1 Preparação da Organizacional para o Desenvolvimento de Software Seguro

O propósito dessa área de processo é preparar a empresa para o desenvolvimento seguro, de forma a estabelecer e manter competências para o desenvolvimento e manutenção de produtos seguros.

Para o desenvolvimento de software seguro a empresa necessita estabelecer competências que permitirão o gerenciamento e manutenção de um ciclo de vida consistente para os produtos que demandem desenvolvimento com segurança, sendo que as práticas dessa área de processo são:

- Estabelecer e manter o comprometimento, patrocinio e envolvimento da alta gerência da empresa com o desenvolvimento de produtos seguros orientados pelos objetivos de negócios de segurança e processos.
- Estabelecer e manter processos padronizados em nível organizacional para o desenvolvimento de produtos seguros.
- Estabelecer e manter o comprometimento dos interessados, o conhecimento e habilidades para o desenvolvimento de produtos seguros.
- Estabelecer e manter padrões de ambiente de trabalho que permitam o desenvolvimento seguro e protejam os ativos de trabalho do uso não autorizado.
- Estabelecer e manter padrões de identificação de vulnerabilidades.

2.4.2 Gerenciamento em Projetos de Software Seguro

Tem como propósito gerenciar as atividades de segurança, estabelecendo, identificando e planejando as diversas atividades ao longo do andamento do projeto e gerenciando os riscos encontrados. As práticas dessa área de processo são:

- Estabelecer e manter planos para o desenvolvimento de um produto seguro e integrá-los com outros planos do projeto.
- Planejar treinamento com o objetivo em adquirir conhecimentos e habilidades necessárias para executar de projetos de segurança.
- A segurança deverá ser endereçada durante a seleção de fornecedores e componentes de terceiros para produtos seguros.
- Analisar e resolver as causas de vulnerabilidades de segurança.
- Executar avaliações de riscos de segurança.
- Estabelecer um plano para mitigação de riscos de segurança.
- Estabelecer um plano para gerenciamento de riscos de segurança.

2.4.3 Desenvolvimento de Requisitos de Segurança e Solução Técnica

Esta área de processo tem como propósito estabelelecer o desenvolvimento de requisitos de segurança e o desenvolvimento seguro, com o intúito de assegurar o desenvolvimento do software seguro.

2.4.3.1 Desenvolvimento de Requisitos de Segurança

Para que um produto seja considerado seguro, é essencial que ele possua requisitos de segurança, que vão além do conceito de atributos de qualidade.

O desenvolvimento dos requisitos de segurança deve ser integrado diretamente aos requisitos regulares do projeto, sendo que os mesmos devem ser usados para a implementação da solução técnica, os padrões de segurança devem ser aplicados a todos os componentes do produto, inclusive componentes adquiridos de terceiros, afim de garantir a cadeia de segurança do produto.

As práticas do desenvolvimento dos requisitos de segurança são:

- Desenvolvimento dos requisitos de segurança junto ao cliente.

- Desenvolvimento do produto em conformidade com a arquitetura de segurança e os princípios de *desgin*.
- Seleção das tecnologias apropriada utilizando os critérios de segurança.
- Estabelecer padrões de configuração para os produtos seguros.

2.4.3.2 Implementação do *Design* para Software Seguro

O desenvolvimento seguro é estabelecido para garantir que os padrões de segurança e as tecnologias adequadas serão aplicadas durante o desenvolvimento do produto.

As práticas da implementação de *design* para software seguro são:

- Adoção do uso de padrões de segurança para implementação.
- Adição de informações de segurança as documentações de suporte do produto.

2.4.4 Verificação e Validação de Segurança

O propósito de validações e verificações de segurança é garantir que o produto entregue esteja aderente aos requisitos de segurança, e que o mesmo atenda as expectativas de segurança quando instalado no seu ambiente operacional.

2.4.4.1 Verificação de Segurança

O objetivo da verificação de segurança é assegurar que o software projetado está condizente com os requisitos estabelecidos pelo projeto, aderente com as diretrizes de segurança pré-estabelecidas.

As práticas da verificação de segurança são:

- Preparação para execução da verificação de segurança.
- Execução da verificação de segurança.

2.4.4.2 Validação de Segurança

A validação de segurança consiste em comprovar a resistência contra ameaças do produto entregue em seu ambiente operacional. O objetivo é identificar vulnerabilidades através de testes que não confrontem diretamente com os requisitos de segurança definidos, como no processo de verificação, os resultados obtidos devem ser devidamente documentados afim de serem utilizados como base para execução de ações corretivas.

As práticas da validação de segurança são:

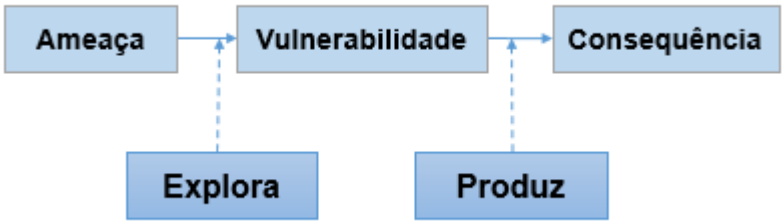
- Preparação para execução da validação de segurança.
- Execução da validação de segurança.

2.5 Riscos de Segurança de Software

Segundo Islam, Shareeful (2010), riscos referem-se a elementos que efetivamente tenham potencialidade de causar danos. Em projetos de desenvolvimento de software, riscos podem ser definidos como a possibilidade de sofrer perdas, sejam elas financeiras (relativas a atrasos ou modificações de cronogramas), insatisfação do cliente com o produto entregue devido à baixa qualidade, ou ainda, devido ao comprometimento dos ativos da empresa ou do cliente devido a um evento indesejável ocorrido durante o ciclo de desenvolvimento e posteriormente do uso do produto.

De acordo com Christopher, Woody e Audrey (2014), o detalhamento dos riscos de segurança estão ligados a probabilidade que uma ameaça explore uma determinada vulnerabilidade no sistema de software e de que essa combinação provoque consequências negativas como perdas para a companhia ou para os seus clientes, sendo assim, um risco de segurança é composto pela combinação dos três elementos: Ameaça, Vulnerabilidade e Consequência.
Desta forma pode-se elaborar o seguinte diagrama que ilustra o ciclo de um risco:

Figura 1 – Ciclo de Vida de um Risco



Fonte – Baseado em Alberts, Woody e Dorofee (2014).

Elementos do ciclo de vida de um risco de segurança

- **Ameaça** – Constitui-se de uma ação que venha a explorar uma ou mais vulnerabilidades existentes no sistema. Esta traz consequências adversas ou perdas.

- **Vulnerabilidade** – Define-se como vulnerabilidade uma fragilidade encontrada em um sistema de software, pode caracterizar-se por uma condição especifica, como uma falha de configuração, sistema de operação, falhas de arquitetura ou codificação. Uma vulnerabilidade pode ser explorada ocasionando uma situação adversa ou perda. A vulnerabilidade é considerada como um elemento passivo, do risco pois ela por si só não leva a perdas.

- **Consequência** – É a perda ocasionada por uma ou mais vulnerabilidades exploradas por uma determinada ameaça. A perda pode ser mensurável (referente a uma perda de valores) ou imensurável (referente a perdas na imagem da marca da corporação).

2.5.1 Exemplo de Risco de Segurança

A companhia *Acme* provedora de serviços possui uma rede de terminais PDV, onde os dados de pagamentos de cartão de crédito são transmitidos sem criptografia entre os terminais espalhados pelos pontos de venda e o Servidor da empresa, que é responsável pela autorização do pagamento das compras. Um software malicioso *(malware)* instalado na rede corporativa da empresa analisa os dados das transações que trafegam em aberto, alteram o valor a ser debitado dos clientes antes que seja

autorizada a transação. Após a resposta do Servidor, os dados são modificados e reencaminhados ao terminal PDV. A quantia adulterada é desviada para uma conta especifica do fraudador. Como resultado a companhia e os clientes finais sofreram perdas mensuráveis (perdas financeiras, devido a necessidade de ressarcimento dos clientes) e perdas imensuráveis (comprometimento da reputação da marca).

Neste cenário identificam-se os três componentes de um risco de segurança:

***Ameaça**:* Software malicioso instalado na infraestrutura de software da empresa que utiliza dados não criptografados das compras para manipulação de solicitação de pagamento, e desvio de valores para uma determinada conta. A ameaça refere-se a um ataque sobre uma transação de valores monetários.

Vulnerabilidade: A corporação que não efetua a criptografia dos dados das compras que trafegam em "*plaintext"* entre os componentes de infraestrutura computacional da companhia.

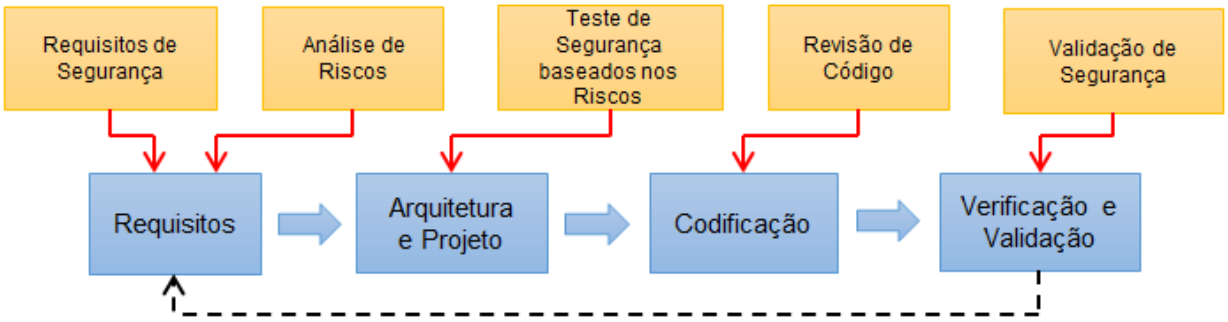
Consequências: A companhia que pode sofrer perdas financeiras significativas devido ressarcimento de clientes, perdas com multas, eventuais processos e grandes perdas da reputação da marca.

Neste exemplo, fica claro o entrelaçamento entre os três componentes que compõe um risco de segurança; A ameaça (o software malicioso), explora uma determinada vulnerabilidade (dados de pagamentos digitais que trafegam sem criptografia entre sistemas) ocasionam perdas para companhia, entretanto, a vulnerabilidade por si só não causa perdas, caso o cenário de ataque não ocorra a vulnerabilidade permanecerá "adormecida" até que uma ameaça venha a explora-la.

2.6 Considerações do Capítulo

O processo de desenvolvimento de software seguro deve cobrir as deficiências de segurança encontradas no ciclo de desenvolvimento padrão, adicionando atividades específicas de elaboração de requisitos de segurança, análise de riscos, modelagem de ameaças e práticas de verificações durante todo o ciclo de vida. A figura 2 ilustra as atividades de segurança agregadas ao ciclo de desenvolvimento padrão.

Figura 2, Processo de desenvolvimento seguro



Fonte - Allen, Barnum, Ellison, McGraw e R.Mead, (2006)

Os controles de segurança devem se estender por todas as fases tradicionais, como Requisitos, Arquitetura e Projeto, Codificação, e Verificação e Validação, bem como continuar em fases de revisão de código, testes de validação de segurança, controle de configuração, qualidade e deploy, as atividades de segurança também devem ser estendidas para a fase de manutenção, assegurando que vulnerabilidades não sejam introduzidas posteriormente.

3. DESENVOLVIMENTO DE REQUISITOS DE SEGURANÇA

3.1 Introdução

Este capítulo apresenta uma proposta para um Processo de Desenvolvimento de Requisitos de Segurança Orientados a Riscos baseado no método SQUARE proposto por Mead, Hough e Stehney (2005) que é fundamental para a estruturação do processo de desenvolvimento de software seguro. A análise de riscos de segurança proposto no processo baseia-se no estudo de Alberts, Woody e Dorofee (2014) que apresenta o método SERA.

