REGINA MARIA THIENNE COLOMBO

**PROPOSTA DE UMA METODOLOGIA DE MEDIÇÃO E PRIORIZAÇÃO DE
SEGURANÇA DE ACESSO PARA APLICAÇÕES WEB**

SÃO PAULO

2013

REGINA MARIA THIENNE COLOMBO

**PROPOSTA DE UMA METODOLOGIA DE MEDIÇÃO E PRIORIZAÇÃO DE
SEGURANÇA DE ACESSO PARA APLICAÇÕES WEB**

Tese apresentada à Escola Politécnica da
Universidade de São Paulo como parte
dos requisitos para obtenção do título de
Doutor em Ciências.

SÃO PAULO

2013

REGINA MARIA THIENNE COLOMBO

**PROPOSTA DE UMA METODOLOGIA DE MEDIÇÃO E PRIORIZAÇÃO DE
SEGURANÇA DE ACESSO PARA APLICAÇÕES WEB**

Tese apresentada à Escola Politécnica da
Universidade de São Paulo como parte
dos requisitos para obtenção do título de
Doutor em Ciências.

Área de Concentração:
Engenharia de Produção

Orientador: Prof. Dr.
Marcelo Schneck de Paula Pessoa

SÃO PAULO

2013

FICHA CATALOGRÁFICA

Colombo, Regina Maria Thienne

Proposta de uma metodologia de medição e priorização de segurança de acesso para aplicações WEB / R.M.T. Colombo. -- São Paulo, 2013.

250 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Produção.

1.Segurança de software 2.WEB (Aplicações) 3. Modelo de segurança de acesso 4.Medição de segurança 5.AHP I.Universidade Paulo. Escola Politécnica. Departamento de Engenharia de Produção II.t.

DEDICATÓRIA

*Para meus queridos amores: esposo Jairo
e filhos Victor, Rodolfo e Luiza,
e meus eternos pais Nelson e Maria,
cujo desprendimento com relação aos seus
projetos pessoais e apoio nos momentos difíceis,
sempre me incentivando e acreditando,
permitiram que esse período de pesquisa pudesse
realmente acontecer e se concretizar.*

Para os queridos amigos que sempre acreditaram em mim.

*Para os profissionais da área de pesquisa e
desenvolvimento, que este trabalho contribua
de alguma forma útil em suas atuações.*

AGRADECIMENTOS

Em primeiro lugar quero agradecer ao Deus Pai Todo Poderoso. Com a minha fé nEle depositada, deram-me forças para vivenciar este momento, aqui humildemente representado.

A lista de pessoas que auxiliaram de sobremaneira, no desenvolvimento e em discussões técnicas e de apoio estratégico é extensa, sendo impossível citar nominalmente a todos.

Quero agradecer ao meu orientador Professor Doutor Marcelo Schneck de Paula Pêsoa, e em seu nome, pela instituição da Engenharia de Produção da POLI-USP, por possibilitarem o meu ingresso no doutorado e pela minha formação e desenvolvimento técnico na área, pela motivação, pelas ideias e sugestões neste trabalho e, sobretudo, pela cordialidade, disponibilidade e paciência na revisão de conceitos, vistos e revistos ao longo desta pesquisa de doutorado.

Quero agradecer em especial aos amigos e companheiros de trabalho do CTI - Centro de Tecnologia da Informação Renato Archer do Ministério da Ciência, Tecnologia e Inovação do Governo Federal, representado pela Divisão da Segurança de Sistemas da Informação, que me permitiram uma dedicação especial, onde encontrei todos os recursos necessários para que as ideias e conceitos aqui apresentados ganhassem corpo. Não posso deixar de registrar as demais pessoas de outras divisões, sem as quais dificilmente obteria o conjunto de dados e informações, bem como importantes informações técnicas relacionadas às suas áreas de especialização.

Finalmente, agradeço de forma muito carinhosa a todas as pessoas verdadeiramente amigas, solidárias, exigentes, incentivadoras que me permitiram compartilhar um pouco de nossas vidas, emoções, conhecimento, experiências sem as quais este trabalho não chegaria neste ponto.

Meu muito obrigada!

REFLEXÕES SOBRE O TEMA

*"Thomas Saaty is known world-wide as the person who figured out how to measure
intangibles"*

(AHP team, 2013)

*"Touchpoints - putting software security into practice requires making some changes
to the way organizations build software."*

(Gary McGraw, 2006)

*"To move from a culture of fear to a culture of awareness and then a culture of
measurement "*

(Dan Geer, 2007)

"If you cannot measure it, you cannot improve it"

(William Thomson, Lord Kelvin, 1883)

*"When you cannot express it in numbers, your knowledge is of a meager and
unsatisfactory kind"*

(William Thomson, Lord Kelvin, 1883)

*"Security traditionally has been a preventative game, trying to prevent things from
happening. What's been going on is people realizing you cannot do 100 percent
prevention anymore"*

(Bruce Schneier, 2001)

RESUMO

Em um mundo tecnológico e globalmente interconectado, em que indivíduos e organizações executam transações na web com frequência, a questão da segurança de software é imprescindível, ela é necessária em diversos nichos: segurança das redes de computadores, dos computadores e dos softwares. A implantação de um sistema de segurança que abrange todos os aspectos é extensa e complexa, ao mesmo tempo em que a exploração de vulnerabilidades e ataques é exponencialmente crescente. Por causa da natureza do software e de sua disponibilidade na web, a garantia de segurança nunca será total, porém é possível planejar, implementar, medir e avaliar o sistema de segurança e finalmente melhorá-la. Atualmente, o conhecimento específico em segurança é detalhado e fragmentado em seus diversos nichos, a visão entre os especialistas de segurança é sempre muito ligada ao ambiente interno da computação. A medição de atributos de segurança é um meio de conhecer e acompanhar o estado da segurança de um software. Esta pesquisa tem como objetivo apresentar uma abordagem top-down para medição da segurança de acesso de aplicações web. A partir de um conjunto de propriedades de segurança reconhecidas mundialmente, porém propriedades estas intangíveis, é proposta uma metodologia de medição e priorização de atributos de segurança para conhecer o nível de segurança de aplicações web e tomar as ações necessárias para sua melhoria. Define-se um modelo de referência para segurança de acesso e o método processo de análise hierárquica apoia a obtenção de atributos mensuráveis e visualização do estado da segurança de acesso de uma aplicação web.

Palavras-chave: Segurança de software. Aplicação WEB. Modelo de segurança de acesso. Medição de segurança, AHP.

ABSTRACT

In a technological world and globally interconnected, in which individuals and organizations perform transactions on the web often, the issue of software security is essential, it is needed in several niches: security of computer networks, computers and software. The implementation of a security system that covers all aspects is extensive and complex, while the exploitation of vulnerabilities and attacks are increasing exponentially. Because of the nature of software and its availability on the web, ensure security will never be complete, but it is possible to plan, implement, measure and evaluate the security system and ultimately improve it. Currently, the specific knowledge in security is detailed and fragmented into its various niches; the view among security experts is always connected to the internal environment of computing. The measurement of security attributes is a way to know and monitor the state of software security. This research aims to present a top-down approach for measuring the access security of web applications. From a set of security properties globally recognized, however these intangible properties, I propose a measurement methodology and prioritization of security attributes to meet the security level of web applications and take necessary actions for improvement. It is defined a reference model for access security and a method of analytic hierarchy process to support the achievement of measurable attributes and status of the access security of a web application.

Keywords: Software security. WEB application. Access security model. Security measurement, AHP.

LISTA DE FIGURAS

FIGURA 1.1 – ABORDAGEM HOLÍSTICA PARA SEGURANÇA (MEIER, 2003).....	32
FIGURA 2.1 – PROCESSO DE ANÁLISE DE DECISÃO (FONTE: CLEMEN 1991 APUD MORITA, 2001)	34
FIGURA 2.2 – ESTRUTURA HIERÁRQUICA DO AHP	39
FIGURA 2.3 - ESTRUTURA HIERÁRQUICA COM <i>RATINGS</i> FONTE: GOMES (2010).....	50
FIGURA 3.1- ABORDAGEM PARA MELHORIA DA SEGURANÇA DE APLICAÇÃO WEB (MEIER, 2003)	60
FIGURA 3.2 – MODELO GERAL DE QUALIDADE.....	72
FIGURA 3.3 – MODELO DE QUALIDADE SOFTWARE	72
FIGURA 3.4 – PESO DA EXPOSIÇÃO VERSUS IMPACTO.....	74
FIGURA 3.5 – COMO MEDIR A DISTÂNCIA DE UMA ESTRELA.....	85
FIGURA 4.1 - PASSOS DA PESQUISA-AÇÃO (COUGHLAN; COGHLAN, 2002) .	100
FIGURA 4.2 – ESTRUTURAÇÃO GERAL DA PESQUISA.....	103
FIGURA 5.1 – ESTRUTURA POR FASES DA PESQUISA-AÇÃO	107
FIGURA 5.2 – ESTRUTURA POR CICLOS DA PESQUISA-AÇÃO	108
FIGURA 5.3 – ESTRUTURA DA FASE 01.....	109
FIGURA 5.4 - MACRO VISÃO DA PROPOSTA.....	112
FIGURA 5.5 – PUBLICAÇÕES POR TIPO DE MÍDIA	113
FIGURA 5.6 – PUBLICAÇÕES ENCONTRADAS ENTRE 1999/2011	113
FIGURA 5.7 – ESTRUTURA DA FASE 02.....	115
FIGURA 5.8 - ESTRUTURA DA FASE 03.....	119
FIGURA 5.9 – PROCESSO DE AVALIAÇÃO GENÉRICO ISO/IEC 25040	120
FIGURA 5.10 – USO DAS PROPRIEDADES DE SEGURANÇA NO CONTEXTO TÉCNICO-GERENCIAL	121
FIGURA 5.11 - REQUISITOS DE SEGURANÇA NO CONTEXTO TÉCNICO- GERENCIAL	122
FIGURA 5.12 – ESTRUTURA DA FASE 04.....	127
FIGURA 5.13 – PROCESSO DE AVALIAÇÃO DE SEGURANÇA DE APLICAÇÃO	129

FIGURA 5.14 - MODELO DE QUALIDADE DE SEGURANÇA DE ACESSO – (WANG; WULF, 1997).....	132
FIGURA 5.15 – COMO PASSAR DOS INTANGÍGEIS PARA OS TANGÍVEIS	136
FIGURA 5.16 – ESTRUTURA DA FASE 05.....	138
FIGURA 5.17 – MODELO DE REFERÊNCIA PARA SEGURANÇA DE ACESSO .	138
FIGURA 5.18 – MODELO DE REFERÊNCIA PARA AUTENTICIDADE	139
FIGURA 5.19 – MODELO DE REFERÊNCIA PARA CONFIDENCIALIDADE	140
FIGURA 5.20 – MODELO DE REFERÊNCIA PARA DISPONIBILIDADE.....	140
FIGURA 5.21 - MODELO DE REFERÊNCIA PARA INTEGRIDADE	141
FIGURA 5.22 – MODELO DE AUTENTICIDADE NO SUPERDECISION®S.....	142
FIGURA 5.23 – BASE PARA FORMALIZAÇÃO DO <i>CHECKLIST</i>	143

LISTA DE TABELAS

TABELA 2.1 - QUESTIONÁRIO PARA COMPARAÇÃO PAR A PAR DE 3 ELEMENTOS - EXEMPLO.....	40
TABELA 2.2 - ESCALA DE SAATY PARA IMPORTÂNCIAS RELATIVAS	40
TABELA 2.3 – ITERAÇÕES DO MÉTODO DAS POTENCIAS	45
TABELA 2.4 – ÍNDICE DE CONSISTÊNCIA PROPOSTO POR SAATY	46
TABELA 2.5 - APLICAÇÕES DO AHP FONTE: HO (2008)	48
TABELA 3.1 - FRAMEWORK DE SEGURANÇA DE SOFTWARE (BSIMM, 2013) ..	57
TABELA 3.2 - ESTRUTURA DO MODELO SAMM (OWASP-SAMM, 2013).....	58
TABELA 3.3 - ÁREAS DE PROCESSOS DO SSE-CMM	59
TABELA 3.4 – EXEMPLOS DE AMEAÇAS AO SOFTWARE NA OPERAÇÃO.....	66
TABELA 3.5 – PUBLICAÇÕES DE 1996 A 2000	95
TABELA 3.6 – PUBLICAÇÕES ENTRE 2001 E 2013.....	95
TABELA 3.7- RESUMO DAS PRINCIPAIS NORMAS RELACIONADAS À SEGURANÇA	96
TABELA 5.1 – ESTRUTURAÇÃO DA PESQUISA.....	108
TABELA 5.2 – <i>JOURNAL</i> E NÚMERO DE PUBLICAÇÕES	113
TABELA 5.3 - CORRELAÇÃO DAS PROPRIEDADES E REQUISITOS DE SEGURANÇA E AS REFERÊNCIAS	120
TABELA 5.4 – CORRELAÇÃO DAS PROPRIEDADES COM OS REQUISITOS ...	122
TABELA 5.5 - CINCO NÍVEIS DA PROPRIEDADE DE AUTENTICIDADE	125
TABELA 5.6 - MATRIZ A PARA O MODELO DE SEGURANÇA DE ACESSO	134
TABELA 5.7 – RESULTADOS DO AHP.....	135
TABELA 5.8 – TABELA DE AUXÍLIO AOS CRITÉRIOS.....	143
TABELA 5.8 - MATRIZ DE DECISÃO	145
TABELA 5.9 - RESULTADO DA AUTENTICAÇÃO NO AHP PARA O SISTEMAWEB	145
TABELA 5.10 – RESUMO DOS RESULTADOS DA METODOLOGIA DE MEDIÇÃO E PRIORIZAÇÃO DE SEGURANÇA DE ACESSO DE APLICAÇÕES WEB...	147

LISTA DE ABREVIATURAS E SIGLAS

<i>ABNT</i>	<i>Associação Brasileira de Normas Técnicas</i>
<i>AHP</i>	<i>Analytic Hierarchy Process</i>
<i>AWA</i>	<i>Aplicação Web Alvo</i>
<i>CC</i>	<i>Common Criteria</i>
<i>CEO</i>	<i>Chief Executive Officer</i>
<i>CERT</i>	<i>SEI - Computer Emergency Response Team no Software Engineering Institute</i>
<i>CERT BR</i>	<i>Computer Emergency Response Team no Brasil</i>
<i>CERT/CC</i>	<i>Computer Emergency Response Team / Coordination Center</i>
<i>CIO</i>	<i>Chief information officer</i>
<i>CNPq</i>	<i>Conselho Nacional de Desenvolvimento Científico e Tecnológico</i>
<i>COTS</i>	<i>Commercial Off The Shelves</i>
<i>CSIAC Center¹</i>	<i>Cyber Security and Information Systems Information Analysis</i>
<i>CSO</i>	<i>Chief Security Officer</i>
<i>CTCPEC</i>	<i>Canadian Trusted Computer Product Evaluation Criteria</i>
<i>CVE</i>	<i>Common Vulnerabilities and Exposures</i>
<i>CWE</i>	<i>Common Weakness Enumeration</i>
<i>DACS</i>	<i>Data and Analysis Center for Software</i>
<i>DHS/USA</i>	<i>Department of Homeland Security dos USA</i>

---

¹ The Cyber Security and Information Systems Information Analysis Center (CSIAC) is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC). The CSIAC is a consolidation of three predecessor IACs: the Data and Analysis Center for Software (DACS), the Information Assurance Technology IAC (IATAC) and the Modeling & Simulation IAC (MSIAC), with the addition of the Knowledge Management and Information Sharing technical area.

<i>EP</i>	<i>Engenharia da Produção</i>
<i>ES</i>	<i>Engenharia de Software</i>
<i>FDIS</i>	<i>Final Draft International Standard</i>
<i>GSI_DSIC</i>	<i>Gabinete de Segurança Institucional da Presidência da República do Brasil - Departamento da Segurança da Informação e Comunicações</i>
<i>HTM</i>	<i>HyperText Markup Language</i>
<i>IATAC</i>	<i>Information Assurance Technology Analysis Center</i>
<i>IEC</i>	<i>International Electrotechnical Commission</i>
<i>ISMS</i>	<i>Information Security Management System</i>
<i>ISO</i>	<i>International Organization for Standardization</i>
<i>MEDE-PROS®</i>	<i>Método de Avaliação da Qualidade de Produto de Software</i>
<i>NIST</i>	<i>National Institute of Standards and Technology</i>
<i>OWASP</i>	<i>The Open Web Application Security Project</i>
<i>PCI SSC</i>	<i>Payment Card Industry – Security Standards Council</i>
<i>SD</i>	<i>Super Decision</i>
<i>SI</i>	<i>Sistema de Informação</i>
<i>SLDC</i>	<i>Software Development Life Cycle</i>
<i>SQuaRE</i>	<i>System and Software QUALity Requirements and Evaluation</i>
<i>SQUARE/SEI</i>	<i>Security Quality Requirements Engineering Methodology/Software Engineering Institute</i>
<i>Sul</i>	<i>Software under Investigation</i>
<i>TCSEC</i>	<i>Trusted Computer System Evaluation Criteria</i>
<i>TI</i>	<i>Tecnologia da Informação</i>
<i>TIC</i>	<i>Tecnologia da Informação e Comunicação</i>
<i>TOE</i>	<i>Target Of Evaluation</i>
<i>WASC ou WEBAPPSEC</i>	<i>Web Application Security Consortium</i>
<i>WWW</i>	<i>World Wide Web</i>

SUMÁRIO

1. INTRODUÇÃO.....	18
1.1 TEMA.....	21
1.2 MOTIVAÇÃO	24
1.3 OBJETIVO	26
1.4 CONTEXTO, PROBLEMÁTICA E JUSTIFICATIVA.....	27
1.5 LIMITAÇÕES	31
1.6 ESTRUTURA DO TRABALHO	32
2. CONCEITOS AUXILIARES À PESQUISA	33
2.1 MÉTODO PARA APOIO À DECISÃO.....	33
2.2 CONCEITOS ALGÉBRICOS	35
2.3 MODELO AHP	38
2.4 POR QUE USAR O AHP	48
2.5 EXPERIÊNCIA EM AVALIAÇÃO DE SOFTWARE	51
2.6 ANÁLISE E DISCUSSÃO	52
3. MODELOS E TRABALHOS RELACIONADOS A MEDIDAS DE SEGURANÇA DE SOFTWARE.....	54
3.1 SEGURANÇA DE SOFTWARE, TI, SI, E APLICAÇÃO WEB.....	54
3.1.1 Sistema de Gestão	54
3.1.2 Modelos de Maturidade	56
3.1.3 Ciclo de Vida de Desenvolvimento de Software Seguro	60
3.1.4 Vulnerabilidade e Ameaças.....	62
3.1.5 Qualidade e Segurança de Software	69
3.2 QUALIDADE DE SOFTWARE E SISTEMAS.....	70
3.2.1 Modelo de Qualidade	70
3.3 REQUISITO DE SEGURANÇA DE SOFTWARE	74
3.3.1 Requisitos funcionais de segurança de TI.	74
3.3.2 Trabalhos sobre Requisitos de Segurança de Software	77
3.4 MEDIDAS E MÉTRICAS DE SEGURANÇA DE SOFTWARE	80
3.4.1 Pesquisadores Filósofos.....	81
3.4.2 Propostas de medição de segurança.....	84

3.5	PESQUISA E DESENVOLVIMENTO PARA GOVERNOS	90
3.5.1	Governo e Institutos Americanos.....	91
3.5.2	Governo Brasileiro.....	92
3.6	ANÁLISE E DISCUSSÃO	94
4.	ESTRUTURA DA PESQUISA	97
4.1	METODOLOGIA DE PESQUISA ACADÊMICA NA ENGENHARIA DE PRODUÇÃO.....	97
4.2	METODOLOGIA PESQUISA-AÇÃO (PA).....	98
4.3	PROJETO DA PESQUISA.....	101
4.4	ESTRUTURAÇÃO DA PESQUISA	102
5.	PESQUISA-AÇÃO PARA MEDIÇÃO E PRIORIZAÇÃO DE SEGURANÇA...107	
5.1	AS FASES E CICLOS DA PESQUISA-AÇÃO (PA)	107
5.2	FASE 1 – EXPLORATÓRIA.....	109
5.2.1	Ponto de Análise.....	112
5.2.2	Entregável.....	112
5.2.3	Próximos Passos	114
5.3	FASE 2 – CICLO 01 DA PESQUISA-AÇÃO	114
5.3.1	Planejar	115
5.3.2	Agir.....	116
5.3.3	Monitorar	116
5.3.4	Entregável.....	117
5.3.5	Ponto de Análise.....	117
5.4	FASE 3 – CICLO 02 DA PESQUISA-AÇÃO	118
5.4.1	Planejar	119
5.4.2	Agir.....	123
5.4.3	Monitorar	126
5.4.4	Entregável.....	126
5.4.5	Ponto de Análise.....	126
5.5	FASE 4 – CICLO 03 DA PESQUISA-AÇÃO	127
5.5.1	Planejar	128
5.5.2	Agir.....	132
5.5.3	Monitorar	135
5.5.4	Entregável.....	136

5.5.5	Ponto de Análise	136
5.6	FASE 5 – CONCLUSIVA	137
5.6.1	Entregável.....	146
5.6.2	Ponto de Análise	146
5.7	RESULTADOS OBTIDOS.....	146
6.	PROVA DE CONCEITO.....	149
6.1	PLANEJAR	149
6.2	AGIR	150
6.3	MONITORAR	151
6.4	ENTREGÁVEL.....	155
6.5	PONTO DE ANÁLISE	155
7.	DISCUSSÕES E TRABALHOS FUTUROS.....	158
8.	REFERÊNCIAS BIBLIOGRÁFICAS.....	163
9.	REFERÊNCIAS DO AUTOR	173
10.	APÊNDICES	174
10.1	APÊNDICE 1 – RELATÓRIO SISTEMAWEB – AVALIAÇÃO EXPLORATÓRIA	174
10.2	APÊNDICE 2 – RELATÓRIO SISTEMAWEB – AVALIAÇÃO FORMAL ...	186
10.3	APÊNDICE 3 – CHECKLIST DE AUTENTICIDADE	194
10.4	APÊNDICE 4 – RELATÓRIO COMPRAS-ONLINE – AVALIAÇÃO FORMAL 213	
10.5	APÊNDICE 5 - GLOSSÁRIO	230

1. INTRODUÇÃO

Várias interpretações podem ser observadas no que se refere à "segurança de computador". "Segurança de computador" pode ser entendida como o processo de garantir a confidencialidade, integridade e disponibilidade de computadores, seus programas, dispositivos de hardware e dados. A falta de resultados de segurança surge de uma falha de uma destas três propriedades. A falta de confidencialidade é a divulgação não autorizada de dados ou acesso não autorizado a um sistema de computação ou a um programa. Uma falha de resultados integridade é a modificação não autorizada de dados ou danos a um sistema de computação ou programa. A falta de disponibilidade de recursos de computação resulta no que é chamado de negação de serviço (WANG; WULF, 1997). Uma ação ou evento que tem o potencial para causar uma falha de segurança do computador é chamado de uma ameaça. Algumas ameaças são efetivamente evitadas por contramedidas chamadas de controles. Tipos de controles podem ser físicos, administrativos, lógicos, criptográficos, legais e éticos. Ameaças que não são evitadas pelos controles são chamadas de vulnerabilidades (DICTIONARY, 2003).

As interpretações para questões de segurança essenciais para um ambiente acadêmico são obviamente diferentes das de um sistema bancário ou ainda de banco de dados de uma empresa de comércio eletrônico. Esta observação aponta para que não exista uma definição única de segurança.

Este trabalho tem o foco na questão da segurança de programas de software. A segurança do software é um atributo multidimensional e suas múltiplas dimensões não são necessariamente propriedades. Cada ramo de negócio pode definir a sua segurança a ser implantada com prioridade, privacidade e disponibilidade diferentes. Aqui se considera a definição de segurança de software como na engenharia de software, que o software continue a funcionar corretamente mesmo sob ataques (McGRAW, 2006). Nesse contexto os riscos de negócio devem ser estudados e analisados para oferecer requisitos para o sistema de segurança em questão.

Quando o objetivo é fazer medição de um atributo multidimensional, as muitas facetas do atributo devem todos ser devidamente identificados e tratados (WANG; WULF, 1997).