3.2 Processo de Desenvolvimento de Software Seguro

Segundo Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nacy R. Mead, (2008), software desenvolvido com os princípios de segurança deverá possuir as seguintes características:

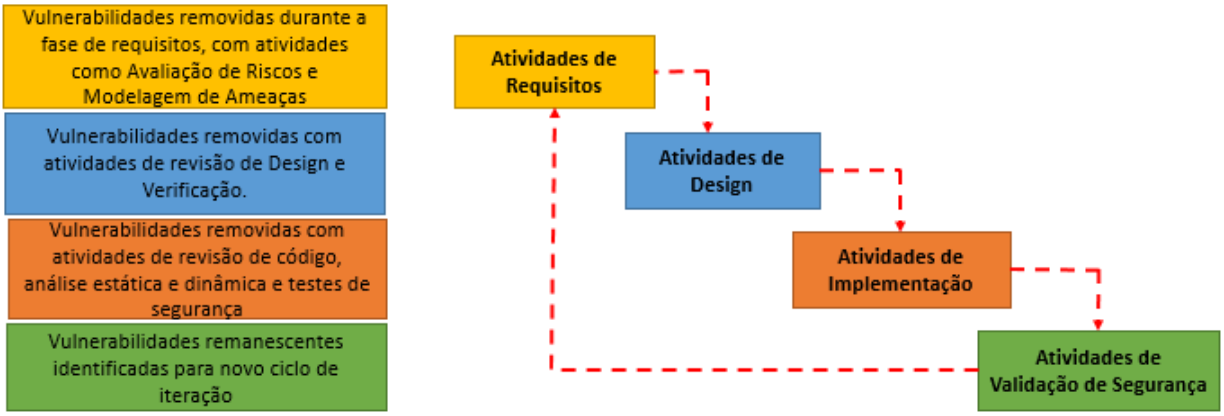
- Previsibilidade de Execução
  Quando o software é confiável, e sua execução segue os fluxos definidos, sem que ocorram quebras de execução, a probabilidade de que ocorram entradas indesejadas, que venham a alterar o funcionamento do software é significantemente reduzida.

- Confiabilidade:
  O objetivo é reduzir ao máximo o número de vulnerabilidades ao longo do ciclo de desenvolvimento seguro que possam ser exploradas por ataques maliciosos.

- Conformidade:
  Garantir através de atividades regulares de validação e verificação que os componentes, artefatos e entregas estão em conformidade com os requisitos estabelecidos e funcionam corretamente no ambiente para o qual foi desenvolvido.

A figura 3, apresenta conceitualmente as quatro etapas fundamentais de um ciclo de desenvolvimento de software seguro, e como as vulnerabilidades são reduzidas gradualmente ao longo de todas as fases do ciclo, expressando a necessidade de aplicação dos conceitos de segurança desde o início do processo. A figura 3, apresenta o ciclo de Identificação e Remoção de Vulnerabilidades ao longo do ciclo de desenvolvimento seguro

Figura 3: Identificação e Remoção de Vulnerabilidades Durante o Ciclo de Desenvolvimento Seguro



Fonte: Adaptado de Noopur, Davis (2006)

A proposta apresentada neste capitulo, situa-se na primeira fase do processo de desenvolvimento de software seguro, ou seja, com enfoque na fase de Engenharia de Requisitos, onde é apresentado um processo para o desenvolvimento de requisitos de segurança baseado em análise de riscos e ameaças.

3.3 Processo de Desenvolvimento dos Requisitos de Segurança

O processo de desenvolvimento dos requisitos de segurança é uma tarefa fundamental para o sucesso de um projeto de desenvolvimento de software.

Usualmente, os fundamentos de segurança não são levados em consideração nesta fase do projeto. A adoção de objetivos de segurança durante o processo de definição dos requisitos do projeto pode traduzir-se na economia de milhares de reais para a companhia. Mead, Hough e Stehney (2005) sita em seu trabalho que a correção de defeitos em fases mais avançadas do projeto podem custar entre 10 e 200 vezes a mais se detectados precocemente na fase de estabelecimento dos requisitos, sendo

assim os custos de correções em fases finais do projeto são sabidamente mais onerosas para as companhias de desenvolvimento de software. Com o estabelecimento de uma metodologia para geração dos requisitos de segurança as empresas serão diretamente beneficiadas ao longo do processo de desenvolvimento.

O processo para o desenvolvimento de requisitos de segurança, tem como intuito incluir as necessidades de segurança no desenvolvimento de software desde as primeiras reuniões de definição do escopo do projeto. Para que os requisitos sejam criados de forma adequada pressupõe-se a interação entre a equipe de requisitos com especialistas em segurança e os demais *stakeholders* do projeto, estabelecendo-se uma equipe com diferentes visões sobre o produto. Esta equipe deverá estar alinhada, definindo padrões de comunicação e definições técnicas que deverão ser utilizadas em todas as fases do processo.

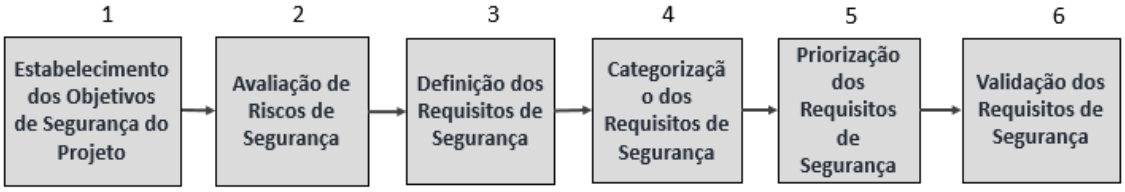
As propostas para estabelecimento dos requisitos de segurança são baseadas no método SQUARE proposto por Mead, Hough e Stehney (2005) onde os objetivos de segurança são definidos em função de análise de riscos derivados dos objetivos de negócios atribuídos ao projeto.

Cabe a equipe de requisitos (composta pelos engenheiros de requisitos, especialistas em segurança e *stakeholders*) desenvolver os artefatos necessários que auxiliem na modelagem dos requisitos de segurança.

O conteúdo dos artefatos fornecerá as entradas necessárias para os estudos de avaliação de riscos, que por sua vez permitirão a visualização de forma efetiva dos possíveis impactos que as ameaças podem representar aos objetivos de segurança estabelecidos, permitindo assim, maior precisão no desenvolvimento dos requisitos de segurança, que satisfaçam os objetivos de segurança do projeto. Os requisitos de segurança por sua vez, devem ser compostos por itens claros e verificáveis que deverão ser aprovados pelos *stakeholders* do projeto.

Para o desenvolvimento dos requisitos de segurança é proposto o processo, composto pelas atividades descritas no diagrama da figura 4.

Figura 4 – Proposta para o processo de desenvolvimento de requisitos de segurança



Fonte - Baseado em Mead, Hough e Stehney (2005)

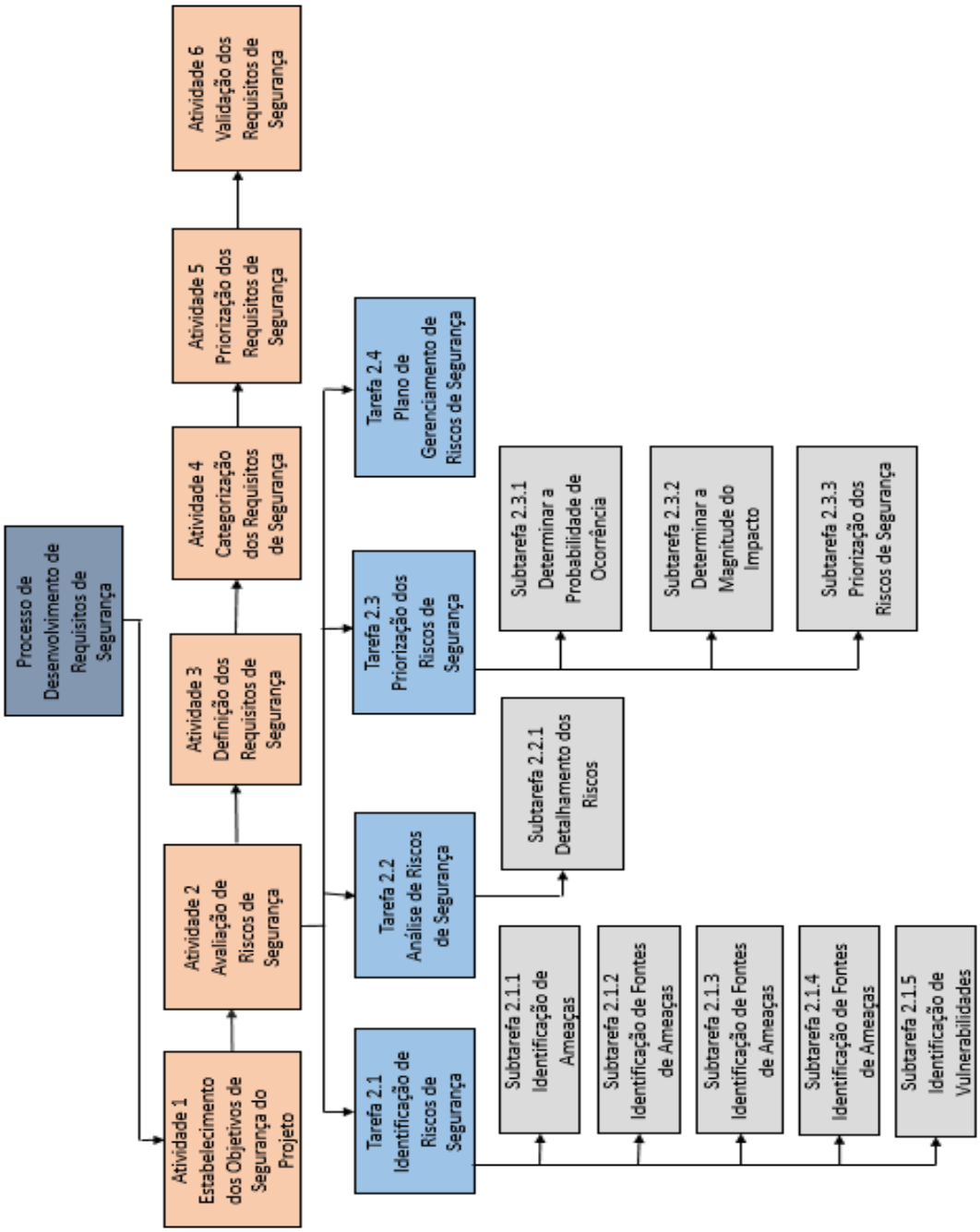
Tabela 2 – Lista de Atividades para o processo de desenvolvimento de requisitos de segurança

ID	Atividade	Descrição
1	Estabelecimento dos Objetivos de Segurança do Projeto	Definição dos objetivos, requisitos de negócio voltados a segurança, políticas e exemplos de procedimentos.
2	Avaliação de Riscos de Segurança	Avaliação dos riscos potenciais que o projeto será exposto, incluindo um processo para modelagem de ameaças.
3	Definição dos Requisitos de Segurança	Elicitação dos requisitos através de entrevistas com *Stakeholders*, baseado na modelagem resultante da avaliação de riscos da etapa anterior.
4	Categorização dos Requisitos de Segurança	Categorizar os requisitos nos níveis de negócio, sistema e software.
5	Priorização dos Requisitos de Segurança	Priorização dos requisitos de acordo com a avaliação de riscos.
6	Validação dos Requisitos de Segurança	Técnicas de inspeção para verificação da validade dos requisitos estabelecidos.

Fonte- Baseado em Mead, Hough e Stehney (2005)

A figura 5 apresenta uma visão geral do processo de desenvolvimento de requisitos de segurança proposto nesse trabalho.

Figura 5, Processo de Desenvolvimento de Requisitos de Seguraça



Fonte - Autor

3.3.1 Estabelecimento dos Objetivos de Segurança do Produto

O objetivo desta atividade é determinar quais são os objetivos de segurança que o sistema deve contemplar. Os objetivos de segurança podem ser classificados como o ponto de partida para o processo de desenvolvimento dos requisitos de segurança, esses objetivos muitas vezes são abstratos e podem entrar em conflito com os

requisitos funcionais do projeto, portanto os objetivos de segurança devem ser elaborados em conjunto pela equipe de requisitos e pelos *stakeholders* do projeto.

Esta atividade é composta por reuniões de *"brainstorming"* onde deverão ser definidos quais serão os objetivos de segurança e que os mesmos sejam alinhados com os objetivos de negócio do projeto.

A figura 6, apresenta conceitualmente a hierarquia lógica para o desenvolvimento dos requisitos de segurança do projeto, onde os objetivos de negócio dão origem aos objetivos de segurança que por sua vez darão origem os requisitos de segurança do projeto.

Figura 6 – Hierarquia lógica para desenvolvimento de Requisitos

Fonte - Baseado em Mead, Hough e Stehney (2005)

Uma vez que os objetivos de negócio são identificados, os objetivos de segurança deverão ser estabelecidos consensualmente. Cabe à equipe de requisitos prover suporte aos *stakeholders* para que os objetivos de segurança estabelecidos estejam dentro do escopo do projeto.

3.3.1.1 Equipe de Requisitos de Segurança

A equipe de requisitos deverá ser composta por Engenheiros de Requisitos e Especialistas em Segurança, de forma conjunta com os *stakeholders* do projeto.

3.3.2 Avaliação dos Riscos de Segurança

O propósito da atividade de avaliação de riscos de segurança é identificar possíveis ameaças e vulnerabilidades de origem interna ou externa à corporação que ameacem

o produto, avaliar quais os potenciais danos que esses ataques possam trazer ao sistema e também a corporação como um todo, e qual a probabilidade de que eles possam ocorrer. Com a execução desta atividade, a equipe de requisitos terá maior precisão para dar continuidade as próximas etapas do processo de elaboração dos requisitos de segurança.

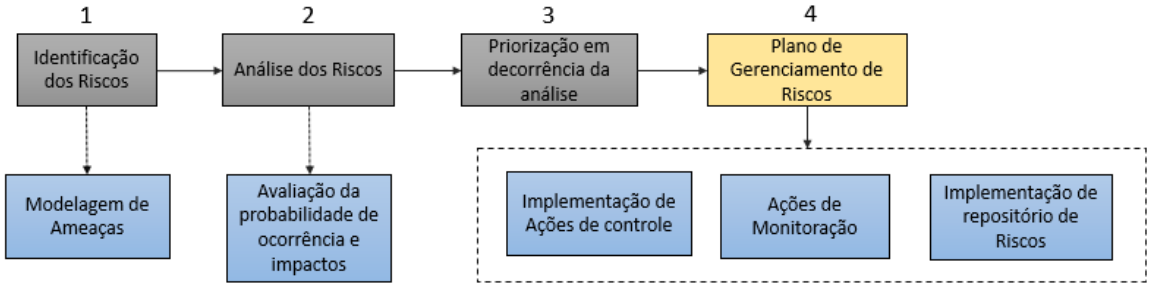
Sem a atividade de avaliação de riscos as empresas não seriam capazes de estabelecer os requisitos de segurança de forma eficaz. A avaliação de riscos também tem como objetivo estabelecer uma linha de priorização para elencar quais os objetivos de segurança, e como os mesmos serão contemplados de acordo com a potencialidade e probabilidade de ocorrência.

Após a identificação das ameaças e vulnerabilidades do projeto, as mesmas deverão ser classificadas como riscos de segurança de acordo com a possibilidade de que elas possam efetivar-se em um ataque, sendo assim, cada risco de segurança posteriormente resultará em um ou mais requisitos de segurança.

Os requisitos de segurança deverão ser categorizados e classificados quanto a cobertura de riscos, dificuldade de implementação e custo relativo do impacto que um potencial ataque pode trazer ao sistema e a corporação.

Na figura 7, apresenta-se a proposta de tarefas para a atividade de avaliação de riscos durante o processo de desenvolvimento de requisitos de segurança fundamentada no método SERA proposto por Alberts, Woody e Dorofee (2014).

Figura 7 – Tarefas para atividade de avaliação de riscos de segurança



Fonte – Baseado em Alberts, Woody e Dorofee (2014).

A atividade de avaliação de riscos de segurança é composta pelas tarefas descritas nas seções a seguir.

3.3.2.1 Identificação dos Riscos

Na tarefa inicial da atividade, os riscos são identificados através do consenso entre a equipe de especialistas de segurança, e os engenheiros de requisitos.

Para esta tarefa, é proposta a identificação de riscos orientada por ameaças, a tarefa tem início com a subtarefa de modelagem de possíveis ameaças que possam ser aplicadas ao software, onde identificam-se as suas possíveis fontes e quais os eventos que podem originá-las. A partir desses cenários de ameaças, são determinadas quais seriam as prováveis vulnerabilidades que permitiriam que essas ameaças se concretizem. As subtarefas que compõe essa tarefa são: Identificação de Riscos, Análise de Riscos, Priorização de Riscos e Plano de Gerenciamento de Riscos, que são detalhadas na sequência.

3.3.2.1.1 Identificação de Ameaças (Fontes e Eventos)

Nesta subtarefa, a equipe de requisitos do projeto devera determinar quais os tipos de ameaças deverão ser considerados durante o processo de avaliação de riscos e qual o nível de detalhamento que deve ser utilizado para descrever esses eventos. Os eventos podem ser descritos em alto nível, utilizando terminologias não técnicas, porém descrevendo táticas, técnicas e procedimentos empregados no evento.

A organização deverá considerar:

- Qual será o conjunto inicial de eventos que serão utilizados como ponto inicial para a identificação de ameaças específicas no processo de avaliação de riscos.
- Qual o grau de confirmação que será demandado para que um evento de ameaça seja considerado como relevante para o processo de avaliação de riscos. (Eventos que já ocorreram / técnicas de *Brainstorming*).

3.3.2.1.2 Fontes de Ameaças

Cabe a equipe de requisitos determinar quais os tipos de fontes serão considerados para a atividade de análise de riscos, deverão ser explicitados os procedimentos

utilizados para identificar as ameaças e quaisquer pressupostos utilizados para tal, a tarefa de avaliação de riscos de segurança deve endereçar todos os tipos de fontes de ameaças, seja uma fonte ampla ou específica. O anexo 1, apresenta uma tabela de taxonomia sugerida por Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002) com as principais fontes de ameaças identificadas.

3.3.2.1.3 Componentes de Ameaça

De acordo com Alberts, Woody e Dorofee (2014), para a construção e documentação de cenários de riscos deverão ser considerados os componentes de ameaça que apoiarão o detalhamento delas com itens que não necessariamente fazem parte do processo de avaliação de riscos. Os componentes de Ameaça são compostos pelos seguintes itens descritos na tabela 3.

Tabela 3 – Componentes de Ameaça de um Risco de Segurança

Componente	**Descrição**
Ameaça	Descrição do evento, que explora uma ou mais vulnerabilidades que leva a uma situação adversa ou perda.
Ator	Quem ou o que está tentando violar o sistema para obter dados críticos
Motivação	Quais são as intenções do Ator que podem ser classificadas como deliberada ou não intencional.
Objetivo	O objetivo final para o qual o ator está aplicando seus esforços.
Resultados	Consequência direta da ameaça (Ex: Divulgação, Modificação, Inserção ou roubo de dados).
Meios	Recursos que o ator utiliza para executar o evento
Complexidade	O grau de dificuldade atribuído a execução da ameaça
Contexto Adicional	Qualquer informação contextual relevante para a ameaça;

Fonte - Baseado em Alberts, Woody e Dorofee (2014)

3.3.2.1.4 Sequência de Atividades da Ameaça

Para a subtarefa de modelagem de ameaças é necessário determinar qual seria a possível sequência de passos envolvidas no evento, essa sequência será utilizada para o desenvolvimento dos cenários de modelagem de ameaças de segurança.

3.3.2.1.5 Identificação de Vulnerabilidades

Identificar as vulnerabilidades através da pré-disposição e condições necessárias para que um evento de ameaça possa resultar em impactos adversos. Cabe a equipe de requisitos de segurança determinar quais os tipos de vulnerabilidades que serão utilizados no processo de avaliação de riscos. Segundo sugerido por Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002) as vulnerabilidades podem ser associadas a sistemas da informação tendo como origem *hardware*, software, *firmware*, controles internos e processos de segurança. A corporação deverá estabelecer as condições de pré-disposição que serão consideradas durante o processo como questões arquiteturais, tecnologias aplicadas e ambiente operacional.

3.3.2.2 Análise dos Riscos

Nesta tarefa, os riscos identificados serão analisados pela equipe de requisitos, de acordo com a probabilidade de que os mesmos ocorram e quais seriam os possíveis impactos que a sua ocorrência possa trazer.

3.3.2.2.1 Detalhamento dos Riscos

A equipe deverá identificar os riscos, através da conversão dos itens levantados nas subtarefas anteriores (Ameaças - 3.3.2.1.2 e Vulnerabilidades – 3.3.2.1.5) em riscos tangíveis, que deverão ser descritos através de narrativas e se possível ilustrados por cenários. A equipe deverá estimar como cada ameaça afetará o fluxo operacional do sistema caso o risco se concretize.

Tabela 4 – Passos para o Detalhamento de um Risco de Segurança

ID	Passo	Descrição	Saída
1	Identificação da Ameaça	A equipe deverá determinar quais as ações/ dados críticos do sistema. Qual seria o processo que o Ator da ameaça se utilizaria para acessar o software utilizando a documentação levantada na fase 1 do processo.	Componentes da Ameaça Sequência de atividades da Ameaça
2	Estabelecer a consequência	Analisar as consequências que as ameaças levantadas na fase 1 podem trazer ao fluxo operacional do sistema, determinar como o software será afetado pela ameaça e que consequências isso implicará.	Consequência no fluxo operacional do Software Consequências para os *Stakeholders*
3	Identificar as vulnerabilidades	Identificar quais as vulnerabilidades que serão exploradas pela ameaça, quais condições e circunstâncias são necessárias para o risco se consolidar.	Vulnerabilidades
4	Desenvolver o cenário de Risco	A equipe documenta a narrativa do cenário de risco baseada nas informações geradas nos passos 1, 2 e 3. A equipe documenta o risco através de um ID e da descrição sucinta do risco para uso nas atividades posteriores.	Cenário de Risco Avaliação do Risco de Segurança

Fonte - Baseado em Alberts, Woody e Dorofee (2014)

3.3.2.2.2 Determinar a probabilidade do risco

A equipe de avaliação de riscos deverá determinar qual a probabilidade que o risco ocorra e gere consequências adversas. Nesta análise, deve-se considerar as características da ameaça como suas fontes para iniciar o evento, vulnerabilidades e pré-condições necessárias para que o evento possa concretizar-se, também deve-se levar em consideração as medidas de segurança implantadas no ambiente operacional para que o evento não ocorra. A tabela 5 apresenta um modelo para avaliação de probabilidade de ocorrência de um risco de segurança.