Dentre as multi dimensões da segurança de software, este trabalho foca na questão da medição da Segurança de Acesso, que é o grau pelo qual um produto ou sistema protege informação e dados de modo que pessoas ou outros produtos ou sistemas tenham o grau de acesso apropriado aos seus tipos e níveis de autorização aos dados (ISO/IEC 25010, 2011).

Segurança de software não é um assunto novo e vem recebendo atenção esporadicamente na maioria das organizações, principalmente em organizações clientes de software, ela é complexa e muito desafiante para os especialistas da área.

Os processos de segurança de software utilizados na concepção, implementação, configuração, manutenção e operação de um sistema precisam ser gerenciados, medidos e melhorados. Estas atividades ainda são muito novas e merecem estudos mais profundos. Em geral, medidas fornecem um valor único do ponto de vista específico, fatores discretos, enquanto as métricas são derivadas pela comparação de duas ou mais medidas tomadas ao longo tempo com uma base pré-determinada (JANSEN, 2009). Estes conceitos devem ser gerenciados para uma visão global entre os envolvidos com a segurança de software

Hinson coloca que segurança da informação é uma área complexa a qual a torna difícil, mas, não impossível de identificar métricas úteis para o conhecimento do sistema em termos de segurança (HINSON, 2006). Relata sete mitos sobre métricas de segurança da informação, entre eles o de que “medir custa caro”, no entanto a organização deve gerenciar as atividades de medição e fazer reuso de métricas verificando, por exemplo, o que a organização gasta em TI e comparar com o que gasta em segurança da informação. Outro exemplo relacionado a esse mito é o tempo gasto com os incidentes ocorridos nessa área.

Verendel fez um trabalho de levantamento e análise de artigos de 1981 até 2008 que analisam quantitativamente a segurança da informação. Nesse trabalho ele constata a falta de uma abordagem conceitual ou pelo menos um suporte empírico para as abordagens de medições. Entre os métodos teóricos, a sua utilização é de difícil aplicação. Entre os métodos empíricos não há experimento de repetibilidade, de compartilhamento de dados que possam ser reutilizados (VERENDEL, 2009).

A viabilidade de medição de segurança e desenvolvimento de métricas de segurança para representar fenômenos reais de segurança tem sido criticada em muitas contribuições. McHugh (McHUGH, 2001) é cético em relação ao lado de efeitos de tal simplificação e à falta de prova científica.

Bellovin (BELLOVIN, 2006) observa que a definição de métricas é difícil, se não inviável, porque um esforço do atacante é frequentemente linear, mesmo em casos onde a segurança requer um trabalho exponencial.

Em outras disciplinas, como por exemplo, no campo das finanças, existem métodos quantitativos aprovados e já conhecidos para determinar o risco junto a tomada de decisões, são *frameworks* baseados em medidas estabelecidas e métricas. Tais medidas padronizadas ajudam a tomada de decisão nessas áreas. Para a segurança do sistema de software esses métodos são apenas emergentes, e como em qualquer disciplina, requerem pressupostos realistas e insumos para atingir resultados confiáveis (JANSEN, 2009).

Avançar no estado da arte cientificamente para obter medidas e métricas de segurança, seria de grande ajuda na concepção, execução e operação de sistemas de informação segura.

No mundo físico a metrologia oferece os números que quantificam e qualificam as propriedades dos sistemas e com isso podem ser melhorados. No caso de segurança de software, mensuração deve ser o processo pelo qual números ou símbolos são atribuídos aos atributos de entidades de tal forma que os descreve de acordo com regras claramente definidas. Assim uma contribuição mesmo que específica, traz mais conhecimento sobre os sistemas de informação seguro e familiaridade com medidas e métricas.

Neste trabalho foram utilizadas as taxonomias de segurança de termos definidos em normas (ISO/IEC 27000, 2009)(ISO/IEC 25010, 2011) e em específico a categoria de requisitos “Autenticação” decomposta em elementos mais simples para que possam ser medidos. A contribuição do trabalho se dá no sentido de oferecer uma metodologia para obtenção de medidas que auxiliem os gestores em tomada de decisão para a evolução da segurança de software.

1.1 TEMA

Um dos problemas que preocupam muito os CEO's, CIO's e CSO's no mundo inteiro são também um dos mais complexos de se resolver: como impedir que informações valiosas da organização caiam em mão erradas, ou simplesmente se percam.

Segurança de software começou a florescer como uma disciplina separada da segurança do computador e da rede no final dos anos 90. Os pesquisadores começaram a colocar mais ênfase no estudo das formas que um desenvolvedor de software pode contribuir ou acidentalmente comprometer a segurança de um sistema de computador (McGRAW, 2006).

A gestão da segurança da informação é um assunto sério, e estratégico e deve estar entre as preocupações centrais da alta direção da instituição. Regulamentos, normas de conduta e diversos mecanismos de defesa têm sido desenvolvidos nos últimos anos, num cenário em que, cada vez mais, as empresas dependem de seus sistemas de informação e do comportamento da sua força de trabalho, para assegurar que seus dados estejam protegidos.

O conhecimento e experiência em segurança de software precisam ser disponibilizados para os técnicos de não segurança e gestores, de uma maneira clara e sem complexidades. Esses conhecimentos precisam ser explicitados em forma de documentos ou de outra forma de fácil acesso, por exemplo, padrões, *checklists de requisitos e de avaliação da segurança*, listas de vulnerabilidades e indicadores do nível de segurança (OWASP, 2013).

Os especialistas em segurança têm experiência e conhecimento tácito sem consciência desse conhecimento e a experiência normalmente não é explicitada, mas fazem uso disso o tempo todo. O conhecimento tácito é necessário para fazer uso do conhecimento explícito. Então é necessário o desenvolvimento de constructos de apoio à questão de segurança em aplicativos de software (HOUMB, 2010).

O levantamento de requisitos de segurança e a metodologia de avaliação da segurança de aplicativos de software tenta englobar o conhecimento tácito dos especialistas em segurança juntamente com o conhecimento explícito encontrado na literatura da área (COLOMBO et al., 2011).

Nos últimos anos, vários problemas no campo de aplicações baseadas na Web foram abordados, e vários métodos e técnicas têm sido usados em aplicativos de forma eficaz. Existem muitas diferenças entre aplicações baseadas na Web e as tradicionais (McGRAW, 2006).

O foco principal desta pesquisa está em avaliar a segurança de um aplicativo baseado na Web. Um aplicativo da Web pode ser considerado como um sistema distribuído, com um cliente-servidor ou arquitetura multicamadas, incluindo as seguintes características principais (MEIER, 2003):

- Um grande número de usuários distribuídos por todo o mundo pode acessá-lo simultaneamente.
- Ambientes de execução bastante heterogêneo, composto de hardware, conexões de rede, sistemas operacionais, servidores Web e browsers diferentes.
- Uma natureza extremamente heterogênea, que depende da grande variedade de componentes de software que geralmente inclui. Esses componentes podem ser construídos de diferentes tecnologias (ou seja, linguagens de programação e modelos diferentes), e podem ser de naturezas diversas (ou seja, novos componentes gerados a partir do zero, os legados, componentes de hipermídia, COTS).
- A capacidade de geração de componentes de software em tempo de execução de acordo com entradas do usuário e o status do servidor.

As vulnerabilidades afetam, basicamente, sistemas web e indicam duas coisas: a recente popularização das interfaces web para comércio eletrônico, internet banking e configuração de elementos de rede; os problemas de segurança deste domínio não estão sendo adequadamente considerados durante o processo de desenvolvimento, tanto por ignorância como pela pressão causada por cronogramas de entrega apertados (McGRAW, 2006).

Para o processo de desenvolvimento, este estudo encontrou modelos e padrões para o ciclo de vida de desenvolvimento de software seguro, a sigla em Inglês SDLC (*Software Development Life Cycle*) e também modelos da maturidade do desenvolvimento de software seguro nas organizações. O site <https://buildsecurityin.us-cert.gov/> é um esforço colaborativo que fornece práticas, ferramentas, diretrizes, regras, princípios, e outros recursos que os

desenvolvedores de software, arquitetos e profissionais de segurança podem utilizar para construir a segurança em software em cada fase de seu desenvolvimento.

Além destas iniciativas e práticas é importante focar no produto do software e neste caso na aplicação web como produto de manufatura. Na Engenharia de software e na qualidade de software encontramos modelos e padrões que apoiam este foco. Pode-se dizer que na engenharia de segurança de software pesquisa e desenvolvimento ainda é imaturo e estudos foram encontrados indicando também esta direção de pesquisa (GOERTZEL, 2008).

Tratar todas as exceções de maneira genérica é um mecanismo genérico – e utilizado para o tratamento de erros, inclusive aqueles que a aplicação não tem nem ideia de como lidar. Isso pode esconder problemas de lógica, deixando-os latentes, até que uma situação específica ocorra e resulte em uma falha (IEEE 610, 1990).

O termo aplicação Web pode ser considerado a partir deste momento como simplesmente aplicação, sendo considerado como um conjunto de componentes de software que implementam os requisitos funcionais, enquanto que o termo meio ambiente no qual esse software é executado indicará o conjunto de infra-estrutura (composta de hardware, software e componentes de *middleware*) necessários para executar um aplicativo da Web.

Vulnerabilidades do sistema afetando a segurança podem estar contidas no código da aplicação, ou em qualquer um dos diferentes hardwares, software, componentes de middleware dos sistemas. Tanto o ambiente de execução e o aplicativo podem ser responsáveis por falhas de segurança. No caso das aplicações Web, aplicação heterogênea e tecnologias de execução, em conjunto com o grande número de usuários possível, e a possibilidade de acessá-los de qualquer lugar pode fazer aplicações Web mais vulneráveis do que as aplicações tradicionais, e avaliações de segurança mais difícil a ser realizadas (GOERTZEL, 2007).

O número crescente de vulnerabilidades (CERT-BRa, 2011) encontrados em software mostra claramente a necessidade de estudos e desenvolvimento de metodologias para assegurar a segurança de software (MEIER, 2003).

1.2 MOTIVAÇÃO

A segurança da rede é considerada o elemento usual e fundamental da segurança da informação moderna. Isso não deixa menos importante à segurança de aplicativos, ou seja, a indisponibilidade de vulnerabilidades no específico contexto de uso. Os objetivos da segurança de aplicativos são para proteger a:

- Confidencialidade dos dados dentro da aplicação;
- A disponibilidade do aplicativo;
- Integridade de dados dentro da aplicação.

Proteger a confidencialidade dos dados em um aplicativo é fundamental no mundo de hoje. A atividade de *Hacking* evoluiu de um passatempo com o direito de se gabar para um negócio sério de alto custo, com os usuários como vítimas inocentes. Governos de todo o mundo têm aprovado regulamento sobre a segurança das informações pessoais (muitas vezes referida como a privacidade), com severas penalidades civis e criminais por trás da regulamentação. Nenhum fornecedor de software pode se dar ao luxo de ignorar a importância da proteção de dados (GOERTZEL, 2007).

A confidencialidade dos dados é protegida quando 1) os dados não podem ser lidos "fora da rede" durante o trânsito, e 2) dados não podem ser roubados quando em repouso. A ferramenta essencial para garantir a confidencialidade dos dados é a criptografia. Existem alguns algoritmos de criptografia familiares como SSL/TLS, que protegem aplicações na web. Estas tecnologias são aplicadas para garantir que um usuário malicioso não pode ter nenhum tipo de acesso a esses dados. Por definição e por projeto, a aplicação deve ser capaz de descriptografar os dados em trânsito ou em repouso. Um usuário mal intencionado procura capturar os dados por meio da aplicação, por meio da manipulação de um pedido de tal forma a obter acesso aos dados de maneira ilícita (OWASP-TOP TEN, 2010).

Os ataques mais comuns hoje são: assumir a forma de *cross-site scripting* ou de injeção de *script*, onde o hacker instrui o aplicativo de software (seja executado no servidor ou no navegador do cliente) para divulgar os dados para um destino especificado pelo hacker. Nenhuma quantidade de segurança de

rede ou criptografia pode impedir que isso aconteça - a solução é construir de forma robusta, uma aplicação de Web segura.

O objetivo das avaliações de segurança é verificar a eficácia das defesas do sistema global da Web contra o acesso indesejável de usuários não autorizados, bem como a sua capacidade de preservar os recursos do sistema de usos impróprios, e conceder o acesso aos usuários autorizados aos serviços autorizados e recursos.

Testar a segurança de software é uma tarefa difícil e testar aplicações na Web pode ser ainda mais difícil, devido às peculiaridades dessas aplicações.

Falhas essas que serão causadas principalmente por falhas no ambiente de execução ou na interface entre a aplicação e o ambiente onde ele é executado. As interfaces são pontos muito importantes para segurança de aplicativos, são nesses pontos que normalmente os dados são capturados (CVE, 2010) (CWE, 2011).

Uma abordagem *top-down*, isto é, que parte da visão do produto para os componentes de ambiente de execução e de desenvolvimento de aplicação web colabora no entendimento e na ação para tratar a segurança de software para os gestores e especialistas em segurança (COLOMBO et al., 2012).

Avançar no estado da arte cientificamente para obter medidas e métricas de segurança de software, seria de grande ajuda na concepção, execução e operação de sistemas de informação segura. Assim uma contribuição mesmo que específica ao atributo “Segurança de acesso” pode trazer mais conhecimento sobre os sistemas de informação seguro e familiaridade com medidas e métricas para esta área (COLOMBO et al., 2011).

Esta pesquisa de doutorado foi motivada pela pesquisa da dissertação de mestrado, nesta pesquisa houve o objetivo de avaliar a qualidade de pacotes de software, ela foi desenvolvida com os conceitos de Modelo de qualidade, Medição e Processo de avaliação, porém as medidas foram calculadas de forma empírica (COLOMBO, 2004). Nesta pesquisa atual há aplicação de Modelo de referência, Medição de segurança de software com o tratamento das medidas de forma matemática e a visão sistêmica da segurança de software.

1.3 OBJETIVO

O objetivo desta proposta de pesquisa parte das seguintes premissas:

- tratar a Segurança de acesso para aplicação web; Segurança de acesso é o grau pelo qual um produto ou sistema protege informação e dados de modo que pessoas ou outros produtos ou sistemas tenham o grau de acesso apropriado aos seus tipos e níveis de autorização aos dados (ISO/IEC 25010; 2011)
- utilizar uma abordagem *top-down*;
- definir um modelo de referência para segurança de acesso;
- medir atributos de segurança;
- desenvolver uma ferramenta para ser utilizada em auditoria da segurança de acesso de aplicação web;
- obter valores quantitativos que mostrem o nível da segurança da aplicação web.

Considerando estas premissas posso definir que esta pesquisa tem como objetivo geral desenvolver uma metodologia de avaliação da segurança de acesso de aplicações web.

O foco é a definição de um modelo de referência para segurança de acesso, e por meio de um processo de análise hierárquica obter a medição de atributos intangíveis e a priorização desses atributos, para apresentar de forma clara o resultado sobre a segurança da aplicação para os interessados (stakeholders) conhecerem o nível de segurança e as prioridades no seu contexto de negócio.

As aplicações Web são sistemas desenvolvidos para atender à gestão das instituições de forma integrada, trazendo maior transparência, rapidez e confiabilidade para as informações corporativas. Esta proposta também retorna um *feedback* para as empresas que desenvolvem software sendo uma das contribuições a identificação dos elementos específicos de Engenharia (Web) que precisam ser reconhecidos e resolvidos antes da apreciação de um processo de Engenharia (Web) a partir de uma perspectiva de segurança. Outra contribuição é que estes elementos podem ser usados para ajudar a orientar iniciativas de melhoria de segurança em (Web) engenharia (GLISSON,

2007). A metodologia também pode ser aplicada à outras propriedades intangíveis dos modelos de qualidade da norma ISO/IEC 25000 (ISO/IEC 25000, 2005).

1.4 CONTEXTO, PROBLEMÁTICA E JUSTIFICATIVA

O problema com a maioria dos softwares de hoje é que contêm falhas e erros que muitas vezes são localizadas e exploradas por atacantes para comprometer a segurança do software. Tais falhas e erros exploráveis ocorrem, porque o software é desenvolvido de forma vulnerável. Meios para melhorar esta situação vão desde a definição de novos critérios e procedimentos da forma como o software é adquirido; mudar os processos, métodos e ferramentas utilizadas para especificar, construir, avaliar e testar o software; a adição de anti-ataque preventivo e reativo com contramedidas para o ambiente em que o software é implantado (GOERTZEL, 2007).

A área de medidas e métricas de segurança coloca problemas difíceis e multifacetadas para os investigadores e profissionais da área. Uma resolução rápida não é esperada e é provável que nem todos os aspectos do problema são solucionáveis. Além disso, apenas alguns desses aspectos que possuem solução, podem ser capazes de serem feitos de forma satisfatória, atendendo às expectativas das características de medição, que são de repetibilidade, reprodutibilidade, relevância, oportunidade e custo.

Vários fatores impedem o progresso em métricas de segurança (JANSEN, 2009):

- A falta de bons estimadores de segurança do sistema;
- A dependência do aspecto humano que é uma entrada qualitativa subjetiva;
- Os meios prolongados e ilusórios comumente utilizados para obter medições;
- A falta de compreensão e conhecimento sobre a composição de mecanismos de segurança.

Jansen propõe várias linhas de pesquisa que abordam esses fatores e poderia ajudar a progredir o estado da arte em métricas de segurança. Foram identificadas as seguintes áreas de pesquisa:

- Modelos formais de medição e métricas de segurança;
- Coleta de dados e análise histórica;
- Técnicas de avaliação de inteligência artificial;
- Métodos de medição concreto e praticáveis;
- Componentes mensuráveis.

Cada área em si é bastante extensa e requer um compromisso para sustentar a investigação em longo prazo e desenvolvimento necessário para ser bem sucedido.

Duas pesquisas tipo *Survey* nos auxiliam a conhecer os pontos mais problemáticos que ocorrem em segurança da informação e aplicação web.

O Instituto Ponemon (PONEMON, 2010), entidade reconhecida em pesquisas de campo nos EUA realizou em 2009 um estudo a pedido das empresas americanas Imperva (IMPERVA, 2013) e Whitehead (WHITEHEAD, 2013) para conhecer o estágio em que as aplicações web estavam perante o quesito segurança.

O estudo observou 638 profissionais de TI e de segurança de TI, com aproximadamente 13 anos de experiência em TI em grandes organizações norte-americanas com um efetivo médio de cerca de 10.000 funcionários. Na maioria das vezes, os respondentes estão envolvidos em atividades de rede, segurança de dados e aplicação, incluindo a garantia de qualidade para o desenvolvimento e testes da segurança de sistemas de software.

A pesquisa mostrou que a camada de aplicação web é o alvo de ataques dos hackers. As razões pelas quais as aplicações estão em risco são resumidas: 70 % não acreditam que suas organizações aloquem recursos suficientes para proteger e assegurar aplicações web críticas; 34 % das vulnerabilidades urgentes não são corrigidas; 38 % acreditam que levariam mais de 20 horas do tempo de um desenvolvedor para corrigir uma vulnerabilidade; 55 % acreditam que os desenvolvedores estão muito ocupados para tratarem das questões de segurança.

A 12^a pesquisa anual de segurança de informação global da Ernst & Young (ERNST&YOUNG, 2009) foi desenvolvida com a ajuda dos clientes em segurança e consultoria, em mais de 60 países. A pesquisa foi realizada entre junho de 2009 e agosto de 2009 com quase 1.900 organizações em todas as grandes indústrias.

Principais resultados da pesquisa foram:

Gerenciamento de riscos:

- Melhorar a gestão de riscos de segurança da informação é uma prioridade de segurança máxima para o próximo ano;
- Ataques externos e internos estão aumentando;
- Represálias dos funcionários separados recentemente tornaram-se uma grande preocupação.

Enfrentar os desafios:

- Disponibilidade de recursos de segurança da informação qualificados é o maior desafio para entregar informação secreta;
- Apesar de a maioria das organizações que mantêm os gastos correntes em segurança da informação, orçamento adequado é ainda um desafio significativo para entregar as iniciativas de segurança;
- treinamento de segurança e programas de conscientização está aquém das expectativas.

Cumprir com os regulamentos:

- Conformidade regulatória continua a ser um fator importante para a segurança da informação;
- Custo de cumprimento a conformidade permanece elevada, com empresas que planejam gastar menos do que gastou no último ano;
- Muito poucas organizações têm tomado as medidas necessárias para proteger as informações pessoais.

Adotando tecnologias:

- Implementação de tecnologias de Prevenção de Vazamento de Dados é a prioridade de segurança para muitas organizações;

- A falta de criptografia nos equipamentos de ponto final continua a ser um risco chave, pois poucas empresas criptografam laptops ou computadores de mesa;
- Virtualização e computação em nuvem estão ganhando uma maior adoção, mas poucas empresas estão considerando as implicações em segurança da informação.

Symantec mantém um dos bancos de dados de vulnerabilidades mais abrangentes do mundo, com relação à segurança da informação, o relatório publicado pela Symantec (FOSSI et al., 2011) no ano de 2010, houve um aumento de 3% para 4% nas atividades digitais maliciosas relacionadas com o Brasil no mundo. O mesmo relatório afirma que foram encontrados 1.656.227 novos artefatos maliciosos (*malware*) o que corresponde a um aumento de 256% (FOSSI et al., 2011). Portanto, devido ao aumento dessas atividades no Brasil e no mundo e ao aumento de potenciais novos alvos, existe uma motivação e preocupação com a segurança de software para traçar um panorama que auxilie os usuários, empresas e instituições a se defender destes artefatos.

Alguns órgãos reguladores internacionais em conjunto com a ISO (*International Organization for Standardization*) e nacionais como a ABNT (Associação Brasileira de Normas Técnicas) estabelecem normas e guias para definir e divulgar as boas práticas de um domínio, que possuam abrangência global podendo ser utilizadas em qualquer parte do mundo nos mesmos moldes e características. Estas exigências em termos da definição e avaliação da qualidade de software e o comportamento do processo de desenvolvimento de software devem ser incorporados aos processos de desenvolvimento de software da instituição e melhorados continuamente. À medida que a tecnologia evolui, novas práticas serão incorporadas num processo de melhoria contínua tanto das normas como também das metodologias em uso (ISO/IEC 27000, 2009).

O conceito de segurança faz parte das características de qualidade atualmente sendo reestruturadas na série ISO/IEC 25000 – *System and Software Engineering – System and Software product Quality Requirements and Evaluation* (SQuaRE), inclusive havendo uma preocupação maior em ressaltar esta característica (ISO/IEC 25010, 2011). Esta nova série descreve um modelo de qualidade, um processo de avaliação, uma diretriz para requisitos

de qualidade e um conjunto de medidas de qualidade. Estes conceitos podem auxiliar na questão crítica para melhorar a segurança do software em aplicações ou domínios específicos.

Este cenário sugere o desenvolvimento de um processo de medição sistematizado. Além disso, motiva mostrar a importância de executar avaliação de segurança de software seguindo um processo definido e de forma sistemática, para garantir a repetibilidade, a reprodutibilidade, a imparcialidade e a objetividade, características estas fundamentais para esse processo (COLOMBO et al., 2012).

1.5 LIMITAÇÕES

Este trabalho se limita à análise de aplicações WEB - Segurança de Aplicação Web em arquitetura cliente-servidor. A Figura 1.1 mostra os diferentes níveis de implementação da segurança, a pesquisa desse trabalho tem o foco em Segurança da Aplicação.

Não estão sendo consideradas as questões de segurança da Rede, de Sistema operacional, e de pessoal que estarão à parte desta pesquisa.

Será trabalhada a “segurança de acesso” (*security*) no modelo mais conhecido e utilizado na literatura: CIDA – Confidencialidade, Integridade, Disponibilidade e Autenticidade. Sendo que os cálculos serão executados para o Modelo de referência de Autenticidade.

Figura 1.1 – Abordagem holística para Segurança (MEIER, 2003)

1.6 ESTRUTURA DO TRABALHO

Este trabalho está estruturado nas seguintes seções. Conceitos auxiliares relacionados a esta pesquisa são descritos inicialmente no Capítulo 2. Estes conceitos são utilizados no desenvolvimento deste trabalho e firmam o que será adotado na pesquisa. O Capítulo 3 traz os conceitos, modelos e trabalhos relacionados com o tema, trabalhos acadêmicos e trabalhos desenvolvidos e utilizados na prática. O Capítulo 4 descreve modelos de metodologia de pesquisa acadêmicos mais utilizados na Engenharia de Produção e detalha o método de pesquisa acadêmica adotado neste trabalho. O Capítulo 5 especifica a metodologia de pesquisa-ação desenvolvida e implementada nesta proposta de medição e priorização de segurança de acesso de aplicações Web. O Capítulo 6 apresenta a aplicação da metodologia para uma aplicação web em que a segurança de acesso é essencial. Finalmente o trabalho apresenta os resultados obtidos nesta pesquisa no Capítulo 7 e por fim conclui, faz uma análise das contribuições apresentadas e os resultados obtidos. Propõe também trabalhos futuros a serem desenvolvidos no âmbito de medição de segurança de aplicação web.