Tabela 5 – Modelo de Avaliação de Probabilidade de Ocorrência de Riscos de Segurança

Valor Qualitativo	Valores Semi Quantitativos	Descrição
Muito Alto	10	Erro, acidental ou ato premeditado considerado como **quase certeza** de ocorrer, ou ocorrer mais de 100 vezes por ano.
Alto	8	Erro, acidental ou ato premeditado considerado como **muito provável,** de ocorrer, ou ocorrer entre 10 a 100 vezes por ano.
Médio	5	Erro, acidental ou ato premeditado considerado como **provável** de ocorrer, ou ocorrer entre 1 a 10 vezes por ano.
Baixo	2	Erro, acidental ou ato premeditado considerado como **improvável** de ocorrer, ou ocorrer mais de uma vez a cada 10 anos.
Muito Baixo	0	Erro, acidental ou ato premeditado considerado como **muito improvável** de ocorrer, ou ocorrer menos de uma vez a cada 10 anos.

Fonte - baseado em Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002).

3.3.2.2.3 Determinar a magnitude do impacto

A equipe de avaliação de riscos deve determinar o impacto adverso que determinado evento possa ocasionar, considerando-se as características da ameaça e a vulnerabilidade envolvida. A tabela 6 apresenta um modelo para avaliação de impactos de riscos de segurança.

Tabela 6 – Modelo para Avaliação de Impactos de Riscos de Segurança

Valor Qualitativo	Valores Semi Quantitativos	Descrição
Muito Alto	10	O risco tem capacidade de provocar impactos **múltiplos efeitos severos e catastróficos** para as operações da organização, ativos da organização e outras organizações.
Alto	8	O risco tem capacidade de provocar impactos **severos e catastróficos** para as operações da organização, ativos da organização e outras organizações.
Médio	5	O risco tem capacidade de provocar **sérios efeitos adversos** nas operações da organização, ativos da organização, indivíduos e outras organizações.
Baixo	2	O risco tem capacidade de provocar efeitos **adversos limitados** nas operações da organização, ativos da organização, indivíduos e outras organizações.
Muito Baixo	0	O risco tem capacidade de provocar efeitos **adversos negligenciáveis** nas operações da organização, ativos da organização, indivíduos e outras organizações.

Fonte - Baseado em Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002).

3.3.2.3 Priorização dos riscos

A tarefa de priorização dos riscos de segurança é realizada com o apoio de uma matriz considerando a probabilidade de que eles ocorram em relação ao impacto que eles possam ocasionar.

A matriz de riscos determinará quais serão os riscos mais graves (maior probabilidade x maior impacto) e será utilizada como ferramenta para determinar a priorização dos riscos.

Tabela 7, Matriz de avaliação de Riscos (Combinação da Probabilidade x Impacto)

Probabilidade	**Nível de Impacto**				
	Muito Baixo	**Baixo**	**Moderado**	**Alto**	**Muito Alto**
Muito Alta	Muito Baixa	Baixa	**Alta**	**Muito Alta**	**Muito Alta**
Alta	Muito Baixa	Baixa	Moderada	**Alta**	**Muito Alta**
Moderada	Muito Baixa	Baixa	Moderada	Moderada	**Alta**
Baixa	Muito Baixa	Baixa	Baixa	Baixa	Moderada
Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa	Baixa	Baixa

Fonte: Baseado em Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002).

Tabela 8, apresenta a referência de valores para os riscos de segurança, atribuindo-se os maiores valores aos riscos de maior criticidade.

Tabela 8 – Referência de Valores para Riscos de Seguraça

Valor Qualitativo	**Valores Semi Quantitativos**
Muito Alto	10
Alto	8
Moderada	5
Baixo	2
Muito Baixo	0

Fonte: Baseado em Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002).

3.3.2.4 Plano de Gerenciamento de Riscos

A tarefa final da atividade de avaliação de riscos é criar um plano para o gerenciamento de riscos de segurança, com o intuito de auxiliar o estabelecimento de ações de mitigação (que resultarão em requisitos de segurança) e ações de monitoração para o acompanhamento das implementações ao longo do desenvolvimento do projeto, evitando-se que os requisitos identificados sejam distorcidos no decorrer do desenvolvimento do software.

O plano de gerenciamento de riscos também contribuirá para a alimentação de um repositório de riscos de segurança para ser utilizado em avaliações de projetos futuros. O plano de gerenciamento de riscos posteriormente será utilizado como base para elaboração dos testes de validação de segurança.

Sendo assim, o plano de gerenciamento de riscos de segurança deve conter os seguintes itens:

- Implementação de ações para o controle de riscos de segurança
- Monitoração de tratamento dos riscos de segurança
- Alimentação do repositório de riscos de segurança.

3.3.3 Definição dos Requisitos de Segurança

Nesta atividade do processo, os objetivos de segurança levantados pelos *stakeholders* deverão ser convertidos em requisitos de segurança. A equipe de requisitos deverá esabelecer a melhor forma para consolidar esses requisitos através do material gerado durante a avaliação dos riscos de segurança, esta atividade do processo é crucial para o sucesso do ciclo de desenvolvimento seguro, sendo que o maior desafio é estabelecer requisitos consistentes e objetivos, possíveis de serem implementados e posteriormente avaliados (que não sejam vagos ou ambíguos), sendo assim, cada requisito estabelecido deverá permitir que os mesmos sejam de passíveis de verificação na medida que o projeto é implementado.

Para iniciar o levantamento dos requisitos é proposto o método de *workshop* com reuniões estruturadas, pois neste estágio do processo, considera-se que já foram estabelecidos os parâmetros de comunicação entre os membros da equipe que facilitam a compreensão das necessidades de segurança do projeto.

Como ponto de partida, com o conteúdo gerado na atividade de análise de riscos de segurança é proposto que a equipe de requisitos participe de reuniões conjuntas de *brainstorming* sobre os riscos elencados, desta forma a equipe deverá estabelecer requisitos de segurança que minimizem a ocorrência dos riscos levantados.

A matriz de avaliação de riscos, fornecerá para a equipe de requisitos os riscos levantados e o grau de criticidade de cada um deles. A partir desse ponto, caberá aos engenheiros de requisitos e os especialistas em segurança dirigir o processo de *brainstorming* para que o foco das discussões esteja nos riscos que foram considerados como os de maior criticidade.

Ao término desta atividade a equipe deverá incorporar a documentação um conjunto de requisitos de segurança.

3.3.4 Categorização dos Requisitos de Segurança

O objetivo desta atividade do processo é que os requisitos desenvolvidos sejam agrupados em categorias específicas. Usualmente requisitos de software são categorizados como funcionais (onde especificam características comportamentais do sistema) e não funcionais, que especificam atributos. Entretanto, segundo Ross Ron, McEvilley Michael e Carrier Oren, Janet (2016) os requisitos de segurança podem ser classificados em três categorias distintas.

3.3.4.1 Requisitos de Segurança Funcionais

Especifica características funcionais de proteção do sistema.

3.3.4.2 Requisitos de Segurança Não Funcionais

Especifica características comportamentais de segurança e desempenho.

3.3.4.3 Requisitos de Confiabilidade de Segurança

Essa categoria de requisitos especifica técnicas e métodos utilizados na construção do software que possibilitem a aferição da correta implementação dos requisitos funcionais e não funcionais do sistema.

A categorização dos requisitos permitirá o balanceamento entre as três características possibilitando maior visibilidade no processo de priorização e validação. Ao término desta etapa a equipe de requisitos deverá incorporar na documentação os requisitos agrupados nas suas respectivas categorias.

3.3.5 Priorização dos Requisitos de Segurança

Provavelmente não será possível atender a todos os requisitos especificados devido a indisponibilidade de tempo e de recursos, desta forma cabe a equipe de requisitos do projeto entrar em consenso e priorizar quais dos requisitos de segurança deverão ser atendidos e em qual ordem de prioridade. Mais uma vez deve-se levar em consideração a associação dos requisitos elaborados com a matriz de avaliação de riscos (elaboradas nas atividades 3 e 4 do processo) uma vez que os riscos remetem as ameaças que o software será exposto.

A priorização dos requisitos pode variar de acordo com a complexidade do projeto em questão, diversos autores propõem diferentes metodologias para a priorização de requisitos, para o presente trabalho foi escolhida, uma forma simples, mas eficaz de priorização através de análise de benefícios de implementação, onde entende-se por benefícios, a capacidade de mitigar os riscos de segurança que a implantação de determinado requisito trará ao projeto.

A tabela 8 apresenta uma matriz onde é mapeada a cobertura de riscos de segurança pelos requisitos. Como forma de auxiliar na priorização dos requisitos a proposta é atribuir pesos através de um fator de multiplicação por cada risco coberto.
O fator de multiplicação é dado pela tabela de avaliação de impactos (Tabela 6) que atribui uma nota a cada item de acordo com sua magnitude de impacto determinada.

Tabela 8, Matriz de Mapeamento de Cobertura de Riscos de Segurança pelos Requisitos de Segurança

Requisitos	**Riscos Mitigados**					
	R1x10	R2x8	R3x5	R4x2	R5x2	Total
RS 1	**10**		**5**			**15**
RS 2	**10**			**2**		**12**
RS 3		**8**	**5**			**13**
RS 4				**2**	**2**	**4**

RS 5		**8**				**8**

Fonte - Autor

A matriz propõe a classificação dos requisitos através da associação de cada um deles aos riscos levantados. Para cada risco coberto por um requisito avaliado, atribui-se um peso baseado na tabela 6. A coluna “Total” da tabela 8, apresenta a somatória dos pontos atribuídos para cada requisito, essa pontuação será utilizada como forma de priorização. Cada requisito pode ser associado a um ou mais riscos, e cada risco poerá ser associado a mais de um requisito.

Esta análise deve ser produzida pela equipe de requisitos e a decisão final deverá ser de comum acordo entre todos os membros da equipe.

É possível que alguns dos requisitos de segurança sejam inviáveis de serem contemplados (devido a questões de tecnologia empregada, tempo de desenvolvimento ou recursos necessários), desta forma, cabe a equipe definir em conjunto se o requisito será anulado ou se o mesmo será incluído em implementações futuras.

A tabela 9 apresenta a classificação dos requisitos de segurança após a priorização de acordo com a pontuação atingida por cada um deles, referenciando a matriz de cobertura de riscos.

Tabela 9, Classificação dos Requisitos de Segurança

Requisito	**Pontuação**
RS 1	15
RS 2	13
RS 3	12
RS 4	8
RS 5	4

Fonte - Autor

3.3.6 Validação dos Requisitos de Segurança

Esta atividade consiste em validar se os requisitos desenvolvidos são consistentes, precisos e possíveis de serem validados durante o processo de validação de segurança software. O objetivo desta atividade do processo é encontrar defeitos nos requisitos estabelecidos, como ambiguidades, inconsistências ou possíveis falhas de conceito.

Ao final desta atividade, todos os requisitos de segurança levantados deverão ser validados pela equipe de requisitos do projeto.

A tabela 11 propõe uma matriz para análise e validação de cada requisito de segurança, onde eles devem ser analisados de acordo com a sua validade e exemplifica propostas para sua validação.

Tabela 11, Matriz de Análise e Validação de Requisitos de Segurança

Requisito	**Validade**	**Como validar**
RS 1	SIM	Implementando teste de *replay* de mensagens
RS 2	SIM	Dados do *Buffer* de Saída devem estar criptografados
RS 3	SIM	Validação da autenticação de Usuário e Senha
RS 4	SIM	Validar Aleatoriedade dos dados enviados
RS 5	SIM	Validar autenticação entre os componentes do sistema.

Fonte: Autor

Ao final das atividades que integram o processo de desenvolvimento de requisitos de segurança, a equipe de requisitos está habilitada a concluir o documento final de requisitos de segurança do projeto.

3.4 Considerações do Capítulo

O capitulo apresentou um processo para o desenvolvimento de requisitos de segurança para software, utilizando como base, técnicas de avaliação de riscos, onde os mesmos são levantados através de um processo de modelagem de cenários orientados por ameaças. Uma vez que os riscos de segurança são estabelecidos, eles deverão ser avaliados em relação ao grau de criticidade e a possibilidade de que ele venha a ocorrer.