2. CONCEITOS AUXILIARES À PESQUISA

A seguir são apresentados e discutidos conceitos auxiliares a pesquisa, isto é, os conceitos e relacionados ao tema.

2.1 MÉTODO PARA APOIO À DECISÃO

Neste capítulo é apresentado assuntos referentes à mapas cognitivos, métodos de apoio à decisão, metodologia AHP de Saaty, Análise de sensibilidade.

A Análise de Decisão fornece uma estrutura e uma linha sistemática do conhecimento intuitivo para a tomada de decisão, facilitando sua aplicação e perpetuação por transferência de conhecimento. As decisões precisam ser rápidas, o que limita a necessidade de contemplar incertezas; são complexas devido ao número elevado de fatores e suas interdependências; e o mundo se comporta de forma dinâmica se não for tomada a decisão no momento não será mais valida no instante seguinte (MORITA, 2001).

Um problema de Análise de Decisão possui as seguintes características: Complexidade e informações incompletas, Incerteza, Múltiplos Objetivos e conflitantes, Perspectivas diferentes dos participantes, muitas informações que envolvem objetivos concorrentes; Processo de decisão influenciado por diferentes poderes; múltiplas soluções.

O processo de análise de decisão é mostrado na Figura 2.1 e seus elementos são: os valores e os objetivos que são parte do contexto da decisão, as decisões a serem tomadas e devem existir pelo menos duas alternativas para uma tomada de decisão sendo elas decisões sequenciais. Além disso, os eventos incertos e as consequências. Existem métodos de estruturação de problemas de decisão (GOMES,2011), aqui citamos três deles como exemplo:

- Mapas Mentais precisam de características descritivas; organização e decomposição do problema alem de ter representação de causa e efeito.
- Árvore de Decisão fornece uma representação detalhada do problema de decisão; é recomendável para uma visão macroscópica do problema. Seus elementos são decisão de risco; informação imperfeita; decisões sequenciais.

- Diagramas de Influência fornece uma representação compacta do problema de decisão; esconde muitos detalhes; recomendável também para uma visão macro do problema.

Figura 2.1 – Processo de Análise de Decisão (Fonte: CLEMEN 1991 *apud* MORITA, 2001)

Os estudos preliminares indicaram que além dessas metodologias já citadas, a metodologia de Processo de Análise Hierárquica - AHP traz as técnicas que mais se aproximam do problema que é tratado neste trabalho (WANG; WULF, 1997),(SAATY, 2008),(HO, 2008). Assim é um dos métodos mais utilizados para o apoio multicritério à decisão, cujos principais aspectos são: a) visa a orientar o processo intuitivo (baseado no conhecimento e experiência) de tomada de decisão; b) depende dos julgamentos de especialistas ou dos decisores quando não há informações quantitativas sobre o desempenho de uma variável em função de determinado critério; e c) resulta numa medida global para cada uma das ações potenciais ou alternativas, priorizando-as ou classificando-as.

2.2 CONCEITOS ALGÉBRICOS

A revisão algébrica da metodologia utilizada neste trabalho facilita a compreensão dos fundamentos do método de análise hierárquica (SAATY, 2006). Observou-se, depois de estudos matemáticos que o método numérico apresentado neste item é mais amigável, de menos complexidade e de mais fácil compreensão para a determinação dos autovalores e autovetores. Dentre os métodos numéricos, o método da potência (iteração de vetores) é o mais simples haja vista que fornece tanto a convergência do autovalor como do autovetor (BRONSON, 1989). A convergência é importante, pois na execução dos cálculos dos modelos de segurança será utilizado um software que automatiza os cálculos e, portanto a convergência passa a ser algo transparente para o usuário desse software ou leitor do trabalho.

Esses conceitos derivam da teoria de matrizes. Uma matriz será uma matriz quadrada, positiva, diagonal e recíproca quando possuindo a seguinte forma:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \dots a_{1n} \\ a_{21} & a_{22} & a_{23} \dots a_{2n} \\ a_{31} & a_{32} & a_{33} \dots a_{3n} \\ \vdots & \vdots & \vdots \vdots \vdots \\ a_{n1} & a_{n2} & a_{n3} \dots a_{nn} \end{bmatrix}$$

Os elementos a_{11} , a_{22} , $a_{33}, \dots$, a_{nn} formam a diagonal, também chamada de diagonal principal (BRONSON, 1989). Uma matriz A é positiva se todos os seus elementos forem reais e positivos. Um vetor coluna não nulo W de uma matriz quadrada A é um vetor próprio à direita (autovetor à direita) se existir um escalar λ tal que:

$$AW = \lambda W \quad (1)$$

Um vetor linha não nulo X de uma matriz quadrada A é um vetor próprio à esquerda (autovetor à esquerda) se existir um escalar λ tal que:

$$XA = \lambda X$$

Em álgebra linear, um escalar λ que satisfaz essa equação é valor próprio (ou autovalor) da matriz A. A partir da equação (1) pode-se expressar a equação característica da matriz A.

$$AW = \lambda W \rightarrow AW - \lambda W = 0 \rightarrow \det (A - \lambda I)W = 0$$

A: $V \rightarrow V$ se existir um vetor X diferente de zero tal que

$$AW = \lambda_{\max} W$$

O vetor W é chamado vetor próprio ou autovetor. Os autovalores de uma dada matriz quadrada A de dimensão $N \times N$ são os N números que resumem as propriedades essenciais daquela matriz. O autovalor de A é um número λ tal que, se for subtraído de cada entrada na diagonal de A , converte A numa matriz singular (1).

Subtrair um escalar λ de cada entrada na diagonal de A é o mesmo que subtrair λ vezes a matriz identidade I da matriz A . Portanto, λ é um autovalor se e somente se a matriz $(A - \lambda I)$ for singular. Uma matriz é singular quando seu determinante é igual a zero. No caso da equação (1), $(A - \lambda_{\max}) W = 0$ isso só vai acontecer se W for igual a zero ou $\text{Det}(A - \lambda_{\max}) = 0$. $W = 0$ não interessa então tem que calcular o determinante. Generalizando o cálculo do determinante, obtém-se o seguinte polinômio característico, onde n é o número de ordem da matriz.

$$\text{Det} \begin{bmatrix} a_{11} - \lambda & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} - \lambda & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} - \lambda \end{bmatrix} = 0$$

$$\text{Det}(A - \lambda I) = b_n \lambda^n + b_{n-1} \lambda^{n-1} + \dots + b_2 \lambda^2 + b_1 \lambda + b_0 = 0,$$

Então o polinômio característico será:

$$b_n A^n + b_{n-1} A^{n-1} + \dots + b_2 A^2 + b_1 A + b_0 I = 0$$

As principais propriedades dos valores e vetores próprios são:

- a) a soma dos valores próprios de uma matriz é igual à soma dos elementos da sua diagonal principal o que se chama “traço”, em álgebra;
- b) o produto dos valores próprios de uma matriz, considerando a sua multiplicidade, é igual ao determinante dessa matriz; e
- c) os vetores próprios correspondentes a diferentes valores próprios são linearmente independentes. Em álgebra linear, um conjunto S de vetores diz-se linearmente independente se nenhum dos seus elementos for combinação linear dos outros.

Os vetores e valores próprios poderão ser obtidos por cálculos algébricos e por métodos numéricos.

A matriz quadrada diz-se recíproca e positiva quando $a_{ij}=1/a_{ji}$, para todo $a_{ij} > 0$. Supondo uma matriz B de dimensão 3x3, recíproca e positiva onde $a_{21}= 1/a_{12}$, $a_{31}= 1/a_{13}$, $a_{32}= 1/a_{23}$ e $a_{ii}=1$.

$$B=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}=\begin{bmatrix} 1 & a_{12} & a_{13} \\ 1/a_{12} & 1 & a_{23} \\ 1/a_{13} & 1/a_{23} & 1 \end{bmatrix}$$

A matriz B será consistente quando $a_{ij}= a_{ik} \cdot a_{kj}$. Neste caso $a_{23} = a_{21} \cdot a_{13}= a_{13}/a_{12}$

$$B=\begin{bmatrix} 1 & a_{12} & a_{13} \\ 1/a_{12} & 1 & a_{13}/a_{12} \\ 1/a_{13} & a_{12}/a_{13} & 1 \end{bmatrix}$$

Observe que quando B for consistente os vetores linha da matriz B (B_1 , B_2 e B_3) passam a ser linearmente dependentes, ou seja, $B_1= \alpha_1 \cdot B_2= \alpha_2 \cdot B_3$, onde α_1 e α_2 valem a_{12} e a_{13} , respectivamente. Nota-se que, se a matriz B for escalonada tem-se apenas a primeira linha da matriz não nula. Pode-se dizer que a matriz possui posto 1, ou seja, só existe um autovalor diferente de zero que satisfaz a equação característica. Também, pode-se afirmar que

$$\det(B)=0: \det(B)=1+a_{12} \cdot a_{13}/a_{12} \cdot 1/a_{13}+1/a_{12} \cdot a_{12}/a_{13} \cdot a_{13}- \\ (a_{13} \cdot 1/a_{13}+a_{12} \cdot 1/a_{12}+a_{13}/a_{12} \cdot a_{12}/a_{13}) =3-3=0.$$

A equação característica de B seria:

$$\det (B-\lambda I)=\begin{bmatrix} 1-\lambda & a_{12} & a_{13} \\ 1/a_{12} & 1-\lambda & a_{13}/a_{12} \\ 1/a_{13} & a_{12}/a_{13} & 1-\lambda \end{bmatrix} = 0$$

$$\det (B-\lambda I)=((1-\lambda)^3+1+1)-((1-\lambda) + (1-\lambda)+1-\lambda)) \rightarrow = (1-3\lambda+3\lambda^2-\lambda^3+2)-(3-3\lambda)=(3\lambda^2-\lambda^3).$$

Generalizando essa equação para dimensão nxn.

$$\det(A-\lambda I)=(-1)^n \lambda^n + (-1)^{n-1} (\text{traço} A) \lambda^{n-1} + \dots + b_2 \lambda^2 + b_1 \lambda^1 + b_0 I =$$

$$\det(A-\lambda I)=(-1)^n \lambda^n + (-1)^{n-1} (\text{traço} A) \lambda^{n-1} = \lambda^n - (\text{traço} A) \lambda^{n-1}$$

$$= \lambda^{n-1} (\lambda - (\text{traço} A)) = 0.$$

Portanto, λ é igual a zero com multiplicidade n-1 e $\lambda_{\max}$ é igual ao traço da matriz A com multiplicidade 1. (BRONSON, 1989).

Estes conceitos de cálculos algébricos com a adoção dos conceitos de autovalores e autovetores dão a base matemática para a questão de medição e priorização de atributos não mensuráveis originalmente.

2.3 MODELO AHP

O Processo de Análise Hierárquica (AHP) (SAATY, 1980) que fornece um procedimento compreensivo e racional para estruturar um problema, assim como representar e quantificar seus elementos, além de relacionar esses elementos com as metas globais e para encontrar soluções alternativas.

Nessa metodologia os usuários, devem decompor o problema de decisão em uma hierarquia de subproblemas mais facilmente compreendidos, onde cada um pode ser analisado independentemente. Os elementos dessa hierarquia podem relacionar-se com qualquer aspecto do problema de decisão – tangível ou intangível, ser medido com precisão ou estimado grosseiramente, ser de fácil ou de difícil compreensão – ou seja, qualquer coisa que se aplique à decisão. Após a construção da hierarquia, como mostra a Figura 2.2, um peso numérico, ou prioridade, é atribuído para cada elemento da hierarquia, permitindo que elementos distintos e frequentemente incomensuráveis sejam comparados entre si de maneira racional e consistente.

Esta potencialidade distingue o AHP de outros métodos de tomada de decisão. O AHP é mais útil quando equipes estão envolvidas em problemas complexos, especialmente aqueles de grande importância como a segurança de software, que necessitam de percepção humana e cuja resolução terá repercussão de longo-prazo (SAATY, 2008). O problema deve ter uma estrutura hierárquica bem definida e Saaty (SAATY, 1980) cita que o método AHP deve respeitar quatro aspectos importantes, que tornam o método robusto e confiável. Esses quatro aspectos são os Axiomas:

- Axioma 1. Comparações recíprocas - os elementos comparados 2 a 2 pelo decisor devem satisfazer a condição de reciprocidade: se A é três vezes mais preferido que B, B será 1/3 vezes mais preferidas que A.
- Axioma 2. Homogeneidade - os elementos de um mesmo nível hierárquico devem possuir o mesmo grau de importância dentro do seu nível.

Axioma 3. Independência: os elementos de um nível da hierarquia devem ser mutuamente excludentes entre si, e quando comparados par a par pelos decisores, os pesos dos critérios devem ser independentes das alternativas.

Axioma 4. Exaustividade: assume-se que a hierarquia do problema de decisão está completa, ou seja, contém todos os critérios e alternativas relativos ao problema.

Figura 2.2 – Estrutura Hierárquica do AHP

A metodologia AHP pode ser explicada pela seguinte sequência de sete etapas:

Etapa 1: Entendimento do Problema de Decisão O sistema é estudado em detalhes com o foco de identificar o objetivo do processo decisório, os critérios/sub-critérios baseados nos valores, crenças e convicções do decisor, e as alternativas para a solução do problema.

Etapa 2: Hierarquização do Problema de Decisão O problema de decisão é dividido em níveis hierárquicos com a finalidade de facilitar a compreensão e avaliação. A Figura 2.2 ilustra a estruturação dos critérios na formulação hierárquica.

Etapa 3: Coleta dos julgamentos par a par dos especialistas. Uma vez montada a estrutura há a necessidade da coleta de dados referente aos julgamentos dos especialistas ou decisores na comparação par a par, tanto das alternativas sob o enfoque de cada sub-critério, quanto dos sub-critérios e critérios em relação ao nível imediatamente superior.

Geralmente, as opções qualitativas dos especialistas, em relação a um determinado critério, são coletadas por meio de questionários, conforme exemplo apresentado na Tabela 2.1. Neste exemplo, o especialista na primeira comparação considerou que A possui uma importância muito maior em relação a B, na segunda comparação considerou que C possui uma importância entre pequena e grande em relação a A e na terceira comparação considerou que C possui uma importância absoluta em relação a B.

Tabela 2.1 - Questionário para Comparação par a par de 3 elementos - exemplo

	Absoluta	Muito Grande	Grande	Pequena	Igual	Pequena	Grande	Muito Grande	Absoluta	
A		X								B
A						X				C
B									X	C

Estes julgamentos, posteriormente, são convertidos em índices quantitativos utilizando uma escala própria que varia de 1 a 9, denominada Escala Fundamental, proposta por Saaty em 1980. A Tabela 2.2 ilustra a escala fundamental de Saaty:

Tabela 2.2 - Escala de Saaty para importâncias relativas

Importância relativa do objetivo	Recíproco	Definição da escala	Explicação
1	1	Igual importância	As duas atividades contribuem igualmente para o objetivo.
3	1/3	Pouca importância	A experiência e o juízo favorecem uma atividade em relação à outra
5	1/5	Forte importância	A experiência ou juízo favorece fortemente uma atividade em relação à outra.
7	1/7	Demonstra importância sobre a outra	Uma atividade é muito fortemente favorecida em relação à outra. Pode ser demonstrada na prática.
9	1/9	Importância absoluta	A evidência favorece uma atividade em relação à outra, com o mais alto grau de segurança.
2,4,6,8	1/2, 1/4, 1/6, 1/8	Valores intermediários de importância	Quando se procura uma condição de compromisso entre duas definições.

No exemplo apresentado na Tabela 2.1, observam-se os seguintes índices convertidos pela escala fundamental nas comparações par a par: 7, 4, e 9, respectivamente.

Etapas 4: Construção das matrizes de decisão. Cada questionário elaborado na etapa anterior deve ser organizado em uma matriz quadrada, denominada matriz de decisão, de ordem igual ao número de elementos comparados. A

inserção dos elementos desta matriz segue as seguintes regras, Saaty (SAATY, 1980):

Regra 1: $a_{ij}=1/a_{ji}$. Indica que se na comparação de A_i em relação a A_j for obtido o índice 7, entra-se na matriz o valor de 7. Consequentemente, na comparação de A_j em relação a A_i , entra-se na matriz o valor de 1/7. Logo, se $a_{ij}=a$, então $a_{ji}=1/a$ para todo $a>0$; e

Regra 2: $a_{ii}=1$ para todo i . Portanto, indica que qualquer critério comparado a ele próprio possui igual importância na escala fundamental. Estas regras caracterizam que a matriz de decisão é sempre uma matriz quadrada, recíproca e positiva e deve possuir a seguinte forma:

$$\begin{bmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 1/a_{12} & 1 & a_{23} & \dots & a_{2n} \\ 1/a_{13} & 1/a_{23} & 1 & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \dots & \dots & 1 \end{bmatrix}$$

A matriz positiva goza de algumas propriedades, sendo que a principal para o AHP é a definida pelo Teorema de Perron: *“Uma matriz quadrada positiva tem um valor próprio (autovalor) de multiplicidade 1 igual ao seu raio espectral², não havendo nenhum valor próprio tão grande em valor absoluto. Existe, além disso, um vetor próprio (autovetor) à direita e um vetor próprio à esquerda correspondentes ao valor espectral somente com componentes positivas”* (PERRON,1907). Esta última frase do teorema de Perron garante que o autovetor, associado ao autovalor de maior valor absoluto, possui somente componentes positivos. Saaty (SAATY, 1980) demonstrou que o melhor processo para obter o vetor de prioridades dos elementos da matriz de decisão é o método do autovetor à direita. Sendo assim, quando não especificado, a expressão autovetor no AHP estará sempre associada ao autovetor à direita.

---

² O raio espectral de uma matriz quadrada é o maior valor próprio em valor absoluto.

Referente ao questionário apresentado na Tabela 2.1 e utilizando as regras apresentadas obtém-se a seguinte matriz de decisão:

	A	B	C
A	1	4	1/7
B	1/4	1	1/9
C	7	9	1

Observa-se que esta matriz de decisão de ordem 3, embora recíproca e positiva, não é consistente, pois o elemento $a_{23} \neq a_{21} * a_{13} \rightarrow 1/9 \neq 1/4 * 1/7$. As matrizes de decisão de ordem 1 e 2 serão sempre consistentes. Na etapa 6 deste item será apresentada a metodologia para verificar a Razão de consistência de uma matriz de decisão proposta por Saaty. Entretanto, antes é necessário obter os autovalor máximo da matriz de decisão e seu autovetor associado.

Etapa 5: Obtenção dos autovalores e autovetores das matrizes de decisão. Pode-se calcular o autovalor e autovetor de qualquer matriz por dois métodos: algébrico e numérico. O cálculo algébrico é efetuado a partir da equação característica da matriz. A equação característica da matriz de decisão descrita pela Tabela 2.1 é a seguinte:

	A	B	C
A	$1 - \lambda$	4	1/7
B	1/4	$1 - \lambda$	1/9
C	7	9	$1 - \lambda$

$$\begin{aligned} \text{Det (M-}\lambda\text{I)} &= ((1-\lambda)^3 + 28/9 + 9/28) - ((1-\lambda) + (1-\lambda) + (1-\lambda)) \rightarrow \\ &= (1 - 3\lambda + 3\lambda^2 - \lambda^3 + 865/252) - (3 - 3\lambda) \rightarrow \\ &= (3\lambda^2 - \lambda^3 + 1,4325) = 0. \end{aligned}$$

A equação característica desta matriz tem como solução o valor próprio $\lambda = 3,1448$ de multiplicidade 1, $\lambda = -0,0724 + 0,6710i$ de multiplicidade 1; e $\lambda = -0,0724 - 0,6710$ de multiplicidade 1.

Observa-se que a soma dos autovalores calculados é igual ao traço da matriz original. Conforme o teorema de Perron enunciado anteriormente, é necessário

obter o maior autovalor ($\lambda_{\max}$) que estará associado ao autovetor principal da referida matriz positiva. Portanto, o $\lambda_{\max}$ será 3,1448.

Uma vez obtido o $\lambda_{\max}$ é necessário calcular o autovetor à direita associado de modo que $AW = \lambda W$. Desta forma, deve-se construir as seguintes equações:

$$\begin{bmatrix} 1 & 4 & 1/7 \\ 1/4 & 1 & 1/9 \\ 7 & 9 & 1 \end{bmatrix} * \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} = 3,1448 \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix}$$

$$w_1 + 4w_2 + 1/7w_3 = 3,1448w_1$$

$$1/4w_1 + 1w_2 + 1/9w_3 = 3,1448w_2$$

$$7w_1 + 9w_2 + 1w_3 = 3,1448w_3$$

$$W = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} = \begin{bmatrix} 2,7404w_2 \\ w_2 \\ 13,1385w_2 \end{bmatrix} = w_2 \begin{bmatrix} 2,7404 \\ 1 \\ 13,1385 \end{bmatrix} = \begin{bmatrix} 0,2086 \\ 0,0761 \\ 1 \end{bmatrix}$$

Como se pode observar o processo algébrico para a determinação de valores e vetores próprios é impraticável para a maioria das matrizes de grande dimensão. Em sua substituição foram desenvolvidos métodos numéricos. Cada método inclui critérios de parada, geralmente um teste para se determinar quando se atinge determinado grau de precisão (se os resultados forem convergentes) e um limite para o número de iterações a serem realizadas (no caso de não haver convergência). O método numérico mais simples para se obter o máximo autovalor e seu autovetor associado é o método da potência (iteração de vetores).

A ideia principal é obter iterações de modo que $X_{k+1} = c A X_k$, onde k é o número de iterações e c é uma constante de normalização que previne X_{k+1} de ser muito grande. Após várias iterações ($k \rightarrow \infty$), X_{k+1} convergirá para o autovetor principal W_1 de A , correspondente ao autovalor $\lambda_{\max} = \lambda_1$. Assume-se que exista um autovalor dominante λ_1 , de tal forma que, $\lambda_1 > \lambda_2 > \lambda_3 \dots > \lambda_n$. Inicializa-se a iteração construindo-se um vetor inicial X_0 . Para observar porque este processo converge decompõe-se o vetor X_0 no espaço em função dos autovetores associados aos $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_n$, obtendo-se:

$$X_0 = c_1W_1 + c_2W_2 + \dots + c_nW_n.$$

Sabe-se que para qualquer autovalor obtido vale a expressão:

$$AW = \lambda W$$

$$A^2W = A(AW) = A\lambda W = \lambda AW = \lambda^2W$$

$$A^3W = A^2(AW) = A^2\lambda W = \lambda A^2W = \lambda^3W$$

$$A^k W = A^{k-1}(AW) = A^{k-1} \lambda W = \lambda A^{k-1} W = \lambda^k W$$

Portanto:

$$X_k = AX_{k-1} = \dots = A^k X_0 = c_1 \lambda_1^k W_1 + c_2 \lambda_2^k W_2 + \dots + c_n \lambda_n^k W_n.$$

Dividindo-se tudo $c_1 \lambda_1^k$, obteremos:

$$\frac{X_k}{c_1 \lambda_1^k} = \frac{A^k X_0}{c_1 \lambda_1^k} = W_1 + \frac{c_2 \lambda_2^k W_2}{c_1 \lambda_1^k} + \frac{c_n \lambda_n^k W_n}{c_1 \lambda_1^k} =$$

$$\frac{X_k}{c_1 \lambda_1^k} = \frac{A^k X_0}{c_1 \lambda_1^k} = W_1 + \frac{c_2}{c_1} \left(\frac{\lambda_2}{\lambda_1} \right)^k W_2 + \dots + \frac{c_n}{c_1} \left(\frac{\lambda_n}{\lambda_1} \right)^k W_n$$

Os termos $\left(\frac{\lambda_i}{\lambda_1} \right)^k$, $i \neq 1$ são menores que 1 e tendem a zero.