Com o processo de avaliação de riscos proposto, a equipe terá mais precisão para o levantamento dos requisitos de segurança, uma vez que os riscos são considerados como ponto central do processo de levantamento de requisitos, através de técnicas de *brainstorming* em reuniões executadas entre os membros da equipe.

Após levantar os requisitos, a equipe deve classificá-los (em funcionais, não funcionais e de confiabilidade) e priorizá-los, de acordo com a abrangência de cada um deles sobre a matriz de riscos.

Por fim, os requisitos de segurança devem ser validados quanto a sua consistência e capacidade de implementação. Para cada requisito proposto, deve-se apresentar uma metodologia de validação, que posteriormente será utilizada para validá-lo.

Ao término do processo, o Documento de Requisitos de Segurança deverá ser preenchido para utilização como ponto de partida para as próximas etapas do processo de Requisitos de segurança para software seguro.

O Anexo apresenta um modelo para o Documento de Requisitos de Segurança do projeto.

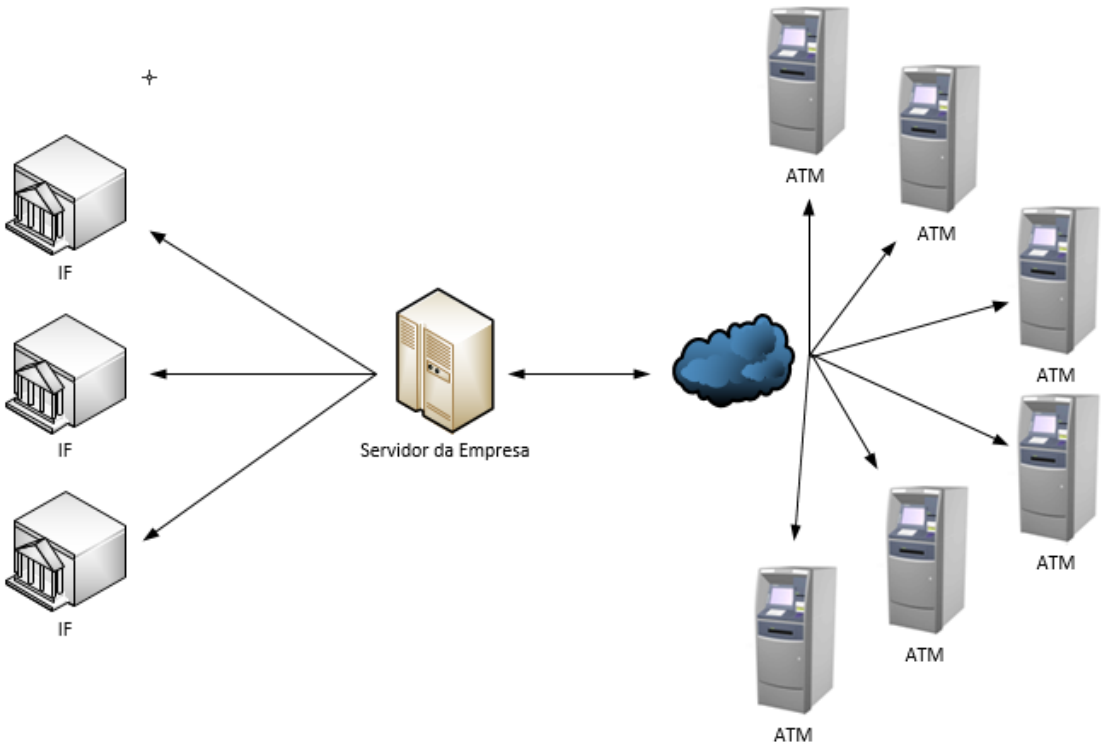
4. APLICAÇÃO DO PROCESSO DE REQUISITOS DE SEGURANÇA

Este capítulo apresenta uma aplicação do processo de desenvolvimento de requisitos de segurança apresentado no capítulo 3, aplicado em um projeto de desenvolvimento de software seguro.

4.1 Empresa

A empresa onde realizou-se o caso de estudo é de origem brasileira, atua na área de tecnologia da informação, fornecendo soluções de redes para meios de transações eletrônicas, por razões de confidencialidade o nome do real da empresa será omitido. A Figura 8 apresenta uma visão geral da rede de autoatendimento da empresa.

Figura 8, Visão geral da rede de terminais.



Fonte - Autor

Pela razão do negócio e área de atuação da empresa é necessário que toda a informação processada, armazenada e transmitida deve ser protegida, pois em diversos casos dependendo da localização geográfica a transmissão de dados ocorre por meio de redes terceirizadas.

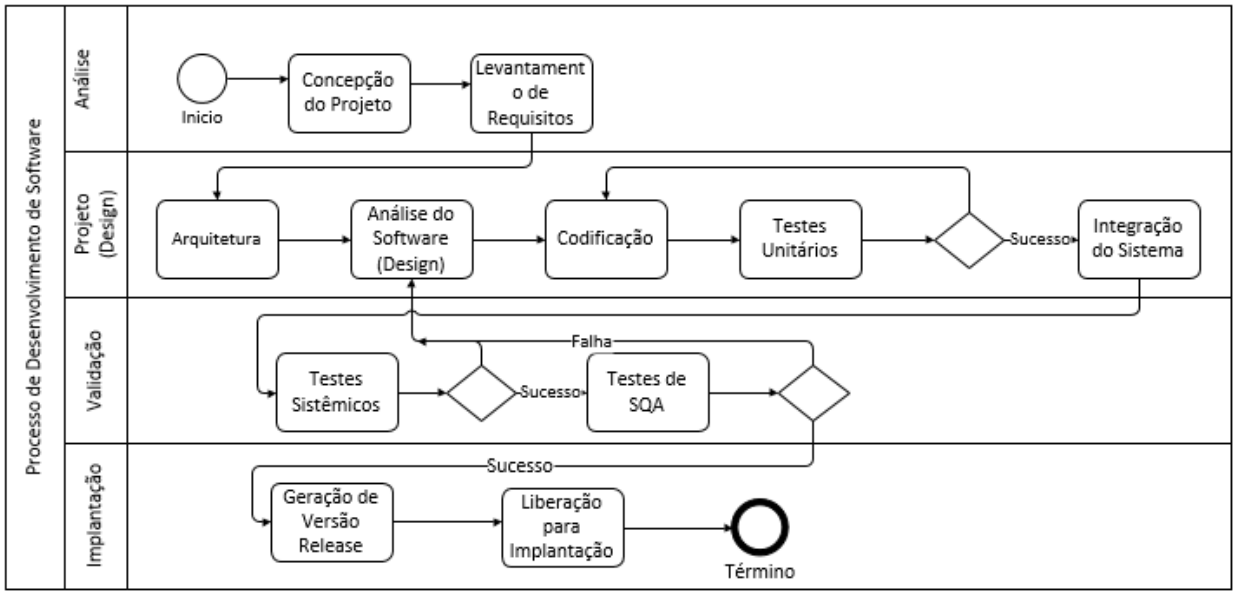
4.2 Cenário Atual

A empresa possui uma grande área de desenvolvimento de software contando com uma equipe com mais de 80 profissionais dedicados a atividades de Engenharia de Requisitos, Arquitetura, Design, Programadores e Analistas de Testes. As equipes são compostas por profissionais contratados pela própria empresa e terceiros.

O processo de desenvolvimento de software praticado é bem definido e documentado, possuindo sistemas de controle para o acompanhamento das tarefas.

O ciclo de desenvolvimento adotado é uma variação do modelo cascata, com múltiplas interações conforme é descrito no diagrama representado pela figura 9.

Figura 9, Processo de desenvolvimento de software atual



Fonte: Autor

Conforme é possível verificar no processo representado pela figura 9, o modelo de desenvolvimento de software adotado utiliza uma abordagem tradicional que não contempla atividades de segurança durante do processo de desenvolvimento.
Apesar das questões relativas à segurança representam as maiores ameaças os negócios da companhia, práticas de implementação de segurança não eram considerados fundamentais para a empresa, projetos considerados críticos eram submetidos apenas a validações contando com testes de penetração ao final do ciclo.

Em diversas situações, problemas de segurança eram identificados somente ao termino do projeto ou quando a empresa contabilizava prejuízos mediante a ocorrências de ataques.

A correção de falhas de segurança identificadas nos testes de penetração ou em fraudes são extremamente custosas e demoradas, uma vez que essas vulnerabilidades não foram previstas durante o desenvolvimento, essas correções também eram realizadas de forma não fundamentada, o que acarretava em novas vulnerabilidades e ataques.

4.2.1 Equipe de Segurança Lógica

Com o intuito de reduzir os prejuízos decorrentes de ataques nos seus sistemas transacionais, a empresa decidiu criar uma equipe de segurança lógica que inicialmente era voltada para identificação de ameaças e pronta reação a eventos de ataques lógicos aos seus sistemas. A equipe de segurança foi idealizada sob uma nova superintendência, separada da área de desenvolvimento de software para que não ocorressem conflitos de interesse dentro da mesma área.

Atualmente a equipe multidisciplinar e é formada por profissionais especializados em diversas áreas que envolvem os serviços prestados pela empresa tais como; Engenheiros de Hardware, Desenvolvedores de Software, Engenheiros de Sistema de Redes e profissionais de Tecnologia da Informação.

Inicialmente a equipe desenvolveu e implementou sistemas de proteções na infraestrutura, adotando políticas de configuração, softwares de monitoração e escaneamento além de processos de validação de segurança aplicados a todos os sistemas desenvolvidos pela área de desenvolvimento de software.

4.3 Ciclo de Desenvolvimento de Software Seguro

O ciclo de desenvolvimento seguro passou a ser considerado pela empresa após a implementação dos mecanismos iniciais para aumentar a segurança dos sistemas da companhia e reduzir os custos de manutenção decorrentes de falhas de segurança encontradas ao término do processo de desenvolvimento.

4.4 Aplicação da Proposta

A proposta de aplicação de um processo para o desenvolvimento de requisitos de segurança através de análise de riscos situa-se na fase 1 do plano de implementação do ciclo de desenvolvimento de software seguro adotado pela empresa, que é o objeto do estudo do presente trabalho.

4.4.1 O projeto

A proposta foi aplicada inicialmente em um projeto de desenvolvimento de software para um sistema que demanda proteção de dados e autenticação entre módulos através de comprovação de credenciais, para estabelecimento de sessão segura entre os componentes de diferentes sistemas.
Os sistemas integrados operam em diferentes ambientes operacionais:

- Sistema de interface com o cliente – plataforma instalada em terminais de campo.
- Sistema de autenticação de plataforma – Servidores.
- Sistema de autenticação de transações – Servidor de Instituições financeiras.

4.4.1.1 Definição da Equipe de Requisitos

A definição da equipe foi feita mediante as características do projeto, por tratar-se de um projeto interno da empresa, todos os envolvidos no processo eram funcionários da própria empresa, a equipe foi definida da seguinte forma:

- Um Engenheiro de Requisitos
- Um Especialista da equipe de desenvolvimento
- Dois Especialistas de Segurança

Os *stakeholders* do projeto também eram representantes da equipe de Operações (área patrocinadora do projeto), sendo que foram nomeados os seguintes representantes:

- Um Gerente de Operações.
- Um Especialista em Implantação de sistema.

- Um Especialista de negócios.

4.4.2 - Levantamento dos Objetivos de Segurança do Software

Esta atividade do processo consiste no levantamento dos objetivos de segurança do projeto aderentes aos objetivos de negócio. Para esta atividade, foi agendada uma reunião inicial onde o escopo do projeto foi discutido entre a equipe. Por se tratar de uma equipe com conhecimentos homogêneos, pois todos os integrantes são funcionários da empresa, todos estavam alinhados em relação aos objetivos de negócio da empresa e também possuem conhecimentos equivalentes dos processos internos, fato que facilitou o estabelecimento de uma linguagem única e objetiva.