Portanto, a expressão tende a convergir para o autovetor principal W_1 , após várias iterações ($k \rightarrow \infty$). A razão de convergência é determinada pela relação do segundo maior autovalor pelo maior autovalor. Quanto menor esta razão, mais rápida será a convergência:

$$\frac{|\lambda_i|}{|\lambda_1|}$$

O algoritmo usual para a utilização deste método é o seguinte:

- define-se a precisão desejada do autovalor (P) e o número máximo de iterações;
- inicializa-se X_0 , construindo-se um vetor coluna não nulo e um contador de iterações. A sugestão é iniciar com um vetor coluna unitário;
- calcula-se o vetor $Y_k = A * X_{k-1}$;
- determina-se o maior valor de Y_k que será representado por $\lambda_k = \max(Y_k)$;
- faz-se $X_k = (1/\lambda_k) * Y_k$;
- se $|\lambda_k - \lambda_{k-1}| < P$, o algoritmo deve parar. O autovalor e autovetor associado são λ_k e X_k . No caso de $|\lambda_k - \lambda_{k-1}| > P$, deve continuar; e finalmente;
- adiciona-se 1 a k. Se k for maior que o número máximo de iterações a serem efetuadas, para-se. Caso contrário, retorna-se (para a alínea c).

Outra maneira de se utilizar o método da potência é elevando-se a matriz de decisão a uma potência elevada e multiplicá-la por um vetor coluna unitário. Em seguida deve-se normalizar o vetor resultante pela norma da soma. Entretanto, esta metodologia converge apenas para o autovetor. Devendo-se obter o autovalor a partir do autovetor convertido por meio da equação $AW = \lambda W$. Exemplificando o método, utilizando-se a matriz de decisão descrita na Tabela 2.3, escolhe-se $X_0 = (1 \ 1 \ 1)^T$, obtendo-se as seguintes iterações:

Iteração 1

$$Y_1 = A X_0 = \begin{bmatrix} 1 & 4 & 1/7 \\ 1/4 & 1 & 1/9 \\ 7 & 9 & 1 \end{bmatrix} * \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 5,1429 \\ 1,3611 \\ 17 \end{bmatrix}$$

$$\lambda_1 = 17 \quad X_1 = \frac{1}{\lambda_1} * Y_1 = [0,3025 \quad 0,0801 \quad 1]^T$$

Iteração 2

$$Y_2 = A X_1 = \begin{bmatrix} 1 & 4 & 1/7 \\ 1/4 & 1 & 1/9 \\ 7 & 9 & 1 \end{bmatrix} * \begin{bmatrix} 0,3025 \\ 0,0801 \\ 1 \end{bmatrix} = \begin{bmatrix} 0,7656 \\ 0,2668 \\ 3,8382 \end{bmatrix}$$

$$\lambda_2 = 3,8382 \quad X_2 = \frac{1}{\lambda_2} * Y_2 = [0,1995 \quad 0,0695 \quad 1]^T$$

As iterações devem continuar com quatro casas decimais até a convergência para o autovalor 3,1448 associado ao vetor $(0,2085 \ 0,0761 \ 1)^T$

Tabela 2.3 – Iterações do método das potências

Iterações	Autovetor			Autovalor
0	1	1	1	0
1	0,3025	0,0801	1	17
2	0,1995	0,0695	1	3,8382
3	0,2053	0,0763	1	3,0220
4	0,2091	0,0764	1	3,1235
5	0,2087	0,0761	1	3,1518
6	0,2085	0,0761	1	3,1455
7	0,2085	0,0761	1	3,1445
8	0,2086	0,0761	1	3,1448
9	0,2085	0,0761	1	3,1449
10	0,2085	0,0761	1	3,1448

Etapa 6: A Razão de Consistência da matriz de decisão. Conforme visto anteriormente, uma matriz recíproca, positiva e consistente possui apenas um autovalor diferente de zero e igual ao número de ordem da matriz. Saaty (SAATY, 2008) demonstrou que uma matriz A recíproca e positiva possui seu

autovalor máximo $\lambda_{\max} \geq n$. A igualdade somente é possível quando a matriz A for consistente.

O Índice de Consistência (IC) foi definido como:

$$IC = (\lambda_{\max} - n) / (n - 1), \quad (xx)$$

Onde $\lambda_{\max}$ é o máximo autovalor da matriz de decisão e n é o número de ordem da matriz. Saaty propôs a Tabela 2.4 com os Índices Aleatórios, do inglês *Random Indices* – RI para matrizes de ordem 1 a 10.

Tabela 2.4 – Índice de Consistência proposto por Saaty

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0,52	0,89	1,11	1,25	1,35	1,40	1,45	1,49

O Índice de Consistência (IC) calculado para a matriz de decisão é comparado com o valor de RI para fornecer a Razão de Consistência (RC), de forma que $RC = IC / RI$. Se RC for menor que 0,1, então os julgamentos da matriz de decisão são considerados consistentes, caso contrário, existe alguma inconsistência nos julgamentos e o especialista pode ser solicitado para rever a sua opinião.

Utilizando-se os resultados obtidos na etapa anterior referente à matriz de decisão de 3ª ordem representativa dos julgamentos descritos na Tabela 2.1, verifica-se a sua razão de consistência. Neste caso teremos $n=3$, $\lambda_{\max}=3,1448$ que proporcionam os seguintes cálculos:

$$IC = (\lambda_{\max} - n) / (n - 1) = (3,1448 - 3) / 2 = 0,0724$$

$$RC = IC / RI = 0,0724 / 0,52 = 0,14.$$

Como o RC é maior do que 0,1, então será necessário solicitar que o especialista revise seus julgamentos antes de considerar o autovetor obtido como o vetor prioridade.

Observando a utilização da metodologia AHP na área de gestão de projetos e de fornecedores, o cálculo do RC ajudou a verificar a consistência dos julgamentos dos especialistas.

Segundo Bastos (BASTOS et al., 2011), nesta etapa da metodologia é determinada a Razão de Consistência, ou seja, evidencia a consistência sobre as notas de julgamento propostas pelos especialistas pois, dependendo da

julgamento proposto, o resultado indicará se os critérios estão consistentemente relacionados.

Mesmo quando os julgamentos par a par estão fundamentados na experiência e conhecimento de profissionais e especialistas, inconsistências podem ocorrer, principalmente quando existir um grande número de julgamentos (COSTA et al, 2011)

Segundo Bible (BIBLE, 2011), decisões precisas são geralmente baseadas em julgamentos consistentes, mas algum grau de inconsistência é tolerável. Ser completamente consistente significa que para cada julgamento realizado, relações comparativas são mantidas, por exemplo: se o critério A é maior que o critério B, e o critério B é maior do que o critério C o critério A sempre será julgado como maior do que o critério C. Segundo o autor, o AHP permite algum grau de inconsistência, que é calculado por meio da Razão de Consistência.

Segundo Bible (BIBLE, 2011) uma Razão de Consistência igual ou menor do que 0.10, ou 10%, é considerado aceitável. Se o valor da RC encontrado for muito alto, pode indicar que tanto indivíduos, ou o grupo, tem diferentes interpretações sobre o significado dos elementos da hierarquia. Nestes casos, pode ser necessário algum tipo de clarificação e ajustes. O autor recomenda que o facilitador revise as inconsistências, identifique soluções e as discuta com os especialistas. As mudanças necessárias devem ser guiadas pelo facilitador.

So (SO et al., 2006) sugere que a consistência das comparações par a par sejam checadas afim de mensurar a intensidade ou grau da consistência e, para isso, deve calcular a Razão de Consistência (RC) das matrizes.

Segundo Saaty o objetivo de calcular a Razão de Consistência é permitir a avaliação da inconsistência em função da ordem máxima da matriz de decisão.

Etapas 7: Processo de Agregação dos Vetores de Prioridade. Após obter os vetores de prioridades das matrizes de decisão referente às alternativas sob cada subcritério, dos subcritérios em relação aos seus critérios superiores e dos critérios em relação ao objetivo principal, devem ser gerados os valores finais das alternativas.

2.4 POR QUE USAR O AHP

Ho (2008) observa que o AHP, na ocasião de seu trabalho, era aplicado em catorze diferentes campos, em diferentes tipos de problemas. O autor cita ainda que as áreas mais populares de aplicação do AHP são: logística e manufatura, representando 59,1% dos trabalhos publicados, de um total de 66 artigos, cuja distribuição é apresentada na Tabela 2.5. Pode-se notar que a utilização do método AHP ainda é pouco explorada pelo Gerenciamento de Projetos, permitindo com que esse trabalho contribua para a ampliação dos horizontes de aplicação dessa metodologia.

Tabela 2.5 - Aplicações do AHP Fonte: Ho (2008)

Área	Qtd. de Trabalhos Publicados
Logística	21
Manufatura	18
Governo	4
Educação	4
Negócios	3
Meio Ambiente	3
Militar	3
Agricultura	2
Saúde	2
Marketing	2
Indústria	1
Serviços	1
Esporte	1
Turismo	1

O uso do AHP nesta pesquisa pode ser resumido como:

- Os modelos de *Multicriteria Decision Aid* (MCDA) - Método Multicritério de Auxílio/Apoio à Decisão ajudam a quantificar os dados pertinentes ao problema. Os modelos multicritério são utilizados quando se precisa encontrar o conjunto ótimo (multi objetivo) como solução de um problema, mesmo que para isso não faça parte da solução nenhum ponto de máximo ou de mínimo, como acontece nas otimizações onde se utiliza a Pesquisa Operacional *hard*, como a metodologia *Simplex*, por exemplo. Os métodos de MCDA precisam

quantificar os critérios utilizados na modelagem do problema, de forma que se tenha o nível de preferência de um em relação ao outro, que se obtém por meio dos julgamentos realizados com as comparações par a par entre os critérios e subcritérios.

- O AHP divide o problema em níveis hierárquicos; fornece uma escala para que os *experts* possam quantificar seus julgamentos de forma par a par entre os múltiplos critérios; usa método matemático (baseado na utilização de autovalores e autovetores) para encontrar as prioridades, prioriza as alternativas.

A aplicação do AHP tem início com a estruturação do problema em uma estrutura hierárquica. Por meio da escala fundamental de Saaty os *experts* realizam as comparações par a par entre os critérios em relação ao objetivo do problema e entre os subcritérios em relação a seus critérios.

Segundo PERRIN (2008), ao contrário de diversos tipos de matrizes de decisão que produzem as médias ponderadas padrão, o AHP é diferente e certamente único, pois permite que os usuários tomem decisões em cenários complexos, com pessoas que podem estar em desacordo ou em conflito, e permite que os usuários não considerem apenas atributos quantitativos mensuráveis, mas também suas preferências individuais para solução de um problema.

PERRIN (2008) também destaca que o AHP permite que decisões sejam tomadas baseadas em diferentes níveis de experiência do fato e usando critérios que não são facilmente comparáveis, como a comparação entre atributos quantitativos e qualitativos.

BIBLE (2011) destaca que o AHP auxilia os decisores pelo fato de:

- Estruturar a complexidade de um problema de decisão por meio da organização dos vários elementos de um problema em uma hierarquia;
- Avaliar por meio de comparações par a par, a importância relativa dos objetivos e a preferência relativa das alternativas identificadas;
- Auxiliar na priorização pela combinação de informações intangíveis, advindas da experiência e intuição dos decisores, e tangíveis como dados quantitativos;

- Sintetizar os resultados de objetivos concorrentes e de pontos de vista diferentes.

O método permite certo grau de inconsistência nos julgamentos, e pela Razão de Consistência RC, controla-se o grau de inconsistência dos julgamentos dos *experts* na fase de iterações da convergência do método numérico.

Com o aprimoramento da Metodologia AHP, foi introduzida uma abordagem de *Ratings* (GOMES, 2010), que estabelece categorias para critérios e subcritérios, neste caso não se utiliza a visão de Alternativas, mas faz uma ponderação final. A abordagem *ratings* fornece ao decisor outra forma de trabalhar com as alternativas. Utilizando *ratings*, não será necessário realizar comparações par a par entre as alternativas para cada um dos critérios avaliados. Nesse caso simplesmente criam-se categorias e classificam-se as alternativas nessas categorias, como mostra o esquema da Figura 2.3. São necessárias comparações par a par entre os diferentes níveis das categorias criadas, para determinar o nível de importância de um nível em relação ao outro.

Figura 2.3 - Estrutura Hierárquica com *Ratings* Fonte: GOMES (2010)

Ratings é uma alternativa para reduzir a quantidade de comparações em um problema complexo, e uma forma de permitir que se use o AHP em problemas com quantidade de alternativas superior a 7 ou 9. (lembre-se que deve haver no máximo 9 elementos em cada matriz, 7 ± 2) (MILLER, 1956)(NASCIMENTO, 2010).

A análise de sensibilidade serve para medir o grau de robustez do modelo, que reflete quão estável está em relação à variação nos valores dos julgamentos. A

Análise de Sensibilidade faz uma checagem dos valores estimados e se estiverem em desacordo permite uma nova estimativa (BUTLER, 2002).

Existe uma ferramenta pública que suporta a metodologia AHP chamada SuperDecision® (SUPERDECISION®, 2010), e que será utilizada na parte prática deste trabalho.

2.5 EXPERIÊNCIA EM AVALIAÇÃO DE SOFTWARE

Experiência com avaliação MEDE-PROS® - Método de Avaliação da Qualidade de Produto de Software (MEDE-PROS, 2006) também pode nos ajudar na avaliação da segurança de software, foco deste trabalho.

MEDE-PROS® foi desenvolvido de modo empírico, onde um apoio estatístico atribuía valores numéricos para as respostas do *checklist*, para as pontuações positivas e negativas; fazia a normalização dos resultados finais para obter uma nota para os pontos de avaliação da qualidade de produtos de software sob a perspectiva do usuário final.

Essa avaliação foi baseada na aplicação de Normas Internacionais: ISO/IEC 9126-1 (NBR ISO/IEC 9126-1, 2002) e NBR ISO/IEC 12119 (NBR ISO/IEC 12119, 1998), que definem as 6 (seis) características de qualidade de software que devem estar presentes em todos os produtos: Funcionalidade, Confiabilidade, Portabilidade, Usabilidade, Eficiência e Manutenibilidade e também requisitos de qualidade para um pacote de software.

Em torno de 500 avaliações de produtos de software realizadas, entre 1993 e 1998, utilizaram um Modelo de Qualidade como referência e seguiu um processo de avaliação, esta experiência em avaliação aconteceu para o Prêmio Assespro, que tinha como objetivo a disseminação de critérios de qualidade tanto para os desenvolvedores como também para os adquirentes. Foi possível acompanhar a evolução de melhoria da qualidade em softwares de vários produtores que participaram nas edições do Prêmio (ROCHA, 2001).

Quanto à Chamada Nacional Softex, experiências de avaliação com o objetivo de selecionar projetos de empresas brasileiras, que desejassem realizar negócios comerciais para produtos de software e serviços desenvolvidos no Brasil no mercado externo e que pretendiam utilizar linhas de crédito especiais oferecidas pelo governo brasileiro proveniente de agências de promoção

industrial e tecnológica, tais como CNPq, FINEP, BNDES e outros. Esta experiência também possibilitou a criação de uma metodologia de avaliação com a utilização de um Modelo de referência de qualidade para este contexto em específico.

Quanto ao PNAFM - Programa Nacional de Apoio à Gestão Administrativa e Fiscal dos Municípios Brasileiros, primeira fase (PNAFM, 2001), projeto cuja meta era chamada de publicação de pré-qualificação das empresas e produtos de software de gestão para os municípios brasileiros, com menos de 50.000 habitantes. Com este projeto, o Ministério da Fazenda, olha para a estabilidade macroeconômica através do equilíbrio fiscal autossustentável, com base em uma política transparente e eficiente pública para as receitas públicas municipais e gestão das despesas. <http://www.ucp.fazenda.gov.br/PNAFM> (PNAFM, 2001). Esta experiência possibilitou o desenvolvimento de onze modelos de qualidade e métodos de avaliação para cada uma das onze áreas de aplicações de software do Programa.

A avaliação de aplicação web em relação à segurança requer a identificação das necessidades de segurança do cliente e uma avaliação dos recursos do produto. Esta pesquisa tem como foco conciliar os diversos conceitos para tratar da segurança com abordagens específicas de segurança de software, de informação ou mesmo de TI.

2.6 ANÁLISE E DISCUSSÃO

Este Capítulo ressaltou a metodologia de apoio à decisão, neste contexto o método de análise hierárquica se mostrou muito adequado para o objetivo desta pesquisa. A metodologia AHP com sua sequência de sete etapas deve apoiar o desenvolvimento da metodologia de medição considerando a existência de propriedades intangíveis e os cuidados que devem ser seguidos quando existem julgamentos realizados por pessoas.

Outra questão relatada é a vivência da autora com a abordagem de avaliação da qualidade de produto de software, que indica uma análise da base conceitual e prática utilizada e que pode auxiliar esta pesquisa.

Finalmente, o Capítulo mostra experiências das quais a pesquisadora participou e que têm objetivos e soluções semelhantes para este contexto. A

utilização de modelos de referências, o desenvolvimento de checklists para serem utilizados por avaliadores e auditores para checarem e medirem atributos alvos para uma aplicação web.

3. MODELOS E TRABALHOS RELACIONADOS A MEDIDAS DE SEGURANÇA DE SOFTWARE

A seguir são apresentados e discutidos os trabalhos acadêmicos e práticos relacionados ao tema. Eles se referem a temas específicos e de interesse para esta pesquisa, tais como: Segurança de software, Requisitos de segurança, Medidas e Métricas, Avaliação de Segurança, Aplicação WEB e iniciativas governamentais.

3.1 SEGURANÇA DE SOFTWARE, TI, SI, E APLICAÇÃO WEB

Nesta seção é detalhado tópicos ligados diretamente a segurança de software, segurança da informação, segurança de TI e mais específico aplicação web. Para estes alvos são mostrados modelos, normas para sistema de gestão, modelos de maturidade, abordagem de ciclo de vida e ressalta a questão das vulnerabilidades e ameaças a estes alvos.

3.1.1 Sistema de Gestão

O Padrão Britânico (*British Standard*) 7799 (BS7799) originou-se de um código de prática do Governo do Reino Unido (*Department of Trade and Industry - DTI*) de 1993, depois publicado como padrão em 1995 pelo *British Standards Institution* (BSI) e revisado em 1999. Quando foi inicialmente publicado como um padrão internacional pela ISO em dezembro de 2000, BS7799 parte 1 (BS7799-1) se tornou ISO/IEC 17799 *Information technology — Security techniques — Code of practice for information security management*.

Em outubro de 2005, *British Standard* BS 7799 parte 2 (BS7799-2) foi adotada pela ISO e re-identificado, iniciando a nova série 27000 de padrões internacionais para gestão da segurança da informação lançada como norma ISO/IEC 27001:2005. No Brasil, a ABNT publica as normas localizadas ABNT NBR ISO/IEC 27002:2005 (NBR ISO/IEC 27002, 2005) e NBR ISO/IEC 27001:2005 (NBR ISO/IEC 27001, 2005).

A ISO/IEC 27001 (ISO/IEC 27001, 2005) é um padrão para sistema de gestão da segurança da informação (ISMS - *Information Security Management System*). Seu objetivo é ser usado em conjunto com ISO/IEC 27002, o código de práticas para gerência da segurança da informação, o qual lista os objetivos

do controle de segurança e recomenda um conjunto de especificações de controles de segurança.

Organizações que implementam um ISMS de acordo com as melhores práticas da ISO/IEC 27002 (ISO/IEC 27002, 2005) estão simultaneamente em acordo com os requisitos da ISO/IEC 27001, mas uma certificação é totalmente opcional. Este padrão é o primeiro da família de segurança da informação relacionado aos padrões ISO. Outros estão sendo incluídos:

- ISO 27000 - Vocabulário de Gestão da Segurança da Informação (sem data de publicação);
- ISO 27001 - Esta norma foi publicada em Outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação;
- ISO 27002 - Esta norma substituiu a ISO/IEC 17799:2005 (Código de Boas Práticas);

A série ISO/IEC 27000 está de acordo com outros padrões de sistemas de gerência ISO, como ISO/IEC 9001 (Sistemas de gerência da qualidade) e ISO/IEC 14001 (Sistemas de gerência ambiental), ambos em acordo com suas estruturas gerais e de natureza a combinar as melhores práticas com padrões de certificação.

Esta série de normas internacionais constitui-se no estado da prática em Gestão da Segurança da Informação. O objetivo da ISO/IEC 27001: 2005 é identificar e controlar os riscos relacionados à segurança da informação da empresa. Tais riscos podem estar relacionados à fragilidades no hardware e software, na forma como as informações são armazenadas e preservadas, como as informações são usadas dentro da organização, como as informações de caráter sigiloso são protegidas contra acessos indevidos, como situações de emergência e acidentes podem afetar a disponibilidade e a qualidade das informações.

Certificações de organização com ISMS ISO/IEC 27001 é um meio de garantir que a organização certificada implementou um sistema para gerência da segurança da informação de acordo com os padrões. Credibilidade é a chave de ser certificado por uma terceira parte que é respeitada, independente e competente. Esta garantia dá confiança à gerência, parceiros de negócios,

clientes e auditores que uma organização é séria sobre gerência de segurança da informação - não perfeita, necessariamente, mas está rigorosamente no caminho certo de melhora contínua.

Certificação ISO/IEC 27001 geralmente envolve um processo de auditoria em dois estágios: Estágio um - é uma revisão “informal/interna” da existência e completude de documentação chave como a política de segurança da organização, declaração de aplicabilidade e plano de tratamento de risco. Estágio dois - é um detalhamento, com auditoria em profundidade envolvendo a existência e efetividade do controle ISMS declarado bem como a documentação de suporte.

A ISO/IEC 27002 define um conjunto de onze (11) recomendações e um guia de implementação das melhores práticas para apoiar os controles especificados para um sistema de gestão de segurança da informação. Estes controles abrangem a Política de segurança organizacional; a gestão da segurança da informação, dos ativos, de recursos humanos, física do ambiente; o gerenciamento das operações e comunicações, do controle de acesso, da aquisição, desenvolvimento e manutenção de SI; a gestão de incidentes e da continuidade de negócios e finalmente a questão da conformidade.

Destas recomendações desta Norma, as que têm relação com este trabalho são os controles relacionados ao gerenciamento do controle de acesso de usuários e os de aquisição, desenvolvimento e manutenção de SI.

3.1.2 Modelos de Maturidade

Os modelos de maturidade são comuns na Engenharia e Qualidade de Software, para Segurança de Software também existem modelos específicos de maturidade, a seguir apresento os mais conhecidos.

O modelo BSIMM está na versão 4 – *Building Security in Maturity Model* (BSIMM, 2013) é um estudo de iniciativas de segurança de software do mundo real organizado para que o interessado possa determinar onde está com a sua iniciativa de segurança de software e como evoluir os seus esforços ao longo do tempo. Ele foi inteiramente construído a partir de observações feitas ao estudar cinquenta e uma iniciativas reais de segurança de software.

A versão BSIMM4 descreve 111 atividades organizadas em doze práticas de acordo com a estrutura de segurança software.

Há doze práticas organizadas em quatro domínios, cada domínio tem três áreas de práticas. Os domínios são os seguintes:

1. Governança: Práticas que ajudam a organizar, gerenciar e medir iniciativa em segurança de software.
2. Inteligência: Práticas que resultam em coleções de conhecimento corporativo utilizados na realização de atividades de segurança de software em toda a organização.
3. Fases do Ciclo de Vida de Desenvolvimento de Software (em inglês - Touchpoints SSDL): Práticas associadas com a análise e garantia de artefatos e processos específicos de desenvolvimento de software
4. Implantação: Práticas que fazem interface com a segurança da rede tradicional e organizações de manutenção de software.

Esta estrutura é mostrada na Tabela 3.1

Tabela 3.1 - Framework de Segurança de Software (BSIMM, 2013)

Framework de Segurança de Software			
Governança	Inteligência	Touchpoints SSDL	Implantação
Estratégia e Métricas	Modelos de Ataque	Análise de Arquitetura	Teste de Invasão
Conformidade e Política	Mecanismos e Projeto de Segurança	Revisão de Código	Ambiente de Software
Treinamento	Padrões e Requisitos	Teste de Segurança	Gestão de Configuração e de Vulnerabilidade

O modelo de maturidade tem as atividades divididas em três níveis (de 1 a 3) de maturidade no BSIMM.

Este modelo é bem abrangente cobrindo os quatro domínios, esta pesquisa tem o foco no domínio de Governança e na prática de Estratégia e Métricas.

O modelo OWASP-SAMM (*Security Assurance Maturity Model*) (OWASP-SAMM, 2013) é uma estrutura aberta para ajudar as organizações a formular e

implementar uma estratégia de segurança de software que é feita sob medida para os riscos específicos enfrentados pela organização.

O modelo SAMM é construído sobre um conjunto de práticas de segurança que estão ligados as principais funções de negócios envolvidos no desenvolvimento de software.

Os recursos fornecidos pelo SAMM ajudam a:

- Avaliar as práticas de segurança de software existentes em uma organização;
- Construir um programa de garantia de software de segurança equilibrado em iterações bem definidas;
- Demonstrando melhorias concretas para um programa de garantia de segurança;
- Definir e medir as atividades relacionadas com a segurança em toda a organização.

O modelo SAMM é estruturado em quatro funções de negócios e cada uma delas em três áreas de práticas. Esta estrutura é mostrada na Tabela 3.2

O modelo de maturidade tem as práticas divididas em três níveis (de 1 a 3) de maturidade que estão relacionadas como objetivos a serem atingidos.

Os modelos BSIMM e OWASP-SAMM são bem similares e cobrem quatro domínios, esta pesquisa tem o foco no domínio de Governança e na prática de Estratégia e Métricas do modelo OWASP-SAMM.

Tabela 3.2 - Estrutura do Modelo SAMM (OWASP-SAMM, 2013)

Estrutura do Modelo SAMM			
Governança	Construção	Verificação	Implantação
Estratégia e Métricas	Avaliação de ameaças	Revisão de projeto	Gestão da vulnerabilidade
Conformidade e Política	Requisitos de Segurança	Revisão de Código	Restrições de Ambiente
Educação e Orientação	Arquitetura de segurança	Teste de Segurança	Habilitação de Ambiente

O SSE-CMM® é um modelo de referência de processo. Ele é focado sobre os requisitos para a implementação de segurança em um sistema ou conjunto de sistemas relacionados ao domínio da segurança da tecnologia da Informação.

O *International Systems Security Engineering Association* (ISSEA) definiu a *System Security Engineering - Capability Maturity Model* (SSE- CMM) (SSE-CMM, 2003), com o objetivo de definir, melhorar e avaliar a capacidade de engenharia de segurança. Este modelo define as características de um processo de engenharia de segurança de 22 passos que é explicitamente definido, gerenciado, medido e controlado.

A Tabela 3.3 mostra a identificação das áreas que exigem a definição de métricas. O modelo representa um guia para organizações que precisam definir um processo de avaliação de segurança utilizado para medir os aspectos de segurança relativos às operações, a informação, redes, pessoal, comunicações e computadores.

Tabela 3.3 - Áreas de processos do SSE-CMM

Áreas de processo de segurança e de métricas de segurança definidas por SSE-CMM	
<i>PA01 Administer Security Control</i>	<i>PA12 Ensure quality</i>
<i>PA02 Assess Impact</i>	<i>PA13 Manage configurations</i>
<i>PA03 Assess Security Risk</i>	<i>PA14 Manage Project Risks</i>
<i>PA04 Assess Threat</i>	<i>PA15 Monitor and Control Technical Efforts</i>
<i>PA05 Assess Vulnerability</i>	<i>PA16 Plan Technical Efforts</i>
<i>PA06 Build Assurance Argument</i>	<i>PA17 Define Organization Systems Eng. Process</i>
<i>PA07 Coordinate Security</i>	<i>PA18 Improve Organization Systems Eng. Process</i>
<i>PA08 Monitor Security Posture</i>	<i>PA19 Manage product line evaluation</i>
<i>PA09 Provide Security Input</i>	<i>PA20 Manage Systems Eng. Support Environment</i>
<i>PA10 Specify Security Needs</i>	<i>PA21 Provide ongoing skills and knowledge</i>
<i>PA11 Verify and Validate Security</i>	<i>PA22 Coordinate with suppliers</i>

O modelo tem cinco níveis de capacidade:

- Nível 1, “Desenvolvido informalmente”;
- Nível 2, “Planejado e acompanhado”;
- Nível 3, “Bem definido”;
- Nível 4, “Controlado quantitativamente”;
- Nível 5, “Melhoria contínua”.

A norma ISO/IEC 21827 foi preparada pela *International Systems Security Engineering Association (ISSEA)* que formalmente projetou o *Systems Security Engineering — Capability Maturity Model* e foi adotada pelo Joint Technical Committee ISO/IEC JTC 1 com sua aprovação pela ISO e IEC (ISO/IEC 21827, 2002).

3.1.3 Ciclo de Vida de Desenvolvimento de Software Seguro

É fundamental entender que as soluções de segurança englobam diversas ações para minimizar os problemas de vulnerabilidade dos sistemas. Nenhuma solução isolada pode erradicar as vulnerabilidades de uma aplicação, de uma só vez. A Figura 3.1 mostra as três grandes áreas em que devem preservar a segurança: segurança de rede, de host e da aplicação (MEIER, 2003).

Figura 3.1- Abordagem para melhoria da Segurança de Aplicação Web (MEIER, 2003)

O caminho para se conseguir atingir uma relativa segurança é o uso das metodologias de segurança nas diversas fases do ciclo de desenvolvimento de software, da definição do sistema à sua utilização (GOERTZEL, 2008).

O documento *State-of-the-Art Report (SOAR)* representa uma produção de colaboração e esforços dos especialistas no assunto no Departamento de Defesa (DoD) em conjunto com organizações e indivíduos no Fórum SwA (Software Assurance) e grupos de trabalho (GOERTZEL, 2008).

O SOAR fornece uma visão geral onde apresenta observações sobre tendências assinaláveis em matéria de “garantia” de software de segurança como uma disciplina mostrando nas diversas fases do ciclo de vida de desenvolvimento exemplos de atividades para garantia de segurança, tais como:

Requisitos:

- Identificação de níveis aceitáveis de tempo de inatividade e perda de dados;
- Identificação de requisitos de segurança.

Projeto:

- Identificação e prestação de contramedidas para vulnerabilidades;
- Projeto para refletir as atividades de necessidades de ciência forense e recuperação de desastres, e a capacidade de testá-los.

Implementação:

- Automação de *scans* de código, de aplicação, de banco de dados e de rede;

Documentação e uso de procedimentos de testes de segurança manual.

Teste:

- Adição de testes de penetração e testes de caixa preta para compatibilidade funcional, e testes de regressão.

Implantação:

- Treinamento de segurança de *help desk*, administração de sistemas, e pessoal de apoio;
- Identificação de questões de política de segurança;
- Estabelecimento de cronograma e procedimentos para *backups* do sistema e os dados e recuperação de desastres.

Operação / Manutenção:

- Repetição de revisões de segurança "de rotina" e varreduras de vulnerabilidades;
- Controle seguro de mudanças.

Desclassificação:

- Sanitização da mídia;
- O descarte adequado de hardware e software.

O principal objetivo da “garantia” do software (*Software Assurance*) é assegurar que os processos, procedimentos e produtos utilizados para produzir e sustentar o software estejam em conformidade com todas as exigências e normas especificadas para gerir estes processos, procedimentos e produtos.

No livro “*Software Security: Building Security In*” Gary McGraw ensina em como implantar segurança durante o desenvolvimento do software, nas fases de requisitos, arquitetura, projeto, codificação, teste, validação, medição e manutenção, ele ressalta sete (7) melhores práticas de segurança de software a serem aplicadas nos artefatos gerados de software que são: Revisão de código, Análise de risco, Teste de invasão, Testes de segurança baseada em risco, Casos de abuso, Requisitos de segurança e Operações de segurança (McGRAW, 2006).

3.1.4 Vulnerabilidade e Ameaças

Vulnerabilidade é o que faz o software inseguro, é o que se busca quando se faz uma avaliação. Vulnerabilidade: um erro, falha, fraqueza, ou a exposição de uma aplicação, sistema, dispositivo ou serviço que poderiam levar a uma falha de confidencialidade, integridade ou disponibilidade. (CVSS, 2007)

Uma “vulnerabilidade” em segurança da informação é um erro de software que pode ser usado diretamente por um *hacker* para ter acesso a um sistema ou rede (CVE, 2010)(CWE,2011). Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador (CERT, 2011).

Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, por meio da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável. As vulnerabilidades não são corrigidas e os motivos são os mais diversos, entre eles: 1- Ninguém na organização compreende ou é responsável pela manutenção do código. 2- Grupo de Desenvolvimento não

entende ou respeita a vulnerabilidade. 3- Melhorias de recursos são priorizados frente de correções de segurança. 4- Falta de orçamento para corrigir os problemas. 5- Código de afetados é de propriedade de um fornecedor de terceiros que não responde. 6- Site será encerrado ou substituído "em breve". 7- Risco de exploração é aceito. 8- Solução de conflitos com o caso de uso. 9- Não existe compromisso para corrigir o problema.

Common Vulnerabilities and Exposures – CVE (CVE,2010) considera um erro se uma vulnerabilidade permite que um invasor use essa vulnerabilidade para violar uma política de segurança. Isso exclui totalmente as políticas de segurança em que todos os usuários são confiáveis, ou quando não há nenhuma consideração de risco para o sistema. Para CVE, a vulnerabilidade é um estado em um sistema de computação (ou conjunto de sistemas) que:

- permite a um invasor executar comandos como outro usuário;
- permite a um atacante, acesso a dados que é contrária às restrições de acesso especificado;
- permite a um atacante passar por outra entidade;
- permite a um invasor realizar uma negação de serviço.

Exemplos de vulnerabilidades incluem:

- PHF (execução de comandos remota como usuário "*nobody*")
- rpc.ttdbserverd (execução remota de comandos como *root*)
- arquivo de senhas do mundo gravável (alteração de dados do sistema crítico)
- senha padrão (execução de comandos remota ou outro acesso)
- negação de problemas de serviço que permitem que um atacante para causar uma Tela Azul da Morte
- *smurf* (negação de serviço pela inundação de uma rede)

Para referenciar as vulnerabilidades, foi escolhido o projeto OWASP, por ter sido adotado pelo PCI SSC - *Payment Card Industry – Security Standards Council*. Embora o OWASP seja mais voltado às aplicações Web, as vulnerabilidades apresentadas nesta seção podem também existir em outras arquiteturas.

Existem autores que trabalham para detalhar guias de orientação para auditoria em segurança de software, este é o caso de Mark Dowd, John McDonald e Justin Schuh (DOWD, 2006). Os autores tratam de TEMAS para descobrir vulnerabilidades em aplicações que vão desde o *sendmail* para Microsoft Exchange, *Check Point* VPN - se ao Internet Explorer. Com base na experiência, que introduzem do começo ao fim uma metodologia para descobrir até mesmo para revelar as falhas de segurança mais sutis e bem escondidas dentro do código fonte.

A “*Software Security Assessment Art*” abrange todo o espectro de vulnerabilidades de software em ambos ambientes UNIX/Linux e em Windows. Demonstra como a auditoria de segurança em aplicações de todos os tamanhos e funções, inclusive de rede e software web. Além disso, ensina com exemplos de código extensos reais retirados de falhas do passado em muitas das aplicações de maior destaque da indústria.

Outro quadro de métricas de vulnerabilidades é o Sistema de Pontuação Comum de Vulnerabilidade (CVSS), (CVSS, 2007), que fornece um hardware e software do sistema de medição independente. Os objetivos do sistema são para definir uma pontuação padronizada de vulnerabilidade que permite priorizar os riscos.

Para ajudar na melhoria da segurança dos sistemas de informação, uma metodologia de identificação de vulnerabilidades em aplicações para ser usada por desenvolvedores de software e profissionais de segurança foi desenvolvida (BARBATO, 2009).

Os níveis de avaliação podem ser selecionados independentemente para cada característica de qualidade relevante. Quando da seleção dos níveis, convém que vários aspectos sejam considerados. Por exemplo, aspectos importantes são aqueles relacionados com segurança, economia, segurança de acesso, ambiente e mercado do produto, quando apropriado. As três fases fundamentais se forem possíveis, para avaliar segurança como característica de aplicativos de software são:

Avaliação da segurança - A primeira fase desta metodologia é destinada a entrevistas com os desenvolvedores. O entendimento correto da aplicabilidade e funcionamento da aplicação é fundamental para o mapeamento de possíveis

pontos de comprometimento e identificação de supostas vulnerabilidades. As entrevistas são conduzidas com intuito de abordar todo ciclo de vida de um dado e formas de acesso.

Verificação da segurança - A segunda fase desta metodologia tem por finalidade identificar vulnerabilidades durante a utilização da aplicação. Algumas supostas vulnerabilidades encontradas na fase anterior podem ser comprovadas com a verificação de segurança. Analisar uma aplicação sob outras perspectivas é a base para a identificação de vulnerabilidades que por ventura podem não ser encontradas por meio de testes de segurança convencionais. Nesta fase, comunicações com redes ou bibliotecas são interceptadas, parâmetros de entrada são alterados, dados em memória são modificados, dentre outras formas de manipulação da aplicação.

Revisão da Segurança - A terceira e última fase desta metodologia visa revisar a aplicação sob uma perspectiva interna, ou seja, por meio de seu código fonte.

Esta fase, além de ser fundamental para encontrar as origens das vulnerabilidades e propor soluções de correção, é extremamente importante na identificação de vulnerabilidades não encontradas pelas fases anteriores, como as que dependem de certas condições para serem exploradas (DUARTE, 2008). Durante a revisão é possível saber quais são as condições e preparar formas de comprovação prática da existência das vulnerabilidades.

As fases são baseadas nas diferentes formas de identificação de vulnerabilidades e nas limitações técnicas existentes em cada uma delas, as etapas no fluxo de dados de uma aplicação e a análise nas atividades que devem ser executadas. As fases desta metodologia são projetadas para que sejam auto-complementares na intenção de identificar novas vulnerabilidades, reafirmar os resultados obtidos e apresentar as origens dos problemas. Já as etapas dividem as aplicações em partes referentes a atividades específicas dentro do fluxo de dados e acessos onde se concentram as vulnerabilidades. Para auxiliar na coleta de informações sobre a aplicação e na identificação de vulnerabilidades específicas, as etapas foram subdivididas em análises que representam as atividades que devem ser executadas em cada etapa. Dessa forma, a metodologia inicia de forma macro e vai detalhando tecnicamente até a identificação de vulnerabilidades sem tratar de procedimentos.

As ameaças podem ser categorizadas em três tipos: intencional, não intencional e maliciosa como na Tabela 3.4. Elas podem estar presentes durante o seu ciclo de vida nas fases de desenvolvimento, implantação e operação. Apesar das ameaças em todas as três categorias tenham o potencial de comprometer a segurança do software, apenas ameaças maliciosas são realizadas por ataques. A maioria dos ataques contra software aproveita, ou exploram alguma vulnerabilidade ou fraqueza do software que, por esta razão, o termo "ataque" é freqüentemente usado como sinônimo de "explorar", apesar de o Glossário Padrão de Ataque *BuildSecurityIn* (BARNUM, 2006) faz uma clara distinção entre os dois termos, com o ataque referindo a ação contra o software orientada e explorar referindo-se ao mecanismo (por exemplo, uma técnica ou código malicioso), pelo qual a ação é realizada. Para o software no desenvolvimento e implantação, a maioria das ameaças vai ser "privilegiada" ameaças, por exemplo, os desenvolvedores do software, testadores, gerentes de configuração e instaladores/administradores. A Tabela 3.4 fornece exemplos de ameaças em na categoria de operação.

Tabela 3.4 – Exemplos de ameaças ao software na operação.

Categoria da ameaça	Fase de operação
Não intencional	O usuário é capaz de entrar com um <i>string</i> maior que o definido, e o formulário de entrada HTML não valida e nem trunca os caracteres em excesso.
Intencional não malicioso	O Usuário inserir repetidamente combinações incomuns de comando em um esforço para ultrapassar a interface de entrada de dados; O usuário repetidamente atualiza e reenvia os mesmos dados de entrada para um aplicativo que não foi projetado para retornar um reconhecimento de que na entrada do usuário os dados foram recebidos.
Malicioso	Atacante insere uma <i>Structured Query Language</i> (SQL) numa injeção a um banco de dados baseado na Web. Desenvolvedor envia uma seqüência de dados predefinidos para uma aplicação Web, sendo que ele sabe que vai executar uma lógica que ele inseriu nessa aplicação.

A capacidade do software para continuar a operar de forma confiável, apesar da presença de atacantes é o que faz com que seja seguro. Essa habilidade é baseada em grande parte na ausência de vulnerabilidade a esses ataques, que pode ser ativados por ataques diretos que exploram vulnerabilidades conhecidas ou suspeitas, ou pela execução de códigos maliciosos embutidos.

É por isso que a maioria das definições de segurança de software enfatiza a ausência de lógica maliciosa e vulnerabilidades exploráveis (GOERTZEL, 2007).

Ponderação age como a 'interface' com ameaça de uma dinâmica mais estável de coleta de métricas de segurança. A natureza dinâmica das ameaças, o impacto e exposição do sistema, podem ser refletidos na coleção de métricas de segurança.

Uma "exposição" em segurança da informação é uma questão de configuração do sistema ou um erro de software que permite o acesso a informações ou recursos que podem ser usados por um *hacker* como um trampolim para um sistema ou rede (CVE, 2010). CVE considera um problema de configuração ou um erro se uma exposição que não permitem diretamente compromisso, mas pode ser um componente importante de um ataque bem-sucedido, e é uma violação da política de segurança razoável. Uma exposição descreve um estado em um sistema de computação (ou conjunto de sistemas) que não é uma vulnerabilidade, mas também:

- Permite que um invasor para realizar atividades de recolha de informação;
- Permite que um atacante ocultar atividades;
- Inclui um recurso que se comporta como esperado, mas pode ser facilmente comprometida;
- É o primeiro ponto de entrada que um atacante pode tentar usar para obter acesso ao sistema ou dados;
- É considerado um problema de acordo com algumas políticas de segurança razoável.

Exemplos de exposição incluem:

- Execução de serviços como finger (útil para recolher informações, que ele funciona como anunciado);
- Configurações inadequadas para as políticas de auditoria do Windows NT (onde "inadequado" é específico da empresa);

- Execução de serviços que são pontos comuns de ataque (por exemplo, HTTP, FTP ou SMTP);

Uso de aplicações ou serviços que podem ser atacados com sucesso por métodos de força bruta (por exemplo, uso de criptografia trivialmente quebrada, ou um pequeno espaço de chaves)

Quantidade de formulários de entrada ou interfaces do aplicativo igual a T (o número de formulário HTML, POSTs, GETs) e chamar de V ao número dessas interfaces que usam mecanismos de validação de entrada. A relação V/T traz uma forte declaração sobre a vulnerabilidade do aplicativo da Web a partir de exposições inválidas de entrada quanto maior a porcentagem, melhor.

A comunidade do projeto OWASP TOP TEN lista as mais sérias vulnerabilidades em aplicações WEB, este relatório é publicado periodicamente, a última publicação de 2010 apresenta as 10 vulnerabilidades mais comuns no ano de 2010, são elas em prioridade (OWASP-TOPTEN, 2010):

1. *Injection* – Injeção de falhas;
2. *Cross-Site Scripting (XSS)* - script entre sites;
3. *Broken Authentication and Session Management* - Quebra de autenticação e gerenciamento da sessão;
4. *Insecure Direct Object References* - Referências inseguras a objetos diretos;
5. *Cross-Site Request Forgery (CSRF)* - Falsificação de pedido entre sites;
6. *Security Misconfiguration* - Má configuração da segurança;
7. *Insecure Cryptographic Storage* – Armazenamento criptográfico inseguro;
8. *Failure to Restrict URL Access* – Falha no acesso restrito a URL;
9. *Insufficient Transport Layer Protection* – Proteção insuficiente a nível de transporte;
10. *Unvalidated Redirects and Forwards* – Encaminhamentos e redirecionamentos inválidos.

3.1.5 Qualidade e Segurança de Software

É comum pensar que qualidade e segurança de software são coisas semelhantes ou mesmo um único aspecto da questão do desenvolvimento e utilização de aplicações. No entanto, em uma análise mais apurada, pode-se verificar que são dois aspectos complementares e cada um tem suas peculiaridades — a garantia de qualidade do software é um processo cumulativo, enquanto a segurança do aplicativo é absoluta (BLACK, 2008).

Qualidade de software é cumulativa, pois considera aceitável certo número de falhas ou *bugs* até certo ponto e, ainda assim, o aplicativo é considerado bom o suficiente para ser entregue ao usuário. A segurança do software, por outro lado, é absoluta já que qualquer vulnerabilidade existente no aplicativo pode se tornar aquela que causará um enorme prejuízo ou desastre. A qualidade do software tem sido uma preocupação constante e parte integral do processo de desenvolvimento desde que se começou a escrever linhas de programação. Desde que as aplicações começaram a ficar expostas para o “mundo exterior” por meio da Internet, extranets e das aplicações de comércio eletrônico, as empresas que trabalham com estes sistemas começaram a ficar, cada vez mais, preocupadas com a segurança de software.

O problema de qualidade de software pode ser definido como a falha de uma parte de código para realizar as operações definidas na sua especificação. Essa afirmação pode abranger situações que vão de um usuário que acredita que a aplicação deveria funcionar de maneira diferente até a falha do software em responder a uma conexão de rede com um protocolo bem definido. Uma vulnerabilidade de segurança de software, em oposição a esta situação, pode ser definida como um recurso de código que permite que sua especificação de operação possa ser comprometida por um ataque externo.

À primeira vista, pode parecer que um ataque externo pode se restringir a explorar problemas de qualidade existentes dentro do software e, conseqüentemente, problemas de qualidade e segurança do software seria a mesma coisa. Na verdade, a maior parte das vulnerabilidades de segurança é encontrada em códigos-fontes considerados aceitáveis do ponto de vista da qualidade. O código-fonte contendo vulnerabilidades teria se comportado de acordo com sua especificação se não tivesse nenhum outro problema que compromettesse sua operação (DUARTE, 2008).

Em relação à segurança de software, assim como no aspecto de qualidade, deve-se examinar o sistema como um todo. Mas, neste ponto, a compreensão das características holísticas de segurança e de qualidade se torna complementar. Se uma vulnerabilidade possibilitar a um *hacker* a realização de uma compra por meio do uso da conta de algum usuário, simplesmente com a mudança de alguns dados utilizados pelo *cookie* da seção do sistema de comércio eletrônico, que se encontra escondido no navegador da vítima, com toda a certeza, esse sistema não é seguro e, espantosamente, esse tipo de vulnerabilidade foi identificado em milhares de sites de comércio eletrônico ao longo dos últimos anos e ainda pode ser detectados em diversos e bem conhecidos sites de e-commerce nos dias de hoje (WEBAPPSEC, 2013).

Segurança é um item essencialmente invisível para praticamente todo mundo, com exceção dos hackers, na medida em que baixa qualidade torna-se facilmente perceptível e o software ainda traz outro problema: as aplicações geralmente apresentam “recursos de segurança” como *login* e criptografia que dão a falsa sensação de segurança e escondem os riscos que existem no sistema. Qualidade é cumulativa, enquanto segurança é absoluta, como já foi mencionado. Isso torna essencial que metodologias para a segurança de software consigam detectar as vulnerabilidades existentes nos sistemas, em todo o ciclo de execução de uma aplicação (BLACK, 2008).

3.2 QUALIDADE DE SOFTWARE E SISTEMAS

Quando falamos em qualidade de software, um dos elementos sempre presente é um modelo de qualidade, esta pesquisa se inspira nesta questão e estuda modelos de qualidade para desenvolver um modelo de referência de segurança de software.

3.2.1 Modelo de Qualidade

As normas e modelos existentes oferecem quadros gerais, mas são necessários modelos mais específicos que reflitam a percepção dos especialistas e clientes, bem como as características específicas deste tipo de produto.

O artigo de Villalba (VILLALBA, 2010) apresenta um método para gerar modelos de qualidade de software orientados a domínio para tipos específicos

de aplicações. É aplicado para a geração de um modelo de segurança para produtos COTS baseado na revisão sistemática das normas, na literatura relacionada e conclusões das experiências de avaliação, bem como a análise estatística das informações coletadas de 203 especialistas em segurança e profissionais. Os resultados revelam conclusões interessantes sobre a importância fornecidas pelos usuários com as características de qualidade diferentes de produtos de segurança de software comercial.