Esta atividade foi concluída em apenas duas reuniões de *brainstorming*, sendo que na primeira reunião foram levantados todos os objetivos de negócio e todos os objetivos de segurança. Na segunda reunião, a equipe revisou e refinou os objetivos levantados.

Tabela 12, Levantamento dos objetivos de negócio do projeto

ON-1	Disponibilidade - O sistema deverá permanecer disponível sempre que for demandado (disponibilidade 24 x 7)
ON-2	Eficiência - Os dados trafegados devem ser íntegros evitando, que ocorram erros em transações otimizando a disponibilidade do sistema
ON-3	Custo – O novo sistema deverá demandar menos manutenções que o sistema atual

Fonte: Autor

Tabela 13, Levantamento dos objetivos de Segurança

ON-1	OS -1	O sistema deverá permanecer disponível sempre que for demandado (disponibilidade 24 x 7)
ON-2	OS- 2	A privacidade dos dados dos clientes do sistema deve ser preservada a todo custo (Identidades, conteúdo de cartões e senhas).
ON-2	OS-3	Todos os dados referentes a transações devem ser protegidos
ON-3	OS-4	O sistema deve ser robusto e resiliente a ocorrência de fraudes conhecidas

Fonte: Autor

4.4.3 Avaliação de Riscos

Com base nos objetivos de segurança levantados iniciou-se a segunda atividade do desenvolvimento dos requisitos de segurança, essa nova atividade voltada a avaliação dos riscos de segurança envolvidos no projeto.

4.4.3.1 Identificação de ameaças

A primeira tarefa, identificação das ameaças foi o foco da primeira reunião de brainstorming da equipe, como ponto de partida utilizou-se os objetivos de segurança levantados na primeira atividade do processo como referência. Diagramas de caso de uso, previamente levantados pelos engenheiros de requisitos também foram utilizados como recurso para o desenvolvimento desta atividade. ATabela 14, apresenta o levantamento de ameaças de segurança identificadas.

Tabela 14 Ameaças Levantadas

ID	Fonte	Eventos
A1	Externa	Atacante captura dados transmitidos em transações com o intuito de clonagem dos dados dos clientes – "*man in the middle*"
A2	Externa	Atacante captura dados transmitidos em transações com o intuito de adulterá-los – " *man in the middle*"
A3	Interna	Atacante instala software malicioso no servidor da empresa com o intuito de adulterá-los
A4	Externa	Atacante substitui terminais de autoatendimento por aparelhos manipulados com inseminação de software malicioso que capture os dados dos clientes, ou manipule dados de uma transação.
A5	Externa	Atacante obtém acesso indevido aos servidores da companhia com o intuito de manipular os dados de transações
A6	Interna	Atacante acessa os bancos de dados da empresa para captura de dados dos clientes
A7	Interna	Atacante insere código malicioso no sistema, com o intuito de criação de um "*backdoor*" no sistema desenvolvido
A8	Externa	Atacante manipula terminal de autoatendimento com o intuito de vasculhar possíveis falhas de implementação. (Busca por fragilidades)

Fonte: Autor

4.4.3.1.1 Detalhamento das ameaças

Após o levantamento das possíveis ameaças ao sistema a equipe efetuou um refinamento dos itens levantados, através do detalhamento conforme descrito na sequência.

Para fins de detalhamento no trabalho, foi escolhida a ameaça A5, com os seus componentes detalhados na tabela 15.

Tabela 15, Detalhamento dos Elementos de uma Ameaça de Segurança

Componente	**Descrição**
Ameaça	A5 - Captura dados transmitidos em transações com o intuito de adulterá-los – *" man in the middle"*
Ator	Atacante Externo
Motivação	Captura de dados referentes a transações, com o intuito de adultera-los para modificação de valores envolvidos,
Objetivo	Manipulação de dados de uma transação de saque, solicitação de um valor elevado (maior que o solicitado pelo cliente real) dados são capturados antes de serem enviados para a IF. Após autorização da IF, resposta é manipulada para o valor original do Saque. Fraudador desvia valor excedente.
Resultados	Modificação de dados de uma transação
Meios	Inserção de código malicioso no servidor da empresa para manipular dados de transações.
Complexidade	Elevada, uma vez que o atacante necessita conhecer os protocolos de transmissão, acesso ao sistema da empresa.
Contexto Adicional	Não há.

Fonte: Autor

4.4.3.1.2 - Sequência de Atividades da Ameaça

Consiste em elaborar para cada uma das ameaças levantadas, qual seria uma possível sequência de atividades necessárias para a consolidação da ameaça, essa sequência de atividades é demonstrada para a mesma ameaça (A5) na tabela 16.

Tabela 16, Sequencia de Atividades de uma Ameaça

Passo	**Descrição**
1	Atacante consegue acesso as dependências da empresa para acesso a rede interna.

	Esta tarefa requer um componente de engenharia social para conseguir acesso privilegiado. Pode-se considerar que um funcionário da empresa, com credenciais de acesso faça a inserção do software malicioso.
2	Atacante consegue *login* no servidor da empresa
3	Software malicioso é instalado no servidor – A partir desse ponto o processo é automatizado, determinadas transações são interceptadas de forma aleatória para manipulação de dados.
4	Software malicioso redireciona quantia " a maior" autorizada pela IF para conta escolhida para receptação de valores.
5	Atacante monitora conta de recepção para efetuar transações de transferência.

Fonte: Autor

A sequência de passos efetuadas para análise da ameaça em questão foi realizada para todas as ameaças levantadas.

4.4.3.1.3 Identificação de vulnerabilidades

A segunda tarefa, consiste na identificação de vulnerabilidades, que são pré-disposições encontradas no sistema para que as ameaças se tornem concretas. A equipe de requisitos de segurança deve estabelecer quais serão as possíveis vulnerabilidades associadas a cada ameaça levantada.

Para fins de detalhamento do trabalho serão elencadas as vulnerabilidades levantadas para a ameaça A1, demonstrados na tabela 17;

Tabela 17, Tabela de Vulnerabilidades ligadas a Ameaça 1

ID	**Fonte**	**Vulnerabilidades**
A1	Externa	- Ausência de criptografia nas mensagens trocadas entre terminal e servidor - Ausência/Falha processo de autenticação de mensagens. - Ausência/Falha de mecanismo de atualização de chaves de criptografia. - Ausência/Falha de componente randômico para evitar repetição de criptogramas. - Ausência/Falha de mecanismos de restrição ao acesso do servidor com duplo fator de autenticação. - Ausência/Falha de mecanismos de proteção contra-ataques de força bruta.

Fonte - Autor

A sequência de passos efetuadas para a identificação de vulnerabilidades para a ameaça em questão foi realizada para todas as ameaças levantadas.

4.4.3.2 Análise dos riscos

A terceira tarefa foi dividida em três passos, compostos pelas seguintes subtarefas;

4.4.3.2.1 Análise de probabilidade

Com base na experiência da equipe, e histórico de ataques, foi atribuída a seguinte graduação aos riscos levantados. A tabela 18 apresenta a análise de probabilidade dos riscos do projeto, onde as oito ameaçãs de segurança levantados gerarm oito riscos de segurança.

Tabela 18 – Análise de Probabilidade de Riscos do Projeto

ID	**Eventos**	**Probabilidade**
R1	Atacante captura dados transmitidos em transações com o intuito de clonagem dos dados dos clientes – "*man in the middle*"	Muito Alto
R2	Atacante captura dados transmitidos em transações com o intuito de adulterá-los – " *man in the middle*"	Moderado
R3	Atacante instala software malicioso no servidor da empresa com o intuito de adulterá-los	Moderado
R4	Atacante substitui terminais de autoatendimento por aparelhos manipulados com inseminação de software malicioso que capture os dados dos clientes, ou que prove que transações inexistentes.	Alto
R5	Acesso indevido aos servidores da companhia com o intuito de manipular os dados de transações	Alto
R6	Atacante acessa os bancos de dados da empresa para captura de dados dos clientes	Baixo
R7	Código malicioso é inserido no sistema, com o intuito de criação de um "*backdoor*" no sistema desenvolvido	Baixo
R8	Atacante manipula terminal de autoatendimento com o intuito de vasculhar possíveis falhas de implementação. (Busca por fragilidades)	Muito Alto

Fonte: Autor

4.4.3.2.2 Determinar a magnitude dos impactos dos riscos

Com base na experiência da equipe, e histórico de ataques, foi atribuída a seguinte graduação aos riscos levantados. A tabela 19 apresenta a análise de magnitude de impacto dos riscos de segurança.

Tabela 19 – Análise de Impactos dos Riscos de Seguraça

ID	Eventos	Impacto
R1	Atacante captura dados transmitidos em transações com o intuito de clonagem dos dados dos clientes – "*man in the middle*"	Moderado
R2	Atacante captura dados transmitidos em transações com o intuito de adulterá-los – " *man in the middle*"	Moderado
R3	Atacante instala software malicioso no servidor da empresa com o intuito de adulterá-los	Moderado
R4	Atacante substitui terminais de autoatendimento por aparelhos manipulados com inseminação de software malicioso que capture os dados dos clientes, ou que prove que transações inexistentes.	Moderado
R5	Acesso indevido aos servidores da companhia com o intuito de manipular os dados de transações	Alto
R6	Atacante acessa os bancos de dados da empresa para captura de dados dos clientes	Alto
R7	Código malicioso é inserido no sistema, com o intuito de criação de um "backdoor" no sistema desenvolvido	Muito Alto
R8	Atacante manipula terminal de autoatendimento com o intuito de vasculhar possíveis falhas de implementação. (Busca por fragilidades)	Muito Alto

Fonte - Autor

4.4.3.2.3 Priorização dos Riscos de Segurança

A partir da graduação atribuída para a probabilidade de ocorrência em função da severidade do impacto causado por cada risco de segurança, chegou-se a seguinte matriz para priorização dos riscos. A tabela 20 apresenta a matriz de priorização de riscos de segurança.

Tabela 20, Matriz de Priorização dos Riscos de Segurança

Probabilidade	**Nível de Impacto**				
	Muito Baixa	**Baixa**	**Moderada**	**Alta**	**Muito Alta**
Muito Alta	-	-	R1	**-**	**R8**
Alta	-	-	R4	**R5**	**-**
Moderada	-	-	R2, R3	-	**R7**
Baixa	-	-	-	R6	-
Muito Baixa	-	-	-	-	-

Fonte: Autor

O preenchimento da matriz de priorização de riscos proporcionou a equipe de requisitos de segurança determinar a prioridade dos riscos, permitindo que os riscos fossem classificados através do método de pontuação proposto na tabela 22, onde se atribuindo valores de referência a cada um deles conforme o seu posicionamento na matriz. A tabela 21 apresenta a Prioridade dos Riscos de Segurança.

Tabela 21, Prioridade dos Riscos de Segurança

Posição	**Eventos**	**Classificação da Prioridade**
1°	R8	10
2°	R7, R1 e R5	8
3°	R6, R4	5
4°	R2 e R3	2

Fonte - Autor

4.4.3.3 Elaboração de um plano de gerenciamento de riscos.

A quarta e última tarefa referente a atividade de avaliação de riscos, foi a elaboração de um plano para gerenciamento de riscos. Para esse plano foi elaborado uma planilha contendo a descrição de cada risco levantado, com as vulnerabilidades referentes a cada um deles elencadas. O artefato será usado como referência para acompanhamento das próximas fases do projeto pela equipe de segurança em conjunto com o gerente do projeto. A tabela 22 apresenta uma proposta o gerenciamento de riscos de segurança.