A avaliação de produto de software tem sido uma das formas empregadas por organizações que produzem ou adquirem software para obtenção de melhor qualidade nesses produtos, sejam eles completos ou partes a serem integradas a um sistema computacional mais amplo.

Para que a avaliação seja mais efetiva, é importante utilizar um modelo de qualidade que permita estabelecer e avaliar requisitos de qualidade. É necessário que o processo de avaliação seja bem definido e estruturado. Os conjuntos de normas ISO/IEC JTC1/SC7 9126 e ISO/IEC 14598, que foram reestruturadas na série ISO/IEC 25000 - *Software Engineering – System and Software product Quality Requirements and Evaluation (SQuaRE)*, descrevem um modelo de qualidade, um processo de avaliação, uma diretriz para requisitos de qualidade e um conjunto de medidas de qualidade.

Alguns exemplos de medidas são encontrados nessas normas e podem ser utilizados por organizações que pretendam fazer avaliação de produto de software.

A norma NBR ISO/IEC 25051 (NBR ISO/IEC 25051, 2008), que também faz parte desta série estabelece requisitos de qualidade para pacotes de software e instruções para avaliação da conformidade de software. Pacotes de software, denominados COTS – *Commercial Off-The-Shelf* –, são produtos de software definidos por uma necessidade orientada pelo mercado, disponíveis comercialmente, cuja adequação para uso foi demonstrada por um grande número de usuários (COLOMBO; GUERRA, 2009).

O modelo de qualidade definido na ISO/IEC 25010 (ISO/IEC 25010, 2011) é estruturado de forma hierárquica, ele categoriza qualidade de software em características que são subdivididas em subcaracterísticas e atributos de

qualidade como mostra a Figura 3.2 em uma forma geral. Os atributos são entidades que podem ser medidas de forma direta ou indiretamente.

Figura 3.2 – Modelo geral de qualidade

A ISO/IEC 25010 (ISO/IEC 25010, 2011) define um modelo de qualidade de produto de software composto de oito características (que são subdivididas em subcaracterísticas) relacionadas a atributos estáticos do software e atributos dinâmicos do sistema de computador. A Figura 3.3 apresenta este modelo e ressalta (em vermelho/grifado) a característica de qualidade Segurança, que é o foco desta pesquisa. Esta nova versão da norma tornou a então subcaracterística Segurança como característica, colocando assim o item Segurança para um nível mais elevado, ressaltando a sua importância.

Figura 3.3 – Modelo de qualidade software

Esta série também contém um subconjunto de normas que têm o foco em Requisitos de qualidade, que é a ISO/IEC 25030 (ISO/IEC 25030, 2008), ela

fornece requisitos e recomendações para a especificação de requisitos de qualidade de software. Complementando a série, um subconjunto de normas que têm o foco de avaliação da qualidade de software - ISO/IEC 2504x, neste subconjunto tem a norma ISO/IEC 25040 (ISO/IEC 25040, 2010) que define um processo de avaliação da qualidade de modo genérico e que será apresentado no Capítulo 5 em específico para medir e avaliar segurança de software.

Pesos diferentes podem ser associados com componentes de medidas diferentes, a fim de indicar a importância relativa entre as medidas de componentes. A atribuição de peso 'próximo do correto' é utilizada na prática, porque não existem resultados analíticos para determinar as prioridades relativas dos elementos, além do uso cuidadoso da própria experiência e julgamento (WANG; WULF, 1997).

Duas dimensões importantes afetam fortemente o peso: o impacto potencial da ameaça e do Sul exposição para que a análise de impacto da ameaça pode ser iterado para reagir às mudanças no ambiente de ameaça. Assim, a estimativa de exposição da ameaça real, o peso de exposição pode variar dinamicamente, dependendo do sistema e do uso da aplicação. Os pesos de impacto e exposição podem ser integrados em fatores de métricas do componente de peso usando a heurística adequada que pode interpretar sua interação (SAVOLA, 2007).

A Figura 3.4 mostra o efeito do impacto e exposição. Região do "alto impacto exposição, alta ", obviamente, representa o mais crítico zona, resultando em maiores coeficientes de peso. Ameaças que caem na "de baixo impacto, alta exposição" ou "de alto impacto, baixa exposição" categorias também podem resultar em aumento da ponderação comparação com o "baixo impacto, baixa exposição" zona 1.

Figura 3.4 – Peso da Exposição versus Impacto

3.3 REQUISITO DE SEGURANÇA DE SOFTWARE

Esta seção trata sobre a questão de requisitos de segurança, descreve normas e modelos que auxiliam a identificação de requisitos.

3.3.1 Requisitos funcionais de segurança de TI.

A série ISO/IEC 15408 – *Information technology – Security techniques – Evaluation criteria for IT security*, surgiu do grupo responsável pelo *Common Criteria* (ISO/IEC 15408-1, 2009), (CC, 2001) que tem como foco a segurança lógica das aplicações e o desenvolvimento de aplicações seguras, ela define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas.

Este padrão internacional (ISO/IEC 15408-1, 2009) para segurança de TI, é voltado para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras. Ele define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas.

É uma estrutura para avaliar e certificar a segurança dos sistemas e produtos de TI, que é reconhecida pelos governos e profissionais de TI do mundo todo como uma medida crítica da qualidade de um produto de segurança de tecnologia da informação. A certificação CC é usada como um dos principais critérios de tomadas de decisões pelas agências de governo internacionais e federais e também está se tornando um diferencial para o setor privado, como o setor financeiro e da saúde.

Os Critérios Comuns-CC têm sua origem em 1990 e surgem como resultado da harmonização dos critérios sobre segurança de produtos software já utilizados por diferentes países com o fim de que o resultado do processo de avaliação pudesse ser aceitos em múltiplos países (ITSEC, 1991). Permitem comparar os resultados entre avaliações de produtos independentes. Para isso, se proporcionam um conjunto comum de requisitos funcionais para os produtos de TI (Tecnologia da Informação). Estes produtos podem ser hardware, software ou firmware. O processo de avaliação estabelece um nível de confiança no grau no qual o produto TI satisfaz a funcionalidade de segurança destes produtos e tem superado as medidas de avaliação aplicadas. São úteis como guia para o desenvolvimento, avaliação ou aquisição de produtos TI que incluam alguma função de segurança.

A origem dos Critérios Comuns-CC é encontrada nos critérios usados por diferentes países para a avaliação da segurança dos produtos software desenvolvidos. Combinam critérios de os: - TCSEC (*Trusted Computer System Evaluation Criteria*) frequentemente conhecido como chamado “Livro Laranja” e usados pelo Departamento de Defesa de EE.UU. - ITSEC (*Information Technology Security Evaluation Criteria*) comumente conhecido como “Livro Branco” e utilizados na Europa, e CTCPEC (*Canadian Trusted Computer Product Evaluation Criteria*) utilizados no Canadá (ITSEC, 1991).

Em 1999 os Critérios Comuns em sua versão 2.0 foram adotados pela *International Organization for Standardization* (ISO) como padrão internacional. Hoje os CC encontram-se normatizados como a série de normas ISO/IEC 15408 (ISO 15408-1, 2009), (ISO 15408-2, 2008) e (ISO 15408-3, 2008) ainda que a última versão encontra-se disponível no site do *Common Criteria* (CC, 2001).

A parte ISO/IEC 15408-1 (ISO/IEC 15408-1, 2009) estabelece os conceitos gerais e os princípios da avaliação de segurança e TI, especifica o modelo geral de avaliação e a sua totalidade é feita para ser usada como base para avaliação das propriedades de segurança de produtos de TI. Ela estabelece o conceito “alvo de avaliação” (*Target Of Evaluation* - TOE), que define o contexto de avaliação. Define as diversas operações em que os componentes funcionais e garantia dada na ISO/IEC 15408-2 e ISO/IEC 15408-3 (ISO/IEC

15408-2, 2008) (ISO/IEC 15408-3, 2008) que pode ser adaptado por meio da utilização de operações permitidas.

Os conceitos-chave de “perfis de proteção” (*Protection Profile* - PP), que define o conjunto de requisitos de segurança e o tema de conformidade. Esta parte da ISO/IEC 15408 fornece diretrizes para a especificação dos “objetivos de segurança” (*Security Target* - ST) e fornece uma descrição da organização dos componentes ao longo do modelo. Esta série também deve ser considerada na questão crítica para melhorar a segurança de software.

O processo de avaliação inclui a certificação de que um produto de TI específico verifica os seguintes aspectos:

- Os requisitos do produto estão definidos corretamente.
- Os requisitos estão implementados corretamente.
- O processo de desenvolvimento e documentação do produto cumpre com certos requisitos previamente estabelecidos.

O CC estabelece então um conjunto de requisitos para definir as funções de segurança dos produtos e sistemas de Tecnologias da Informação e dos critérios para avaliar sua segurança. O processo de avaliação, realizado segundo o prescrito nos Critérios Comuns, garante que as funções de segurança de tais produtos e sistemas reúnem os requisitos declarados. Assim, os clientes podem especificar a funcionalidade de segurança de um produto em termos de perfis de proteção padrões e de forma independente selecionar o nível de confiança na avaliação de um conjunto definido por sete níveis.

3.3.1.1 Perfis de proteção

Um perfil de proteção (*Protection Profile-PP*) define um conjunto de objetivos e requisitos de segurança, independente da implantação, para um domínio ou categoria de produtos que cobre as necessidades de segurança comuns a vários usuários. Os perfis de proteção são reutilizáveis e normalmente públicos e estão compostos de:

Requisitos funcionais de segurança (SFR, *Security Funcional Requirement*) proporcionam mecanismos para fazer cumprir a política de segurança. Como exemplos de requisitos funcionais: mencionar a proteção de dados do usuário, o suporte criptográfico, a autenticação, a privacidade ou o controle de acesso.

Requisitos de confiança ou garantia de segurança (SAR, *Security Assurance Requirement*) proporcionam a base para a confiança em que um produto verifica seus objetivos de segurança.

Os requisitos de confiança agruparam-se em níveis de confiança na avaliação (EAL, *Evaluation Assurance Levels*) que contêm requisitos de confiança construídos especificamente em cada nível. Os EALs proporcionam uma escala incremental que equilibra o nível de confiança obtido com o custo e a viabilidade de aquisição desse grau de confiança. O incremento de confiança de um EAL a outro se obtém incrementando rigor, alcance e/ou profundidade no componente e acrescentando componentes de confiança de outras famílias de confiança (por exemplo, acrescentando novos requisitos funcionais).

3.3.1.2 Níveis de Confiança

Os níveis de confiança na avaliação definidos na ISO/IEC 15408-3 (ISO 15408-3, 2008) vão desde EAL1 (o menor) ao EAL7 (o maior) e definem-se de forma acumulativa:

- EAL1 (funcionalidade provada); EAL2 (estruturalmente provado); EAL3 (provado e verificado metodicamente); EAL4 (desenhado, provado e revisado metodicamente); EAL5 (desenhado e provado semi formalmente); EAL6 (desenhado verificado e provado semi formalmente); EAL7 (desenhado verificado e provado formalmente):

Os níveis EAL 5 ao 7 incluem modelos e demonstrações semi-formais e formais portanto, aplicam-se a produtos com objetivos de segurança muito específicos (meio militar, por exemplo).

3.3.2 Trabalhos sobre Requisitos de Segurança de Software

A Engenharia de Requisitos vem demonstrando ser uma necessidade para a fase crítica e essencial no ciclo de vida de desenvolvimento de software.

Uma fonte a ser considerada é a Especificação de Requisitos nas atividades do desenvolvimento de software segundo a NBR ISO/IEC 12207 (NBR ISO/IEC 12207, 1998) onde se destacam:

- Levantamento dos requisitos

O levantamento dos requisitos consiste em entender os requisitos e solicitações do sistema; obter e definir os requisitos e solicitações do cliente por meio de sua solicitação direta ou por outras entradas como revisão da proposta de negócio, objetivos operacionais, ambiente de hardware e outros documentos.

É imprescindível entender as expectativas do cliente e assegurar que tanto o cliente quanto o fornecedor entendam os requisitos da mesma forma. Isso pode ser feito por meio do processo de apoio "Revisão Conjunta" descrito na norma NBR ISO/IEC 12207 (NBR ISO/IEC 12207, 1998). É necessário acordar os requisitos e obter um acordo entre as equipes que irão desenvolver o trabalho em relação aos requisitos do cliente. É importante também gerenciar todas as mudanças feitas nos requisitos do cliente em relação à linha-básica definida assegurando que o resultado de mudanças tecnológicas e de necessidades do cliente serão identificados e os impactos de introdução dessas mudanças serão avaliados.

- Análise dos requisitos do sistema

Após o levantamento de requisitos, segue para a especificação dos requisitos do sistema. Esta especificação deve descrever: Funções e capacidades do sistema;

Requisitos de negócio, organizacionais e de usuários; Requisitos de proteção, de segurança, de engenharia de fatores humanos (ergonomia), de interface, de operações e de manutenção; Restrições de projeto e requisitos de qualificação.

Os requisitos precisam ser avaliados. Por isso, para formalizar e facilitar a avaliação, os critérios listados a seguir devem ser seguidos:

- Rastreabilidade com os requisitos do cliente e necessidades de aquisição;
- Consistência com as necessidades de aquisição e com o levantamento dos requisitos;
- Testabilidade;
- Viabilidade do projeto da arquitetura do sistema;
- Viabilidade da operação e manutenção.

Após esta fase é importante estabelecer mecanismos de comunicação para disseminar os requisitos do sistema e suas atualizações para todas as partes interessadas. Pode-se conduzir uma ou mais revisões conjuntas e estabelecer as *baselines*.

Estas orientações serão utilizadas para estabelecer o modelo de qualidade com os requisitos do sistema e do software para assegurar a segurança do software e juntamente com a norma ISO/IEC 25030 (ISO/IEC 25030 , 2008) que estabelece os requisitos e recomendações para a especificação de requisitos de qualidade do produto software. Ela se aplica às organizações em ambos os papéis de compradores e ou fornecedores.

Outra fonte a ser considerada é a utilização de uma metodologia para elicitar e priorizar os requisitos de segurança no desenvolvimento Da metodologia *Security Quality Requirements Engineering - SQUARE* (MEAD, 2005).

Requisitos são considerados a parte fundamental sobre a qual todo software pode ser construído e avaliado. Não considerar os requisitos dessa forma pode trazer problemas de variadas natureza e qualidade, sendo que ambos continuam a crescer exponencialmente com o aumento da complexidade e versatilidade do software. O fracasso e o sucesso de qualquer programa dependem da qualidade dos requisitos. Existem relatos que cerca de 70% do software não inclui devidamente os requisitos, sendo eles pobres ou mal formulados (CONALLEN, 2000).

Estudos indicam também que mais de 60% da taxa de insucesso em projetos de software nos EUA, se deve aos requisitos mal formulados. Contrariamente a essa percepção, os especialistas em segurança são da opinião de que não se pode adicionar a segurança a um sistema pronto (MKS, 2007).

É uma propriedade emergente que exige atenção e planejamento rigoroso durante a fase de requisitos, além de um projeto cuidadoso. Barry Boehm e Victor R. Basili, especialistas em software da Universidade do Sul da Califórnia e Universidade de Maryland, observaram que encontrar e corrigir um problema de software após a sua entrega é 100 vezes mais caro do que encontrar e consertá-lo durante os “Requisitos e projeto” (BOEHM; BASILI, 2001). Durante este processo, a equipe deve considerar como os recursos de segurança

essenciais, desejáveis e as medidas para garantir ao software a perfeita integração e funcionamento com outros aplicativos que forem necessários.

O Padrão de Segurança de Dados PCI-DSS *Payment Card Industry Data Security Standard* (PCI-DSS, 2010) fornece um quadro acionável para o desenvolvimento de um processo de segurança dos dados do cartão de pagamento robusta - incluindo a prevenção, detecção e reação apropriada a incidentes de segurança.

O *PCI Security Standards Council* é um fórum aberto global para contínuo desenvolvimento, aprimoramento, armazenamento, disseminação e implementação de padrões de segurança para a proteção de dados de contas.

O Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) foi desenvolvido para incentivar e aprimorar a segurança dos dados do titular do cartão e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. Ele oferece a base de requisitos técnicos e operacionais projetados para proteger os dados do titular do cartão e se aplica a todas as entidades envolvidas nos processos de pagamento do cartão - inclusive comerciantes, financeiras, adquirentes, emissores e prestadores de serviço, bem como todas as entidades que armazenam, processam ou transmitem os dados do titular do cartão. O PCI DSS compreende um conjunto mínimo de requisitos para proteger os dados do titular do cartão e pode ser aperfeiçoado por controles e práticas adicionais para amenizar os riscos ainda mais. Ele define uma visão geral de alto nível dos 12 requisitos.

3.4 MEDIDAS E MÉTRICAS DE SEGURANÇA DE SOFTWARE

Esta seção inicia primeiramente com algumas reflexões de pesquisadores sobre a possibilidade de definir medidas e métricas para segurança de software. Em seguida, apresenta abordagens para medição de segurança de software.

3.4.1 Pesquisadores Filósofos

Para progredir na área de métricas em segurança, há uma necessidade de se concentrar no desenvolvimento de melhores requisitos de segurança, e as métricas e modelos relacionados com o poder preditivo³ prática. Existe uma hipótese de que o nível (ou força) de segurança pode ser maior pela aplicação de um modelo de segurança e de coleta de evidências de segurança na rede. Obviamente, há a necessidade de métricas de segurança tanto on-line como off-line.

Com métricas on-line usadas para monitoramento de segurança, podem ser feitas as decisões automáticas e confiáveis sobre segurança. Off-line, as métricas podem ser usadas para a previsão, para aumentar a qualidade de execução, e ajustar as atividades on-line de medição. Na prática, é necessário identificar as informações mensuráveis e os mecanismos para se obter e processar os dados. Medição on-line da arquitetura e off-line (planejadas fora do ambiente eletrônico) da coleta de provas deve ser planejada. Medições on-line e off-line muitas vezes dependem uma do outra (SAVOLA; ABIE, 2009a).

Estimativas do nível de segurança de um sistema é um desafio muito grande e extremamente difícil, se não impossível, encontrar uma solução geral ou métricas (BELLOVIN, 2006).

Em 2001 aconteceu o *Workshop on Information Security System Scoring and Ranking – WISSSR 2001*, organizado pelo *Applied Computer Security Associates (ACSA)* e pelo *MITRE Corporation*. Participaram desse evento os maiores institutos de pesquisa, tal como o NIST, a Carnegie Mellon University e empresas reunindo os maiores especialistas no assunto de métricas e medidas de segurança de TI. Os representantes estão até hoje envolvidos com o assunto, sendo que parte da bibliografia aqui apresentada são de pesquisadores que participaram desse evento como Nadya Bartol (BARTOL 2009) da empresa *Booz-Allen & Hamilton*, Dennis McCallam da *Logicon*, Rayford Vaughn da *Mississippi State University* (McCALLAM, 2001).

---

³ O poder preditivo de uma teoria científica refere-se à sua habilidade em gerar previsões testáveis

Elizabeth Nichols apresentou em 2007 um framework dizendo que o projeto OWASP *Top Ten* (OWASP-TOPTEN, 2010) oferece o ponto inicial para métricas que podem ajudar a quantificar o impacto que mudanças nas fases do processo de um ciclo de vida. Para resumir ela divide o ciclo de vida do software em três fases principais: medidas em tempo de design, implantação e execução e afirma que se colherem métricas em tempo de execução, por exemplo, está na fase de garantia de qualidade do software (NICHOLS; PETERSON, 2007).

A métrica software é um modelo matemático desenvolvido com base em uma equação que tem a forma $y = f(x)$, onde x é uma variável ou conjunto de variáveis, que são associadas com os fatores de influência, e y é o resultado (DICTIONARY, 2003). Um modelo matemático contém uma ou mais equações, inequações e tem uma ou mais funções objetivas. Seu papel é o de descrever, medir o estado de um sistema associado.

O papel da métrica software é medir certa característica de um software, incluindo todos os fatores que influenciam o nível de característica medida.

As métricas sendo aplicadas a todas as aplicações de software a partir de um conjunto homogêneo, as métricas tornam-se um instrumento que ajuda a fazer classificações de aplicações de software analisadas. Com base no modelo matemático, o processo de definição de uma métrica é composto de duas fases distintas:

- Definir o objetivo da métrica, que é a variável y ; o objetivo deve descrever claramente o que medir e isso requer um elemento mensurável;
- Identificar e definir os fatores de influência, que são as variáveis x , que são independentes e por seu comportamento ou ações determinam o valor objetivo da métrica.

A complexidade da métrica depende do seu modelo e isso pode afetar sua qualidade. Uma maior complexidade exige procedimentos de difícil utilização e interpretações de resultados (GEER, 2007).

Na prática, uma métrica simples e bem definida é mais apropriada porque é simples de usar e seus resultados são menos propensos a serem mal interpretados. As métricas de segurança representam padrões mensuráveis

que são usados para monitorar a eficácia das metas e objetivos estabelecidos para a segurança de TI.

Métricas são diferentes de medições, porque as medições fornecem visões específicas de um determinado tempo (*single-point-in-time*), são fatores discretos, enquanto as métricas são obtidas por comparação com uma linha de base pré-determinada de duas ou mais medidas tomadas ao longo do tempo.

Boas métricas são aquelas que são SMART – (***Specific, Measurable, Attainable, Reatable, and Time-dependent***), tem um significado específico, é mensurável, atingível, repetitiva, e dependente do tempo, de acordo com (SSE-CMM, 2003).

Essas características definem uma métrica como uma ferramenta valiosa e útil no processo de avaliação de segurança.

Métricas devem ser definidas com base na análise de riscos e de vulnerabilidades. A função da métrica é analisar o nível medido de vulnerabilidade ou de risco e indicar o grau em que:

- a política de segurança é implementada,
- as vulnerabilidades conhecidas tenham sido resolvidas,
- a aplicação tem sido testada para vulnerabilidades desconhecidas.

O aumento de ataques por aplicações vulneráveis levou a um reconhecimento gradual de que as proteções de rede e de sistema operacionais, atualmente rotineiras, para proteger sistemas acessíveis pela Internet não são mais suficientes. Este reconhecimento tem levado a pensar em medidas (atitudes) emergentes de segurança de aplicações para aumentar a segurança do sistema e da rede. Proteções de segurança de aplicativos e mitigações são especificadas quase exclusivamente ao nível da arquitetura do sistema e da rede em vez da arquitetura de aplicações individuais de software (GOERTZEL, 2007). Elas são primariamente implementadas durante a implantação do aplicativo e operação.

Aplicação de segurança combina técnicas de engenharia de sistemas, tais como medidas de defesa em profundidade (por exemplo, firewalls de camada de aplicação, *eXtensible Markup Language* (XML) *gateways* de segurança, área de segurança de assinatura de código) e configurações de segurança,

com práticas de segurança operacional, incluindo correção gestão e gerenciamento de vulnerabilidades.

Aplicações de segurança operam predominantemente usando proteções de fronteira para reconhecer e bloquear ataques padrões, e usando ambientes de execução restrita para isolar aplicativos vulneráveis, minimiza sua exposição a agressores e sua interação com os componentes mais confiáveis.

Medidas de segurança operacional estão focadas na redução do número de vulnerabilidades ou exposição nas aplicações e por várias vezes a reavaliação do número e a severidade das vulnerabilidades, e das ameaças que podem ser alvo, assim as medidas pode ser ajustada em conformidade para manter seu nível requerido de eficácia (GOERTZEL, 2007).

Da literatura encontrada, pode-se observar que existem os pesquisadores céticos como BELLOVIN, McCALLAM, McHUGH que ressaltam a dificuldade de se criar medidas de segurança. Em 2001 aconteceu um marco nesta área com a realização do *WISSSR - Workshop on Information Security System Scoring and Ranking*. Outros pesquisadores propõem abordagens de medições de software e de segurança como PFLEEGER&CUNNINGHAM (2010), JAQUITH (2007) , JANSEN (NIST), PAYNE (SANS), Dan Geer (2007) e Bayuk (2011). Todos eles tratam de medidas e métricas de segurança de forma viável.

3.4.2 Propostas de medição de segurança

Um modelo para relacionar os diferentes atributos deve ser definido no caso do valor desejado ser um único valor. Por exemplo, quando a medição é um padrão de vida, pode-se considerar o nível de salário médio, os preços dos imóveis, e os custos das necessidades diárias. Em alguns casos, uma simples adição das classificações de vários atributos pode ser suficiente e prever uma medida, em outros podem exigir um modelo mais sofisticado, como a soma ponderada para calcular uma medida final, onde se pondera o que se considera de maior importância. Outro ponto é medir como em metrologia, uma medida direta, caso em que um instrumento de medição pode ser usado. Por exemplo, para medir distâncias entre as estrelas os cientistas usam medidas indiretas, no caso, usando-se um pouco de trigonometria, a distância da estrela pode ser então calculada e não medida, como mostra a Figura 3.5.

Figura 3.5 – Como medir a distância de uma estrela

O ano de 1997 foi um marco para o assunto tratado neste trabalho. Neste ano foi publicado o artigo *Towards a Framework for Security Measurement* por Chenxi Wang e William A. Wulf da University da Virginia, no 20th *National Information Systems Security Conference* em Baltimore – USA, onde é descrito pela primeira vez uma estrutura para medição de segurança com embasamento da teoria e prática de medições formais (WANG; WULF, 1997). Essa estrutura inclui um processo hierárquico que contempla os atributos de segurança a serem medidos. Esses atributos foram decompostos em estruturas mais simples passíveis de serem calculados com respectivos pesos ou prioridades. Nesse cálculo utiliza o processo de análise hierárquica só citando um exemplo de outra área, deixando as medidas de segurança como sugestão para trabalhos futuros.

O processo de decomposição, com base no trabalho de Wang e Wulf (WANG; WULF, 1997), é usado para identificar os componentes mensuráveis dos requisitos de segurança:

1. Identificar os componentes sucessivos de cada requisito de segurança (objetivo) que contribuem para a exatidão, eficácia e/ou eficiência da meta. Objetiva exatidão ou eficácia são enfatizadas dependendo das necessidades de métricas em qualquer dimensão;
2. Examine os nós subordinados para determinar se a decomposição adicional é necessária. Se for, repita o processo com os nós subordinados como metas atuais, decompondo-os em seus componentes essenciais, e
3. O processo de decomposição termina quando nenhum dos nós folha pode ser decomposto para uma análise mais aprofundada, ou quando a decomposição desses componentes não é mais necessária.

De acordo com Wang e Wulf (WANG; WULF, 1997) uma metodologia para estimar medidas de segurança pode ser composta das seguintes fases:

- Decomposição
- Relação de funcionalidade (pai/filho)
- Pesos e prioridades (AHP)
- Medições básicas
- Análise sensitiva dos componentes.

A decomposição para medidas de segurança pode ser resumida como identificação de um conjunto de atributos de segurança relacionados com o objetivo da análise.

Os responsáveis pela decisão indicam sucessivamente os componentes que contribuem para o sucesso da segurança ou para que o sistema não falhe.

Na composição da hierarquia coloque o objetivo de análise em primeiro lugar e examine os nós subordinados para saber se nova decomposição é necessária. Se precisar, repita o processo com o novo objetivo em primeiro lugar.

O processo de decomposição se encerra quando os nós subordinados não puderem mais ser decompostos. Nesse ponto todas as folhas nós devem ser componentes mensuráveis que são independentes uns dos outros. Todos os nós folha deve ser componentes mensuráveis.

As aplicações também têm metas de segurança diferentes. As métricas de alto nível de segurança serão uma composição de uma série de métricas de segurança concentrando-se em diferentes aspectos da segurança. Além disso, para monitoramento de segurança *on-line*, técnicas de avaliação da segurança *off-line* são necessários a fim de encontrar soluções adequadas (SAVOLA; ABIE, 2009b).

Evidências de segurança na forma de métricas podem ser usadas para diferentes propostas: Segurança e monitoração QoS (atividade *on-line*) Gerenciamento Adaptativo de segurança (combinação de atividades *on-line* e *off-line*) Engenharia de Segurança, Gerenciamento e Garantia da segurança de software do sistema (atividades *off-line*) (SAVOLA; ABIE, 2009).

Em (PAYNE, 2006) são descritos sete passos essenciais para ser usado no processo de definição de um programa de métricas de segurança:

- Definir as metas e objetivos das métricas,
- Decidir quais métricas serão geradas,
- Desenvolver estratégias para gerar as métricas,
- Estabelecer parâmetros (*benchmarks*) e metas,
- Determinar como as métricas serão relatadas,
- Criar um plano de ação e agir sobre ela, e
- Estabelecer um programa formal de ciclo de revisão / aperfeiçoamento.

Em (CHAULA, 2004) os autores examinam diferentes estruturas para o desenvolvimento de requisitos e métricas de segurança de sistemas de informação.

Outro padrão de métricas de segurança amplo é o NIST 800-55, (CHEW, 2008). Este guia define um processo de desenvolvimento de métricas que consiste em duas atividades principais:

- Definir os objetivos de segurança do programa de segurança de TI;
- Definir e selecionar as métricas para medir a implementação, eficiência, eficácia e impacto dos controles de segurança.

Indicadores representam formas de interpretar o valor da métrica. A qualidade de métricas de segurança é analisada, também em (ISO/IEC 27002, 2005), do ponto de vista de mitos:

- Métricas devem ser objetivas e tangíveis;
- Métricas devem ter valores discretos;
- Métrica não requer a utilização de medidas absolutas;
- Métrica não deve ser cara;

Métricas são úteis porque "não se pode gerenciar o que não pode medir e não se pode melhorar aquilo que você não pode gerenciar", (ISO/IEC 27002, 2005);

Modelos matemáticos e algoritmos podem ser utilizados para prever o desempenho de segurança de um sistema de software. O objetivo alvo das

métricas pode ser a organização, seus processos e recursos, seus produtos/sistemas ou subsistemas.

A norma ISO/IEC FDIS 25020 (ISO/IEC FDIS 25020, 2006) define que “métrica direta é uma métrica definida em termos de um atributo e o método para quantificá-la, e métrica indireta é uma métrica que é definida em função de dois ou mais valores de métricas básicas”. Desta forma, métrica direta é a métrica de um atributo que não depende de outro atributo e a métrica indireta depende de um ou mais atributos. Sendo que as propriedades das métricas de segurança podem ser diretas ou indiretas, qualitativas ou quantitativas, objetivas ou subjetivas e absolutas ou relativas.

De acordo com a norma ISO/IEC 15939 o termo medida é uma variável para a qual um valor é atribuído como o resultado de uma medição. A norma também define medida básica, que é definida em termos de um atributo e o método para quantificá-la, uma medida básica é funcionalmente independente de outras medidas e também medida derivada, que é definida como uma função de dois ou mais valores de medidas básicas (ISO/IEC 15939, 2007).

A norma ISO/IEC FDIS 27004 integra a série 27000 que tem o foco em Sistema de Gestão da Ssegurança da informação (sigla ISMS em inglês). Esta norma fornece orientação sobre o desenvolvimento e a utilização de medidas e de medição, a fim de avaliar a eficácia de um ISMS implementado e seus controles ou grupos de controles, conforme especificado na ISO/IEC 27001 (ISO/IEC FDIS 27004, 2009).

Esta Norma dá recomendações sobre as seguintes atividades como base para uma organização para cumprir os requisitos de medição:

- a) o desenvolvimento de medidas (ou seja, medidas básicas, medidas e indicadores derivados);
- b) implementar e operar um Programa de medição de segurança da Informação;
- c) coleta e análise de dados;
- d) o desenvolvimento de resultados de medição;
- e) comunicar os resultados de medição desenvolvidos para as partes interessadas;

- f) utilizar os resultados das medições, como fatores que contribuem para as decisões relacionadas com o ISMS;
- g) utilizar os resultados das medições para identificar as necessidades para melhorar o ISMS implementado, incluindo o seu alcance, políticas, objetivos, controles, processos e procedimentos, e
- h) Facilitar a melhoria contínua do Programa de Medição de Segurança da Informação.

O conjunto de atributos de segurança que mais se aproxima do trabalho aqui apresentado será dependente do sistema, que deve identificar um conjunto de atributos relacionados à segurança que são importantes para a utilização do sistema. Este conjunto também deve definir se o sistema de segurança deve ser representado como um vetor ou um único valor.

Para segurança de software, as medidas serão extraídas de sistemas decompostos para simplificar o contexto e neste trabalho será mostrado como medir e pontuar segurança para tomada de decisão baseado no processo de análise hierárquica (COLOMBO et al., 2012).

Chandra & Khan (CHANDRA, 2009) propõem um framework adaptável para métricas de segurança que contribuem para a quantificação e conhecimento da segurança.

Nesta linha, Bayuk (BAYUK, 2011) fez um survey onde visualizou que métricas de segurança de sistema evoluíram lado a lado com o advento de ferramentas de segurança cibernética e técnicas. Essas ferramentas foram obtidas a partir das técnicas, em vez de especificadas como requisitos do sistema. Seu trabalho analisa a evolução do estado da prática de métricas de segurança de sistema, tanto numa perspectiva técnica como histórica.

A pesquisa leva à conclusão de que atualmente as metodologias para medir a segurança de sistema não tem qualquer base empírica. Sua pesquisa fornece novo critério para avaliar métricas de segurança. A fim de proporcionar articulação precisa para um conceito intangível, a definição de segurança de sistema é apresentada com a teoria de segurança usando lógica formal.

A aplicação reporta à estudos de caso em *Cloud Computing* e Comunicações Móveis. Recomenda pesquisa específica em uma variedade de tópicos de

segurança de sistema para reforçar esses resultados, e também fornecer embasamento teórico para as ferramentas mais eficazes e técnicas de engenharia de sistemas de segurança. Conclui que é necessária uma fundamentação teórica para obter uma engenharia de segurança efetiva.

Nichols & Peterson (NICHOLS; PETERSON, 2007) também propõem um framework de métricas específico para aplicação web e sugere a utilização do balance scorecard para uma melhor visualização dos resultados obtidos das medições. O *scorecard* resume as métricas de granularidade relativamente pequenas que calculam valores de dados a partir de testes de invasão de código, análise estática, sistemas de gerenciamento de incidentes, scanners de vulnerabilidade, e outros instrumentos relacionados no artigo. Relata que várias empresas clientes têm utilizado este scorecard para monitorar melhoria na de segurança centrada em práticas de codificação com as respectivas organizações de desenvolvimento de aplicações Web.

O scorecard fornece uma classificação para sete das categorias OWASP Top Ten (OWASP-TOPTEN, 2010). Resultados de uma métrica qualitativa são coloridos e ajudam na análise: vermelho quando o resultado é mal, verde quando é bom, e amarelo para algum lugar no entre os dois. As chaves para o sucesso dessa ferramenta incluem formação de consenso em todo o mapeamento que só permite alterações em um ambiente controlado e totalmente auditável. Fazendo uma mudança com base em uma pseudo-política, necessidade de transformar um vermelho em um amarelo ou um amarelo em um verde, vai causar uma série de danos em longo prazo, tornando, o scorecard e sua subjacente métrica inúteis (NICHOLS; PETERSON, 2007).

3.5 PESQUISA E DESENVOLVIMENTO PARA GOVERNOS

Esta seção aborda pesquisa e desenvolvimento de segurança de software em iniciativas governamentais, todos países têm preocupações e ações, pode-se notar o grande investimento nesta área no governo americano. O governo brasileiro tem órgãos dedicados a questão da segurança digital governamental e também programas de desenvolvimento em segurança.

3.5.1 Governo e Institutos Americanos

O governo Americano, como um todo, patrocina vários órgãos para a pesquisa e desenvolvimento de tecnologia para segurança de TI. Entre eles temos:

O NIST - *National Institute of Standards and Technology*, é uma agência do Departamento de Comércio dos EUA, foi fundada em 1901 como o primeiro laboratório de pesquisa da ciência física da nação federal.

Avançando no estado-da-arte em T,I em aplicações tais como a segurança cibernética e biometria, o NIST acelera o desenvolvimento e implantação de sistemas que sejam confiáveis, utilizáveis, interoperável e seguro; avanços em ciência de medição por meio de inovações em matemática, estatística e ciência da computação, e realiza pesquisas para desenvolver medidas e padrões de infra-estrutura para a TI e aplicações emergentes.

O NIST tem área de TI e a de *Computer Security Resource Center* - CSRC, que tem publicações da série NIST SP 800, entre elas SP 800-55 (CHEW et al, 2008) já considerada aqui.

O Departamento de Defesa Nacional dos EUA (DHS-USA) tem a área de Segurança Cibernética, que trata das questões de crime cibernético e de orientações para os cidadãos.

Em julho de 1958, o MITRE foi fundado como uma empresa privada sem fins lucrativos para prestar serviços técnicos e de engenharia para o governo federal americano. Atualmente o MITRE trabalha com o DHS-USA e tem vários Centros, incluindo o *Cyber Security & Information Systems - Information Analysis Center* (CSIA) que é um Centro de Análise de Informação (*Information Analysis Center -IAC*) do Departamento de Defesa dos EUA (*Department of Defense - DoD*) patrocinado pelo *Defense Technical Information Center - DTIC*).

O CSIA is é uma consolidação dos IACs antecessoras: o *Data and Analysis Center for Software* (DACS), e *Information Assurance Technology* (IATAC). Estes Centros têm muitas publicações na área.

O *Software Engineering Institute da Carnegie Mellow University* (SEI-CMU) tem o Centro de Coordenação CERT - *Community Emergency Response Teams* (CERT/CC) que aborda os riscos em nível de software e sistema. Apesar de ter

sido criado como uma equipe de resposta a incidentes, o CERT / CC evoluiu concentrando-se em identificar e enfrentar as ameaças existentes e potenciais, notificando os administradores de sistema e outros profissionais técnicos dessas ameaças, e em coordenação com fornecedores e equipes de resposta a incidentes no mundo para enfrentar as ameaças.

3.5.2 Governo Brasileiro

O governo Brasileiro tem instituições governamentais e centros que tratam da questão da segurança de TI e da segurança cibernética, são eles:

O Departamento de Segurança da Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI/PR (<http://dsic.planalto.gov.br>) tem como missão as seguintes ações no âmbito da segurança cibernética e de segurança da informação e comunicações:

- Adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento - SISEC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos;
- Planejar e coordenar a execução das atividades, e definir requisitos metodológicos na administração pública federal - APF;
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da APF;
- Estudar legislações correlatas e implementar as propostas, e avaliar tratados, acordos ou atos internacionais sobre matérias afins;
- Coordenar a implementação de laboratório de pesquisa aplicada de desenvolvimento e de inovação metodológica, bem como de produtos, serviços e processos.

O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores - CTIR da APF está subordinado ao DSIC do GS/IPR, sua finalidade é o atendimento aos incidentes em redes de computadores da APF (<http://www.ctir.gov.br>).

O Instituto Nacional de Tecnologia da Informação - ITI é uma autarquia federal vinculada à Casa Civil da Presidência da República, tem como missão: Atuar

na inovação, regulação e provimento de soluções tecnológicas que garantam segurança, autenticidade, integridade, privacidade e validade jurídica de documentos e transações eletrônicas, respeitando o cidadão, a sociedade e o meio ambiente (<http://www.iti.gov.br>)

A Rede Nacional de Ensino e Pesquisa (RNP) é a primeira rede de acesso à Internet no Brasil, integra mais de 800 instituições de ensino e pesquisa no país, beneficiando a mais de 3,5 milhões de usuários. Em 2005, o então Ministério da Ciência e Tecnologia (MCT) lançou a Nova RNP. O objetivo é melhorar a infraestrutura de redes em níveis nacional, metropolitano e local (redes de campus); atender, com aplicações e serviços inovadores, as demandas de comunidades específicas (telemedicina, biodiversidade, astronomia etc.); e promover a capacitação de recursos humanos em tecnologias da informação e comunicação (<http://www.rnp.br>).

A RNP engloba o CAIS – Centro de Atendimento a Incidentes de Segurança que atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

O Comitê Gestor da Internet no Brasil (CGI.br) foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995 e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados (<http://www.cg.org.br>).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet (<http://www.cert.br>).

O CERT.br desenvolve projetos de análise de tendências de ataques, com o objetivo de melhor entender suas características no espaço Internet Brasileiro:

- *Honeypots* Distribuídos: para aumentar a capacidade de detecção de incidentes e correlação de eventos;
- *SpamPots*: obter informações sobre o abuso da infra-estrutura de redes conectadas à Internet para envio de spam.

O Núcleo de Informação e Coordenação do Ponto BR (NIC.br) é uma entidade civil, sem fins lucrativos, que desde dezembro de 2005 implementa as decisões e projetos do Comitê Gestor da Internet no Brasil.

A Divisão de Segurança de Sistemas de Informação (DSSI) é a unidade do Centro de Tecnologia da Informação Renato Archer (CTI) responsável por desenvolver pesquisas e criar soluções na área de Segurança da Informação (<http://www.cti.gov.br>). A DSSI possui duas Linhas de pesquisa:

1. Metodologias de Defesa Contra Códigos Maliciosos - Código malicioso é a maior ameaça atual à Segurança de Sistemas de Informação. Pesquisas e desenvolvimentos na área de coleta, análise e identificação de Malware é fundamental para a criação de contramedidas e prevenção;
2. Sistemas de Gestão e Métricas de Segurança da Informação - O objetivo dessa linha de pesquisa é estudar métodos, técnicas e desenvolver sistemas para especificar, implantar, operar e manter a segurança das Informações.

Além da pesquisa, a DSSI tem mais duas áreas de interesse, que são:

Computação Forense - Pesquisa de métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital, buscando a validade probatória em juízo;

Visualização de Dados de Segurança - A área de visualização de dados aplicada à segurança ainda é muito recente, tendo, portanto, uma ampla gama de ferramentas e aplicações a se explorar, principalmente para análise de tráfego de rede suspeito ou malicioso, identificação de padrões de ataque baseados em dados temporais e análise de classificação de malware.

3.6 ANÁLISE E DISCUSSÃO

A procura crescente de produtos seguros com relação à vulnerabilidade exige uma melhoria de métodos para desenvolver e avaliar a segurança de software.

Na prática, a construção de grandes e complexos sistemas de software desprovidos de erros, e vulnerabilidades de segurança, continua a ser uma tarefa difícil. Em primeiro lugar, especificações com os pressupostos explícitos, podem mudar ao longo do projeto, então algo que não era um erro pode se tornar um erro mais tarde. Segundo, especificações formais são raramente escritas na prática. Terceiro, ferramentas de verificação formal usado na prática

para encontrar e corrigir erros, incluindo vulnerabilidades específicas, como estouros de *buffer*, geralmente são ditas sólidas e robustas no comércio. Em quarto lugar, não se pode prever as vulnerabilidades do futuro, ou seja, os erros presentes em software não se sabem como serão atacados no futuro.

As características de qualidade são utilizadas para derivar subcaracterísticas, atributos e medidas de qualidade, especificamente as características para medidas internas refletem nos atributos estáticos e, conseqüentemente, no *design* do software.

A vulnerabilidade de códigos (DUARTE, 2008), (BARBATO, 2009) com relação à ataques ou ações involuntárias que possam modificar dados restritos, pode ser utilizada como indicadores de medidas a serem coletadas e analisadas.

Um resumo de publicações entre 1996 e 2000 foram encontradas e consideradas como pode ser visto na Tabela 3.5.

Tabela 3.5 – Publicações de 1996 a 2000

Ano	1996	1997	1998	1999	2000
N. de publicações	1	1	1	2	0

A Tabela 3.6 mostra o número de publicações em requisitos e medições segurança de TI entre 2001 e 2013. À partir de 2006 as publicações sobre medições e requisitos de segurança se tornaram mais frequentes sendo que um dos que mais publicaram a partir de 2006 foi Reijo M. Savola (SAVOLA, 2007), pesquisador do Centro de Pesquisa Técnico VPP do Governo da Finlândia, com aproximadamente 20 publicações até 2013.

Tabela 3.6 – Publicações entre 2001 e 2013

2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
5	15	17	10	8	9	3	5	5	4	1	4	3

A Tabela 3.7 indica as normas que têm relacionamento com segurança da informação, de software, de TI.

Com essa visão, fica mais fácil entender as diferenças (ou semelhanças) e nuances entre essas normas. A série ISO/IEC 27000 pode ser utilizada para a gestão e certificação de sistemas de gestão da segurança, a série ISO/IEC 15408 pode ser utilizada para a avaliação e certificação de segurança de TI e software, a série ISO/IEC 25000 pode ser utilizada para a elaboração de um modelo de qualidade de segurança de software.

Tabela 3.7- Resumo das principais normas relacionadas à segurança

NBR ISO/IEC 17799 (27002)	ISO/IEC 27001	ISO/IEC 15408-1	ISO/IEC 25010
Propriedades de Segurança	Gestão da Segurança	Alvo de avaliação (TOE)	Qualidade e Segurança
Confidencialidade	Controles de segurança	Perfil proteção (PP)	Confidencialidade
Integridade		Nível de avaliação (EAL)	Integridade
Disponibilidade		Objetivo da (ST)	Não-repúdio
Autenticidade			Responsabilidade
			Autenticidade
			Conformidade da segurança

Modelo de segurança utilizado no contexto abordado neste trabalho se refere ao modelo de referência de atributos de segurança. Esse modelo serve como ponto de partida para ser desdobrado em componentes mensuráveis da segurança do software. Os requisitos a serem desdobrados do modelo de segurança foram estudados em várias fontes (ISO/IEC 25000, 2005), (ISO/IEC FDIS 27000, 2009), (SAVOLA; ABIE, 2009b), (ISO/IEC 15408-1, 2009), entre outros e foi possível extrair as melhores práticas de segurança de uma aplicação web sem levar em conta o ambiente no qual está inserida essa aplicação. São requisitos fundamentais de segurança para que um aplicativo de software na web contenha o mínimo de práticas utilizadas pela comunidade de prática.

4. ESTRUTURA DA PESQUISA

Esta seção introduz os métodos de pesquisa mais utilizados na Engenharia de Produção e apresenta os métodos utilizados neste trabalho.

4.1 METODOLOGIA DE PESQUISA ACADÊMICA NA ENGENHARIA DE PRODUÇÃO

As alternativas de métodos de pesquisa em Engenharia de Produção podem seguir algumas vezes os chamados métodos tradicionais utilizados em outras áreas da engenharia como, por exemplo, métodos quantitativos, como também podem ser necessárias outras abordagens oriundas das ciências sociais como os métodos qualitativos (NAKANO; FLEURY, 1998).

Com relação aos métodos quantitativos utilizados nas ciências matemáticas, físicas cujo pensamento científico se dá de duas formas: pensamento indutivo ou dedutivo, nestas duas situações se exige coleta sistemática de dados, medição de dados. Pesquisas que precisam deste tipo de abordagem utilizam os chamados métodos de pesquisa experimental e pesquisa *survey* (FORZA, 2002).

O método *survey* coleta dados por meio de entrevistas, questionários e sempre exige um tratamento estatístico; é um método bastante utilizado (FORZA, 2002).

Com relação aos métodos qualitativos ou também chamados interpretativos, as pesquisas têm as seguintes características (NAKANO; FLEURY, 1998):

- O pesquisador observa os fatos,
- A pesquisa busca compreender o contexto,
- É importante considerar a sequência cronológica dos fatos,
- Não há hipóteses fortes no início da pesquisa,
- Pesquisa utiliza várias fontes de dados.

Os métodos mais utilizados na pesquisa qualitativa são a pesquisa participante, a pesquisa-ação e o estudo de caso.

A pesquisa participante e a pesquisa-ação são bastante similares, para Thiollent (THIOLLENT, 2007) toda pesquisa-ação é do tipo participativo, porém

nem toda pesquisa participante é pesquisa-ação, pois neste caso o pesquisador tem um papel ativo nas decisões e ações.

O estudo de caso, segundo Yin (YIN, 2005) não utiliza só a pesquisa qualitativa, pode fazer uso da pesquisa quantitativa também, segundo Yin o estudo de caso investiga um fenômeno contemporâneo dentro de um contexto, as fronteiras entre o fenômeno e o contexto não são claras e assim utiliza múltiplas fontes de dados e informações. Um instrumento muito utilizado neste método é o uso de entrevistas e outras fontes de coleta de informações. Uma dificuldade do uso deste método é que não podem ser feitas generalizações dos resultados (VOSS, 2002).

4.2 METODOLOGIA PESQUISA-AÇÃO (PA)

Esta seção mostra e conceitua o instrumento de pesquisa científica, que é a pesquisa-ação, que se mostrou adequada para o desenvolvimento desta pesquisa.

A pesquisa-ação é um método de pesquisa social no qual o pesquisador detecta um problema em seu meio social ou laboral e busca, junto com outros atores, sua solução. O pesquisador está envolvido no problema que detectou e participa de sua solução. Apresento antes algumas definições.