Tabela 22, Proposta para Gerenciamento de Riscos de Segurança

Riscos					
ID	**Prioridade**	**Ações**	**Entrada (Operações)**	**Status**	**Resultado**
R8	10	Elaborar Requisitos para tratar o problema	Implementação de RS4, RS7	Análise	N.OK
R7	8	Elaborar Requisitos para tratar o problema	Implementação de RS5, RS6, RS9	Análise	N.OK

Fonte - Autor

4.4.4 Desenvolvimento de Requisitos de Segurança

A atividade de desenvolvimento dos requisitos de segurança foi executada através de reuniões de *brainstorning* realizadas entre os membros da equipe de requisitos. Os requisitos de segurança foram elaborados orientando-se pelos os riscos levantados na atividade 4.4.3 (Avaliação de Riscos). Durante as reuniões de *brainstorming* surgiram requisitos que não estavam ligados a nenhum dos riscos, porém, através do consenso dos membros da equipe eles foram adicionados ao projeto. Ao longo de duas reuniões, foram levantados os seguintes requisitos de segurança para o projeto. A tabela 23, Lista de requisitos de segurança do projeto.

Tabela 23, Requisitos de Seguraça do Projeto

ID	**Descrição**
RS-1	Todos as mensagens transmitidas pelo sistema devem ser criptografadas utilizando-se o algoritmo – AES 256.
RS-2	O sistema deverá identificar, autenticar e registrar todas as tentativas de acesso ao sistema.
RS-3	Toda informação armazenada nos bancos de dados dos servidores e nos terminais deverá ser mantida em containers criptografados.
RS-4	Todos os terminais que fizerem parte do sistema deverão ser autenticados previamente em ambiente seguro com o servidor da empresa.
RS-5	Todos os componentes de software do sistema deverão ser assinados, permitindo-se que apenas componentes certificados e assinados possam ser executados.
RS-6	Todos os componentes de software passiveis de atualização deverão ser previamente assinados no servidor.
RS-7	O sistema deverá possuir um canal de gerenciamento de terminais, onde será possível auditar o software em execução.
RS-8	O sistema deverá possuir *backup* dos dados do servidor em ambiente protegido

RS-9	O sistema deverá permitir operação com funcionalidades reduzidas em caso de suspeita de incidente. Gerar alerta de suspeita de ataque ao administrador do sistema.

Fonte: Autor

4.4.5 Categorização dos Requisitos de Segurança

A atividade de categorização dos requisitos foi feita mediante a análise dos requisitos levantados, os requisitos foram categorizados em Requisitos de Segurança Funcionais, Não Funcionais e de Confiabilidade, conforme demonstrado na tabela 24.

Tabela 24, Categorização dos Requisitos de Segurança

Requisitos de Segurança Funcionais	**Requisitos de Segurança Não Funcionais**	**Requisitos de Segurança de Confiabilidade**
RS1, RS2, RS4, RS9	RS3, RS8	RS5, RS6, RS7

Fonte: Autor

4.4.6 Priorização dos Requisitos de Segurança em Função dos Riscos

A atividade priorização de requisitos de segurança foi feita mediante a conexão dos requisitos em relação aos riscos levantados. Atribuindo-se pesos aos riscos conforme resultado da *tarefa* 4.4.3 (Avaliação de Riscos), onde os riscos foram priorizados, a matriz de priorização de requisitos de segurança mostra como os riscos foram atendidos A tabela 25 apresenta a Matriz de Cobertura de riscos de segurança pelos requisitos de segurança do projeto.

Tabela 25, Matriz de Cobertura de Riscos de Segurança

Requisitos	**Riscos Mitigados**								**Total Pontos**	**Classificação**
	R1	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**		
Peso:	[5]	[2]	[2]	[2]	[8]	[5]	[8]	[10]		
RS1	**5**	**2**							**7**	**6º**
RS2			**2**		**8**				**10**	**4º**
RS3			**2**			**5**			**7**	**6º**
RS4				**2**				**10**	**12**	**3º**
RS5			**2**				**8**		**10**	**4º**
RS6							**8**		**8**	**8º**

RS7			**2**				**8**	**10**	**20**	**1º**
RS8						**5**			**5**	**9º**
RS9				**2**	**8**		**8**		**18**	**2º**

Fonte: Autor

Com o preenchimento da matriz, verifica-se a cobertura dos riscos em função dos requisitos de segurança desenvolvidos. Para priorizar cada requisito, foram utilizados como fator de multiplicação os pesos atribuídos a cada risco em função de sua criticidade.

A priorização de requisitos de segurança foi feita mediante a conexão dos requisitos em relação aos riscos levantados. Atribuindo-se pesos aos riscos conforme resultado da tarefa 4.4.3, onde os riscos foram priorizados. A matriz de priorização de requisitos de segurança mostra como os riscos foram atendidos. A somatória dos pontos define a priorização dos requisitos.

4.4.7 Validação dos Requisitos de Segurança

A atividade de validação tem como objetivo verificar a consistência dos requisitos elaborados e como eles deverão ser avaliados após a sua implantação. A planilha de validação de requisitos de segurança deverá ser empregada em fases futuras como referência para a fase de validação de segurança ao término do projeto.

A tabela 26 apresenta o resultado da validação dos requisitos de segurança e propõe uma técnica ou procedimento para validar a implementação de cada um deles.

Tabela 26 – Validação dos Requisitos de Segurança

Requisitos	**Validação do Requisito**	
	Viabilidade Técnica	**Procedimento de Validação**
Todos as mensagens transmitidas pelo sistema devem ser criptografadas utilizando-se o algoritmo – AES 256.	**SIM**	A verificação consiste em analisar a troca de mensagens capturando-se os pacotes enviados entre os sistemas. Mensagens com o mesmo conteúdo devem apresentar criptogramas diferentes.

O sistema deverá identificar, autenticar e registrar todas as tentativas de acesso ao sistema.	**SIM**	Verificação de logs de autenticação de usuários, todas as tentativas (sucesso ou não) devem ser registradas.
Todos os terminais que fizerem parte do sistema deverão ser autenticados previamente em ambiente seguro com o servidor da empresa.	**SIM**	A validação consiste na impossibilidade de realizar a leitura dos dados armazenados.
Atacante substitui terminais de autoatendimento por aparelhos manipulados com inseminação de software malicioso que capture os dados dos clientes, ou que prove que transações inexistentes.	**SIM**	Servidor deverá barrar terminal sem autenticação prévia de se conectarem na rede da empresa. Sistema deve apresentar registro de tentativa de conexão de terminal não autenticado.
Todos os componentes de software do sistema deverão ser assinados, permitindo-se que apenas componentes certificados e assinados possam ser executados.	**SIM**	Validação ocorre com a geração de componente sem assinatura. Sistema deverá rejeitar módulo sem assinatura, terminal deverá ficar inoperante.
Todos os componentes de software passiveis de atualização deverão ser previamente assinados no servidor.	**SIM**	Efetuar tentativa de *upgrade* de componente de software sem assinatura de validação no servidor. Software do terminal deverá rejeitar a atualização
O sistema deverá possuir um canal de gerenciamento de terminais, onde será possível auditar o software em execução.	**SIM**	A auditoria deverá ocorrer através de componente que permita acesso remoto ao sistema.
O sistema deverá possuir *backup* dos dados do servidor em ambiente protegido	**SIM**	Validação de *backup* deve ser feita através de comparação entre *hash* do conteúdo dos contêineres operacionais e de *backup*. Os conteúdos dos dados armazenados devem ser inacessíveis aos usuários uma vez que o mesmo deve ser criptografado.

O sistema deverá permitir operação com funcionalidades reduzidas em caso de suspeita de incidente. Gerar alerta de suspeita de ataque ao administrador do sistema.	**SIM**	Sistema deverá se proteger de tentativas de fraudes, uma vez detectada suspeita de ataque sistema deverá reduzir suas funcionalidades.

Fonte: Autor

4.5 Considerações do Capítulo

Neste capítulo foi apresentada a aplicação do processo de desenvolvimento de requisitos de segurança para um projeto de desenvolvimento de software seguro.

A aplicação do processo ocorreu em um projeto interno da empresa e de pequeno porte, porém de elevada criticidade, o que demandou um alto grau de confiabilidade. Durante o experimento, constatou-se a necessidade de implementar melhorias no processo para que o mesmo se torne parte do ciclo de desenvolvimento de software seguro da empresa.

A proposta para adoção de um processo de desenvolvimento seguro foi bem recebida pela liderança da área, uma vez que existe uma lacuna entre as questões de segurança e a metodologia adotada no processo de desenvolvimento de software dentro da companhia, causando conflitos e desgastes.

A proposta de modificação no ciclo habitual de desenvolvimento de requisitos gerou resistências por parte da equipe de desenvolvimento de software, uma vez que os retornos sob o investimento em atividades de segurança ao longo do projeto seriam intangíveis, aumentando o tempo de desenvolvimento e consequentemente o custo do projeto.

Para que o procecesso de desenvolvimento de requisitos de segurança torne-se eficaz e parte de um ciclo de desenvolvimento de software seguro, é fundamental que a corporação adote um processo de desenvolvimento seguro, onde politicas de segurança da informação devem ser estabelecidas e implementadas para a proteção dos artefatos gerados ao longo do projeto. Tal processo pode torna-se eficaz tanto

para softwares que necessitam de características de segurança para a sua operação como para softwares desenvolvidos sob o ciclo de desenvolvimento tradicional.

Com o término do processo, constatou-se que os requisitos de segurança foram estabelecidos de forma consistente, através da análise de diversos cenários de ameaças e vulnerabilidades que não seriam abordados em um ciclo de desenvolvimento padrão o que permitiu maior consistência nos requisitos levantados, fundamentados em ameaças reais já enfrentadas pela empresa e que usualmente não seriam explorados.

Mesmo enfrentando diversos problemas ao longo da implementação do processo, devido a falta de treinamento adequado para lidar com questões de segurança, o resultado da iniciativa foi considerado como positiva pela empresa, pois conceitos de segurança não faziam parte da cultura do desenvolvimento de software.

5. CONSIDERAÇÕES FINAIS

O capitulo apresenta as considerações obtidas ao longo do desenvolvimento do estudo, críticas ao método adotado e pontos positivos observados. Como encerramento do trabalho são propostas algumas sugestões para trabalhos futuros.

5.1 Conclusões do Trabalho

O processo de desenvolvimento de requisitos de segurança para o desenvolvimento e manutenção de software seguro foi estabelecido como tema para este trabalho por tratar-se da atividade fundamental no estabelecimento de um ciclo de desenvolvimento de software seguro.

Pela importância deste processo, verificou-se que a aplicação de técncias de análise de risco através de um procedimento de modelagem de ameaças e vulnerabilidades mostrou-se de grande valor pois garantem que os requisitos estabelecidos estarão devidamente orientados a mitigar as ameaças que o software será submetido em seu ambiente operacional, durante a sua operação.

5.1.1 Considerações sobre o Processo

Apesar da proposta ser fundamentada em um processo já existente (modelo SQUARE), verificou-se que é necessário refinar as técnicas propostas para estabelecimento de requisitos de segurança.

Para que o processo seja aplicado de forma efetiva é necessário que os envolvidos passem por treinamento para que os conceitos de segurança sejam padronizados e consistentes.

Durante o caso de estudo, foi possivel verificar que a falta de treinamento dificultou o desenvolvimento das tarefas propostas (mesmo com o envolvimento de profissionais experientes). Apesar de existir um roteiro inicial para cada atividade do processo, o modelo adotado para execução das tarefas baseado reuniões de *brainstorming* mostrou-se de baixa eficácia devido ao tempo gasto e falta de objetividade nas discussões, que facilmente se desviavam do foco original.

Com a evolução das atividades propostas, verificou-se a necessidade de propor melhorias, como o aperfeiçoamento das técnicas adotadas para classificação de riscos e requisitos que se mostraram subjetivas pois dependem da experiência dos membros da equipe, entretanto, foram extremamente positivas, pois mostraram a necessidade de se levar em consideração diversos cenários que usualmente não seriam explorados.

5.2 Trabalhos Futuros

Como proposta para trabalhos futuros os estudos sobre processos para o desenvolvimento de software seguro serão aprofundados com o objetivo de estender os princípios de desenvolvimento e manutenção de software seguro para todas as fases do ciclo de vida do produto.

REFERÊNCIAS

Allen Julia H., Barnum Sean, Ellison Robert J., McGraw Gary, Mead Nacy R.. Software Security Engineering A Guide for Project Managers. J. Pearson Education, Inc., 2008.

Ansar-Ul-Haque Yasar, Katholieke Univ. Leuven, Leuven, Davy Preuveneers, Yolanda Berbers, Ghasan Bhatt. Best practices for software security: An overview. Multitopic Conference, 2008.

Christopher Alberts, Woody Carol, Dorofee Audrey. Introduction to the Security Engineering Risk Analysis (SERA) Framework. Techinical note CMU/SEI, 2014.

CMMI Institute / Siemens AG Corporate Technology. Security by Design with CMMI for Development, An Application Guide for Improving Processes for Secure Products -, Carmegie Mellon University, 2013.

McGraw Gary Cigital, Inc., Dulles, VA. Software Security: Building Security In. Software Reliability Engineering, 2006.

Noopur, Davis. Secure Software Development Life Cycle Processes. Techinical Report CMU/SEI, 2013.

Mead Nancy R., Hough Eric D., R. Stehney II Theodore. Security Quality Requirements Engineering (SQUARE) Methodology. Techinical Report CMU/SEI, 2005.

Ross Ron, McEvilley Michael, Oren Janet Carrier. Systems Security Engineering, NIST Special Publication 800-160, 2016.

Shareeful Islam - Lehrstuhl fur. Software Development Risk Management Model – A goal driven approach. University at Munchen, 2010.

Stoneburner Gary, Goguen Alice, Feringa Alexis. Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1, 2002.

Wincor Nixdorf. How crime can undermine the convenience of cash. ATMIA 2015.

GLOSSÁRIO

BRAINSTORMING - Nome dado à uma técnica na qual são realizados exercícios mentais com a finalidade de resolver problemas específicos. Popularizado pelo publicitário e escritor Alex Faickney Osborn, o termo no Brasil também é conhecido como 'Tempestade de ideias

BACKDOOR - Backdoor é um recurso utilizado por diversos softwares malicios para garantir acesso indevido ao sistema ou software.

MALWARE - O "malware", termo do inglês "malicious software", é um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

HASH - Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo com o intuito de garantir a integridade de uma informação.

PLAINTEXT - Texto transmitido em claro, sem proteção de criptografia.

ANEXO - Tabela de Taxonomia de Ameaças

Este apêndice apresenta a tabela de taxonomia de ameaças proposta por Gary Stoneburner Gary, Goguen Alice, Feringa Alexis (2002).

Tipos de Fontes de Ameaças	Descrição	Características
ADVERSARIO - Individuo - Exterior - Interior - Invasor Confiável - Invasor com Privilégios - Grupo - Ad hoc - Estabelecido - Organização - Competidor - Fornecedor - Parceiro - Cliente - Natação ou Estado	Indivíduos, Grupos, Organizações, ou Nações que buscam explorar a organização através dos seus recursos cibernéticos (ex. informações em forma eletrônica, informações transitadas em comunicações digitais e informações armazenadas em meios digitais)	Capacidade, Intenção e Alvo
ACIDENTAL - Usuário - Usuário privilegiado / Administrador	Ações erradas durante o curso de execução das atividades diárias ou de sua responsabilidade	Range de Defeitos
Estrutural - Téncologia da Informação - Equipmento - Armazenamento - Processamento - Comunicações - Display - Sensores - Controles - Ambiente de Controle - Controles de Temperatura e umidade - Fonte de Alimentação - Software - Sistema Operacional - Redes - Aplicações de propósito geral	Falhas de equipamento, controles ambientais, ou software devido ao envelhecimento, o esgotamento de recursos ou outras circunstâncias que excedem os parâmetros de funcionamento esperado.	Range de Defeitos
Do Ambiente - Desastres naturais ou provocados pelo Homem. - Fogo - Enchentes / Tsunami - Vendavais / Tornados - Furacões - Terremotos - Atentados - Evento natural não usual (Ex: tempestades solares) - Falha ou interrupção de infraestrutura:	Desastres naturais ou falhas de infraestruturas críticas naturais, dos quais a organização depende, mas que estão fora do controle da organização. Nota: Os desastres naturais provocados pelo homem também podem ser caracterizados em termos de sua gravidade e / ou duração. No entanto, porque a fonte de ameaça e o evento ameaça são fortemente	Range de Defeitos

- Telecomunicações - Energia Elétrica	identificados, gravidade e duração podem ser incluídos como evento de ameaça. (Por exemplo, inundações causou grandes danos aos sistemas de missão crítica instalações de alojamento, tornando esses sistemas indisponíveis por três semanas).	

APÊNDICE – Modelo de Documento

Este anexo apresenta um modelo para elaboração do Documento de Especificação de Requisitos de Segurança.

Fonte: Autor

PECE Programa de Educação Continuada Escola Politécnica da USP	**Projeto:** ***XYZ***	**Folha: 1/8**	**Data:**
Departamento de Segurança Lógica			**Template: 1.00**

Documento de Especificação de Requisitos de Segurança

Preparado: *Autor*
Data: 01/01/2016

	**Projeto:** ***XYZ***	**Folha: 2/8**	**Data:**
Departamento de Segurança Lógica			**Template: 1.00**

Histórico de Revisões

Rev.	Data	Autor	Comentários
1.0	12/05/2016	Alexandre Balesteros	Versão Inicial

Cronograma

Data Prevista Inicio	Data Real Inicio	Data Prevista de Término	Data Real de Término	Justificativa

Aprovações		
Cargo	**Assinatura**	**Data**
Engenheiro de Requisitos		
Especialista de Segurança Lógica		
Coordenador de Segurança Lógica		
Superintendente de Segurança Lógica		
Coordenador de Desenvolvimento de Software		
Superintendente de Desenvolvimento de Software		
Gerente de Operações		

	**Projeto:** ***XYZ***	**Folha: 3/8**	**Data:**
Departamento de Segurança Lógica			**Template: 1.00**

1. Introdução

1.1 Finalidade Geral do Documento

[Descrever nesse item quais as principais características do projeto]

1.2 Referências

[Inserir os documentos que foram utilizados como referência para este documento]

2. Objetivos de Negócio

[Descrever nesse item os objetivos de negócio do projeto]

2.1 Descrições do Objetivo

Objetivo	
Afeta	
Cujo impacto é	
Uma boa solução seria	

3 Objetivos de Segurança

[Descrever nesse item os objetivos de segurança do projeto]

3.1 Objetivos de Segurança Levantados

Nome	Descrição	Responsabilidades

4 Avaliação de Riscos

[Este item descreve os riscos e ameaças levantados]

4.1 Ameaças

[Tabela de Ameaças]

Componente	Descrição
Ameaça	*Descrição do evento, que explora uma ou mais vulnerabilidades que leva a uma situação adversa ou perda.*
Ator	*Quem ou o que está tentando violar o sistema para obter dados críticos*
Motivação	*Quais são as intenções do Ator, podem ser classificadas como deliberada ou não intencional.*
Objetivo	*Considera-se como o objetivo final para o qual o ator está aplicando seus esforços.*
Resultados	*Consequência direta da ameaça (Ex: Divulgação, Modificação, Inserção ou roubo de dados).*
Meios	*Recursos que o ator utiliza para executar o evento*
Complexidade	*O grau de dificuldade atribuído a execução da ameaça*
Contexto Adicional	*Qualquer informação contextual relevante para a ameaça;*

4.2 Sequência de Atividades

[Para o procedimento de modelagem de ameaças é necessário determinar qual seria a possível sequência de atividades envolvidas no evento, essa sequência de atividades será utilizada para o desenvolvimento dos cenários de modelagem de ameaças de segurança.]

Passo	Descrição
1	
2	
3	
4	

4.3 Identificação de Vulnerabilidades

[Determinar quais vulnerabilidades estariam envolvidas para cada ameaça]

ID	Fonte	Vulnerabilidades
1	Interna/Externa	
2		
3		
4		

:

4.4 Análise de Probabilidade

[Neste item, determinar a probabilidade de ocorrência de cada ameaça]

ID	Evento	Impacto
R1		Muito Alto
R2		Alto
R3		Moderado
R4		Baixo

4.5 Magnitude de Impactos

[Neste item, determinar a gravidade do impacto que cada ameaça pode causar]

ID	Evento	Impacto
R1		Muito Alto
R2		Alto
R3		Moderado
R4		Baixo

4.6 Priorização dos Riscos

[Matriz de priorização de risco, dispor os riscos levantados de acordo com a probabilidade de ocorrência e sua gravidade]

Probabilidade	Nível de Impacto				
	Muito Baixa	Baixa	Moderada	Alta	Muito Alta
Muito Alta	-	-	-	-	-
Alta	-	-	-	-	-
Moderada	-	-	-	-	-
Baixa	-	-	-	-	-
Muito Baixa	-	-	-	-	-

[Tabela de classificação, demonstrar os riscos levantados de acordo com a sua classificação]

Valor Qualitativo	Valores Semi Quantitativos
Muito Alto	10
Alto	8
Médio	5
Baixo	2
Muito Baixo	0

4.7 Plano de Gerenciamento de Riscos

[Tabela de Gerenciamento de riscos, demonstrar os riscos levantados de acordo com a sua classificação, ações propostas para resolver o problema, operações implementadas, status e resultado]

Riscos					
ID	Função	Ações	Entrada (Operações)	Status	Resultado
1					
2					
3					
4					

PECE Programa de Educação Continuada Escola Politécnica da USP	**Projeto:** ***XYZ***	**Folha: 7/8**	**Data:**
Departamento de Segurança Lógica			**Template: 1.00**

5 Requisitos de Segurança

[Neste item descrever os requisitos de segurança elaborados, identifica-los atribuindo um ID próprio para cada item]

ID	Descrição
RS-1	
RS-2	
RS-3	
RS-4	

6 Categorização dos Requisitos de Segurança

[Neste item classificar cada um dos requisitos de acordo com as categorias propostas]

ID	Requisitos de Segurança Funcionais	Requisitos de Segurança Não Funcionais	Requisitos de Segurança de Confiabilidade
RS-1	X		
RS-2		X	
RS-3		X	
RS-4			X

7 Priorização dos Requisitos de Segurança

[Este item priorizará os requisitos, conforme a cobertura de riscos]

Requisitos	Riscos Mitigados								Total Pontos
Peso:	R1	R2	R3	R4	R5	R6	R7	R8	
	[5]	[2]	[2]	[2]	[8]	[5]	[8]	[10]	
RS1	5	2							7 (6)
RS2			2		8				10 (4)
RS3			2			5			7 (6)
RS4				2				10	12 (3)

8 Validação dos Requisitos de Segurança

[Neste item descrever os requisitos devem ser validados na visão técnica e apresentar um método para validação do mesmo.]

Requisitos	Validação	
	Viabilidade Técnica	Método de Validação
RS1	SIM ☒ Não ☐ N/A☐	
RS2	SIM ☒ Não ☐ N/A☐	
RS3	SIM ☒ Não ☐ N/A☐	
RS4	SIM ☒ Não ☐ N/A☐	