Vergara (VERGARA, 2007) define o seguinte conceito: "Pesquisa-ação é um tipo particular de pesquisa participante e de pesquisa aplicada que supõe intervenção participativa na realidade social. Quanto aos fins é, portanto, intervencionista".

Thiollent (THIOLLENT, 2007) define a pesquisa-ação como sendo: Um tipo de pesquisa social com base empírica que é concebida e realizada em estreita associação com uma ação ou com a resolução de um problema coletivo e no qual os pesquisadores e os participantes representativos da situação ou do problema estão envolvidos de modo cooperativo ou participativo.

Hugues Dionne (DIONNE, 2007) define assim pesquisa-ação: A pesquisa-ação é definida como prática que associa pesquisadores e atores em uma mesma estratégia de ação para modificar uma dada situação e uma estratégia de pesquisa para adquirir um conhecimento sistemático sobre a situação identificada.

A pesquisa-ação pode ser vista como um dos inúmeros tipos de investigação-ação, que é um termo genérico de qualquer processo que siga um ciclo, no qual é aprimorada a prática pela mudança sistemática entre agir no campo da prática e investigar a respeito dela. Existe o Planejamento, a implementação, a descrição e a avaliação de uma mudança para melhorar sua prática. Neste ciclo existe tanto o apredizado no decorrer do processo, quanto a respeito da prática da própria investigação (TRIPP, 2005).

Westbrook (WESTBROOK, 1995) conclui que enquanto a maioria das pesquisas empíricas, isto é pesquisa tradicional, deve ser capaz de fornecer resultados relevantes gerenciais, a relevância de pesquisa-ação é normalmente garantida com a gestão em que a própria empresa quer abordar. Com métodos baseados em casos, nos quais se pode ter uma visão desestruturada, a pesquisa-ação é vista (pelo menos fora da Gestão de Operação e Produção) como especialmente valiosa para a construção de teoria em situações complexas.

COUGHLAN e COGHLAN (COUGHLAN; COGHLAN, 2002) apresenta o ciclo no qual abrange 3 (três) passos para se realizar uma pesquisa-ação, como apresentado na Figura 4.1

- (1) Entender o contexto e o propósito;
- (2) O ciclo da pesquisa inclui 6 (seis) passos - coletar dados, obter *feed back* e analisar dados, em seguida inclui as ações de planejar, implementar e avaliar;
- (3) Meta passo global de monitoramento. Este meta passo - monitoramento é o foco desta dissertação acadêmica, pois o projeto de PA investiga como os ciclos da pesquisa são realizados.

Figura 4.1 - Passos da Pesquisa-Ação (COUGHLAN; COGHLAN, 2002)

A pesquisa-ação é então vista como principal contribuição para a dinâmica de tomada de decisão no processo de ação planejada. O aspecto "ação" é valorizado na definição de pesquisa-ação.

As definições apresentadas para a metodologia pesquisa-ação são conciliatórias e conclusivas. No que tange as principais características desta metodologia e que estão em consonância com esta pesquisa são:

- O pesquisador faz parte do projeto de pesquisa;
- As pessoas relacionadas ao alvo do projeto participam da pesquisa;
- A pesquisa segue por meio de fases e ciclos os quais implementam ações e validam os resultados até chegar no objetivo geral.

Segundo EISENHARDT (EISENHARDT, 1989) a análise dos dados é feita em dois passos: análise dos dados dentro do caso e também a busca pelas referências entre os casos em busca de padrões. É necessário melhorar a generalidade das conclusões dos casos.

Este método de pesquisa denominado Pesquisa-Ação aplicado no desenvolvimento desta pesquisa demonstra ser o mais adequado, principalmente no que se refere à estruturação das proposições e no protocolo de pesquisa. O próximo item detalha a questão da pesquisa e as principais referências relacionadas ao trabalho.

4.3 PROJETO DA PESQUISA

Nesta pesquisa está sendo utilizado o método de pesquisa acadêmica “Pesquisa-Ação”. Adicionalmente foi realizada a pesquisa bibliográfica e também foi utilizada a pesquisa tipo *survey* do Instituto Ponemon (PONEMON, 2010) e da Ernst & Young (ERNST&YOUNG, 2009), já citadas neste trabalho.

Esta pesquisa parte de uma questão central de indagação:

Como medir e conhecer o nível de segurança de acesso de aplicação web?

E traz como premissa a especificação e avaliação de propriedades e requisitos de segurança que possam ser medidos para conhecer o nível de segurança de aplicativos Web.

Assim, a pesquisa bibliográfica possibilitou focar em quatro (4) áreas chave para segurança para aplicação web, relacionadas com o objetivo geral desta pesquisa, elas são:

- **Segurança de TI, SI, Sw , Aplicação web**

As principais referências para este tópico e que já foram comentadas são: Séries 27000 (ISO/IEC FDIS 27000, 2009), (NBR ISO/ IEC 17799, 2005), 15408 (ISO/IEC 15408, 2008), Goertzel (GOERTZEL, 2008), (GOERTZEL, 2007), Lipner (LIPNER, 2006), CERT-BR (CERT-BR, 2006), SSE-CMM (SSE-CMM, 2003), Ponemon (PONEMON, 2010), Symantec (FOSSI ET al., 2011), Bradley (BRADLEY, 2007).

O conhecimento do estado atual da prática e da pesquisa dará o embasamento para esta pesquisa.

- **Requisitos de segurança**

As principais referências para este tópico são: Série 25000 (ISO/IEC 25000, 2005), (ISO/IEC 25010, 2011), (ISO/IEC 25030, 2008), Houmb (HOUMB, 2010), OWASP-ASVS (OWASP-ASVS, 2009), SQUARE/SEI (MEAD, 2005), CVE (CVE, 2010), CVSS (CVSS, 2007), MS-IWAS (MEIER, 2003).

Um modelo de referência com atributos e requisitos de segurança dará a estrutura conceitual para medições de segurança.

- **Medidas e Métricas de segurança**

As principais referências para este tópico são: Wang&Wulf (WANG; WULF, 1997), Bellovin (BELLOVIN, 2006), McHugh (McHUGH, 2002), Jansen (JANSEN, 2009), Hinson (HINSON, 2006), Verendel (VERENDEL, 2009), Chew (CHEW, 2009), Payne (PAYNE, 2006), Jaquith (JAQUITH, 2007), (SAVOLA; ABIE, 2009a), (SAVOLA; ABIE, 2009b), Nichols&Peterson (NICHOLS; PETERSON, 2007).

A pesquisa utiliza a abordagem de decomposição de requisitos para obter os componentes básicos mensuráveis (BMCs); e utiliza métodos formais consagrados, como o AHP para possibilitar a medição e priorização; fará utilização da ferramenta SuperDecision® no cálculo do AHP.

- **Avaliação de software e de segurança de aplicação web**

As principais referências para este tópico são: ISO 25040 (ISO/IEC 25040, 2011), Villalba (VILLALBA, 2010), MEDE-PROS (MEDE-PROS®, 2006), OWASP-ASVS (OWASP-ASVS, 2009), Dowd (DOWD, 2006), Jelen (JELEN, 1997).

A avaliação de atributos de segurança será realizada pela equipe responsável pela AWA.

Por meio de um referencial teórico específico para este contexto procura-se preencher a lacuna que existe entre o estágio atual e o desejável deste cenário, visando obter mecanismos que permitam melhorar a qualidade da aplicação em relação ao atributo segurança.

Também, por meio de um referencial de experiências práticas e iniciativas, são consideradas os diversos objetivos relacionados à questão da segurança de aplicações web.

Diante deste cenário, o objeto de estudo busca pesquisar a hipótese de que o desenvolvimento de uma metodologia sistemática englobando um conjunto de conceitos de segurança reconhecidos internacionalmente e de práticas no mercado, possam se materializar para uma especificação e avaliação da segurança de acesso para aplicações web.

4.4 ESTRUTURAÇÃO DA PESQUISA

A estruturação desta pesquisa é apresentada de forma geral na Figura 4.2. Ela tem uma estrutura hierárquica, parte do Objetivo geral da pesquisa, em seguida

este é desdobrado em Objetivos específicos. A pesquisa tem suas proposições e seus pontos de análise que são relacionados com os objetivos específicos.

Figura 4.2 – Estruturação Geral da Pesquisa

A seguir são apresentados os objetivos, as proposições e os pontos de análise definidos nesta pesquisa e que serão rastreados durante o desenvolvimento da metodologia da pesquisa-ação. O objetivo geral é:

Objetivo Geral – Desenvolver uma metodologia de avaliação da segurança de acesso de aplicações web.

Este objetivo geral desdobra-se nos seguintes objetivos específicos:

Objetivo Específico 01 – Levantar e conhecer atributos de segurança de software e o estado da arte e o estado da prática no tema;

Objetivo Específico 02 – Avaliar aplicações web em tempo de execução por meio de um Modelo de Referência de Segurança (empiricamente);

Objetivo Específico 3 – Medir a propriedade de segurança Autenticidade.

Objetivo Específico 04 – Transformar propriedades de segurança intangíveis em atributos de segurança tangíveis e quantificar atributos tangíveis de segurança;

Objetivo Específico 05 – Elaborar uma metodologia com um Modelo de Referência, um método de avaliação com medição e pontuação para segurança da aplicação web;

Objetivo Específico 06 – Estender a metodologia com os modelos e métodos de avaliação para segurança da aplicação web.

A seguir são apresentadas as proposições que serão desenvolvidas em cada Fase da metodologia de “pesquisa-ação” para atenderem aos objetivos específicos:

Proposição 01 – A visão de segurança de aplicação web é segmentada.

A seguir tem-se a relação de referências estudadas e que formam a base da visão de segurança de aplicação Web nesta pesquisa. Os itens abaixo correspondem aos itens descritos e comentados no Capítulo 3.

III 1.1 - Sistema de Gestão – ISO/IEC FDIS 27000, 2009; ABNT NBR ISO/IEC 27001, 2006 ABNT NBR ISO/IEC 27002, 2005;

III 1.2 - Modelos de maturidade – McGRAW, 2006; 2010 (BSIMM); OWASP-SAMM, 2013; SSE-CMM, 2003; ISO/IEC 21827, 2002; CHEWetal, 2008 (NIST800-55);

III 1.3 - SDLC – McGRAW, 2006; GOERTZEL et al., 2007; GOERTZEL et al., 2008; MEIER, 2003;

III 1.4 - Vulnerabilidade/Ameaça – CVSS, 2007(MELL et al., NIST); SYMANTEC, 2010; BARBATO, 2009; CVE, 2013; CWE, 2013; CWSS, 2013; OWASP-TOPTEN, 2007;

III 1.5 – Qualidade e Segurança de software – DUARTE, 2008; BSI, 2013; WEBAPPSEC, 2013; *Improving Web Application Security* (IWAS) MEIER, 2003;

Proposição 02 – Modelo de referência de segurança de acesso para aplicação web.

Para esta proposição as referências estão listadas a seguir

III 2.1 - Modelo - ABNT NBR ISO/IEC 25000, 2008; ISO/IEC 25010, 2011; ISO/IEC FDIS 27000, 2009; ABNT NBR ISO/IEC 27001, 2006 ABNT NBR ISO/IEC 27002, 2005;

3.3; CC PART2, 2004; ISO/IEC 15408-2, 2008; IWAS, 2003; MEAD et al, 2005; ABNT NBR ISO/IEC 27002, 2005; SAVOLA, 2007; ABNT NBR ISO/IEC 25030, 2008; OWASP-ASVS, 2009; PCI-DSS, 2010;

Proposição 03 – Checklist para avaliar propriedade de segurança de aplicação web.

Para elaboração de um *checklist* de auditoria de segurança de aplicação web, foram:

WANG&WULF, 1997; MEDE-PROS, 1997; BUTLER, 2002; LEAO et al., 2009; ISO/IEC 25040, 2011; OWASP-ASVS, 2009; PCI-DSS, 2010; OLLMAN, 2013; MEHTA, 2013;

Proposição 04 – Metodologia de apoio à decisão auxilia na medição e priorização de atributos de segurança.

A seguir estão referenciados os itens que formam a base teórica desta proposição.

2.1 Método para apoio à decisão; 2.2 Conceitos Algébricos; 2.3 Modelo AHP; 2.4 Por que usar o AHP ;

Proposição 05 – Valor quantitativo para uma propriedade de segurança intangível.

As referências seguem com o respectivo item referente ao Capítulo 3.

III 4 2 - Propostas - WANG&WULF, 1997; VAUGN et al., 2002a; VAUGN et al., 2002b; VILLARUBIA et al., 2004; PAYNE, 2006; BATISTA; 2007; JAQUITH, 2007; SAVOLA, 2007; CHEW et al., 2008; JANSEN, 2009; ABNT NBR ISO/IEC 25020, 2009; ABNT NBR ISO/IEC 15939, 2009; SAVOLA&ABIE, 2009; BARTOLetal, 2009; CHANDRA&KHAN, 2009; RADACK, 2010; BAYUK, 2011;

Proposição 06 – Metodologia para medir e priorizar segurança de acesso.

Referência para Modelo de relatório se encontra em: NBR ISO/IEC 14598-5, 2002.

Pontos de análise são colocados para verificarem se há o atendimento das proposições aos objetivos específicos e para dar o sequenciamento das fases da pesquisa-ação para o atendimento ao objetivo geral da pesquisa. A seguir são apresentados os pontos de análise para esta pesquisa.

Ponto de Análise 01 – Levantamento bibliográfico;

Ponto de Análise 02 – Escolha de uma aplicação web alvo (AWA) para estudo preliminar;

Ponto de Análise 03 – Avaliação preliminar;

Ponto de Análise 04 – Esboço de um Modelo de Referência;

Ponto de Análise 05 – Esboço de um *checklist*;

Ponto de Análise 06 – Elaboração da metodologia;

Ponto de Análise 07 – Aplicação da metodologia na AWA.

Com esta estrutura de pesquisa definida, o próximo passo é apresentar a metodologia de pesquisa a ser utilizada.

O próximo Capítulo detalha os ciclos e fases realizadas na proposta de uma metodologia de medição e priorização de segurança de acesso de aplicações web.

5. PESQUISA-AÇÃO PARA MEDIÇÃO E PRIORIZAÇÃO DE SEGURANÇA

Este capítulo apresenta o relato de como foi desenvolvido o trabalho de acordo com a metodologia de pesquisa “Pesquisa-ação”. Inicialmente é mostrada a estruturação da “pesquisa-ação” na forma geral relacionando as fases e os ciclos da pesquisa e em seguida eles são apresentados detalhadamente no tema em particular. Esta metodologia foi adotada devido ao desenvolvimento da pesquisa de doutorado ter ocorrido com a participação na equipe de desenvolvimento da aplicação AWA.

5.1 AS FASES E CICLOS DA PESQUISA-AÇÃO (PA)

A Pesquisa-ação aconteceu em cinco (5) fases apresentadas na Figura 5.1, sendo que a Fase 1 (Exploratória) é a fase de conhecimento e levantamento do estado atual para o Objetivo Geral e finalizando com a Fase 5 (Conclusiva) que apresenta a metodologia desenvolvida e os resultados obtidos na pesquisa-ação.

Figura 5.1 – Estrutura por fases da pesquisa-ação

As Fases 2, 3 e 4 indicadas na Figura 5.2 por meio de ciclos, consistem de 03 (três) ciclos da Pesquisa-ação no seu formato geral, os quais implantam e avaliam a proposta para a medição da segurança de acesso para aplicação web alvo (AWA). Estes ciclos obedecem a metodologia do COUGHLAN e COGHLAN (COUGHLAN e COGHLAN, 2002). Cada ciclo parte de objetivos específicos e se direcionam pelo planejamento, ação, monitoramento e

avaliação. A avaliação é colocada aqui como Ponto de análise e reflexão do estudo realizado.

Figura 5.2 – Estrutura por ciclos da pesquisa-ação

A Tabela 5.1 relaciona as cinco fases do processo de pesquisa-ação com seus respectivos objetivos específicos, proposições e pontos de análise já explicitados no item 4.4.

Tabela 5.1 – Estruturação da Pesquisa

FASES	OBJETIVOS	PROPOSIÇÕES	PONTOS DE ANÁLISE
1-EXPLORATÓRIA	01	01	01
2-AVALIAÇÃO-AWA	01 e 02	01	02 e 03
3-AVALIAÇÃO/CHEKLIST	03	02 e 03	04 e 05
4-MODELO WANG-EXCEL	04 e 05	04 e 05	06
5-METODOLOGIA	06	06	07

A seguir estão detalhadas as cinco (5) Fases do processo de pesquisa-ação específicas desta pesquisa.

Cada uma das Fases tem como entrada um ou mais Objetivos específicos; tem como resposta a Proposição que é obtida e tem como saída: Entregáveis, Ponto de Análise e Próximo passo.

5.2 FASE 1 – EXPLORATÓRIA

A literatura pesquisada e apresentada no Capítulo 3 mostra a falta de visão sistêmica para segurança de software, formalização de avaliações e obtenção de resultados que sejam compartilhados entre especialistas e gestores em segurança. No caso de segurança de software e aplicações web o assunto aborda segurança de rede, exploração de vulnerabilidades, ferramentas de análise de código e modelos para desenvolvimento de software seguro, este porém, muito pouco utilizado. O que não é tratado dessa forma será minha contribuição para o tema. Esta fase, como mostra a Figura 5.3, tem o foco em conhecer o estado atual de segurança de software e delimitar o contexto do tema dessa pesquisa.

Figura 5.3 – Estrutura da Fase 01

Esta Fase tem como Objetivo Específico - OE 01: “Levantar e conhecer atributos de segurança de software e o estado da arte e o estado da prática no tema” e como proposição a Proposição 01 – “Obtenção de uma visão geral da Segurança de software”.

Esta fase exploratória consiste da revisão bibliográfica e estudo do estado da arte e da prática em segurança de software e em como avaliá-la e medi-la . Foi notada na literatura a falta de visão sistêmica para medição de segurança, incluindo também a falta de uma taxonomia para esta área de pesquisa.

Existem indicações para medição de segurança como citado no Capítulo 3, porém estas indicações para medição são isoladas e tratam de pontos específicos de segurança.

Devido à experiência da autora na área de avaliação de qualidade de produto de software (COLOMBO, 2004) a primeira ideia foi construir modelo de requisitos de segurança para aplicativos de software na web (AWA) e depois avaliá-los em conformidade ao modelo.

Nesta Fase foram explorados inicialmente textos e práticas que pudessem aliar qualidade de produto de software e avaliação de produto de software com o contexto específico de avaliação de segurança de software.

Aprofundando mais os estudos sobre segurança de TI, de SI foram estudados artigos, normas e trabalhos práticos referentes à academia, empresas e instituições conceituadas na área como CMU/SEI (academia), MITRE, NIST (instituições), OWASP, WEBAPPSEC (Fóruns), Microsoft, Imperva, Whitehat, SANS, Symantec (empresas privadas).

Além dessas, existem grandes contribuições na área de instituições ligadas ao governo americano como, por exemplo, DACS & IATAC, NIST – CSCR, CERT/SEI, MITRE e ao governo brasileiro GSI/DSIC, CTIR, CERT.

Nas instituições, empresas e governos foram identificadas práticas utilizadas, mas sem uma sistemática definida, levando ao uso e adoção de práticas isoladas em contextos específicos de segurança de TI e SI, como exemplo: segurança de rede, análise de código fonte, garantia da segurança por meio de controles para a gestão dentre outras e utilização de algumas ferramentas específicas em contextos.

Entre os acadêmicos, a área de segurança de SI ainda é emergente (SAVOLA; ABIE, 2009a) e muito se discute sobre os valores científicos da área (BELLOVIN, 2011). Alguns pesquisadores e centro de pesquisas indicam alguns caminhos a serem pesquisados e fazem alguns experimentos na área (JANSEN, 2009), (GOERTZEL, 2008).

Não foram encontrados modelos e metodologias de medição e avaliação da segurança em aplicações web.

Com as informações obtidas, tanto de publicações como trabalhos práticos e também das pesquisas de campo como a do Ponemon, Ernst & Young, Symantec, a autora começou a compor uma Identificação de fatores que influenciam a Segurança de TI e SI e que são reconhecidos, mesmo que parcialmente, pelas comunidades de práticas e pesquisadores.

Sabe-se que em diversas áreas, existe a necessidade de estabelecer contextos genéricos aceitáveis por comunidades afins, é a criação de modelos, normas nacionais e internacionais. No contexto específico de gestão de segurança de sistemas de informação a série de normas ISO/IEC 27000 (ISO/IEC 27000, 2009) e as iniciativas do modelo *Common Criteria* que levaram à norma (ISO/IEC 15408-1, 2009) (CC, 2001) colaboraram para uma identificação de requisitos para segurança de sistemas de software.

A identificação de requisitos de segurança para sistemas de software indicou a necessidade de estudos mais aprofundados para segurança de aplicações web (AWA), dado que este estudo tem como premissa não utilizar análise de código de aplicações web.

O resultado desse estudo concluiu a existência da falta de uma visão sistêmica, a falta de uma parte conceitual homogênea tal como uma taxonomia e nomenclatura consensual na área.

A autora construiu a macro visão da proposta para avaliação da segurança de software mostrada na Figura 5.4. Esta proposta parte da definição de um Modelo de segurança para aplicação web que é criado a partir de um conjunto de propriedades de segurança reconhecidas mundialmente. Este Modelo permite criar de forma organizada um conjunto de requisitos funcionais e não-funcionais para implementar segurança em aplicação web (AWA). Com esta estrutura definida, é possível estabelecer uma metodologia para avaliar o quanto a aplicação web está conforme ao Modelo de segurança.

Figura 5.4 - Macro visão da proposta

5.2.1 Ponto de Análise

Neste ponto, a reflexão mostrou que a proposta era muito genérica e que mais estudos eram necessários para atingir o Objetivo Geral. As propriedades e requisitos de segurança foram identificados, no entanto não havia meios de avaliar estas propriedades e estes requisitos de segurança. Outra percepção foi de que a pesquisa Ponemon apontou para aplicações Web (AWA) e como não havia interesse em análise de código ficou decidido que o próximo objetivo específico era trabalhar com aplicações Web em tempo de execução.

5.2.2 Entregável

O estudo nesta fase possibilitou construir uma primeira visão do caminho que teria que ser desenvolvido para a solução para a questão desta pesquisa, a Figura 5.4 mostra a macro visão.

A bibliometria realizada mostrou uma a seguinte classificação como mostra a Figura 5. 5:

Figura 5.5 – Publicações por tipo de mídia

A Figura 5.6 mostra o número de publicações encontradas na área entre os anos de 1999 e 2013 -.

Figura 5.6 – Publicações encontradas entre 1999/2011

A Tabela 5.2 mostra os *Journals* onde foram encontradas as publicações.

Tabela 5.2 – *Journal* e número de publicações

<i>Journal</i>	Número de Publicações
<i>IJCSNS – Internacional Journal of Computer and Network Security</i>	2
<i>Journal of Information Processing Systems</i>	1
<i>International Journal on Advances in Security</i>	1
<i>Journal of Networks</i>	1
<i>Crosstalk The Journal of Defence Software Engineering</i>	2
<i>International Journal of SoftwareEngineering and Knowledge Engineering</i>	1
<i>IJCSE – International Journal on Computer Science and Engineering</i>	1
<i>IEEE Security & Privacy</i>	2

<i>Journal</i>	Número de Publicações
<i>IEEE Computer and Realiability Societies</i>	2
<i>http://msdn.microsoft.com/pt-br/magazine/ee532082(en-us).aspx</i>	1
<i>IA newsletter Vol9 N2 Fall 2006- http://iac.dtic.mil/iatac</i>	1
<i>Produto & Produção</i>	1
<i>Future Generations of Computer Science</i>	1

O ARTIGO PIBIC 2011 “Qualidade de software e de gestão de TI com foco no atributo de Segurança de software” AUTORES: Regis Teruo Nomi; Regina Maria Thienne Colombo Centro de Tecnologia da Informação Renato Archer – CTI Divisão de Segurança de Sistemas da Informação PUBLICADO na XI Jornada de Iniciação Científica do CTI Renato Archer – JICC’2011 PIBIC/CNPq/CTI– Setembro de 2011 – Campinas – São Paulo.

5.2.3 Próximos Passos

As próximas três fases são compostas por ciclos obedecendo à estrutura da Figura 5.2. Foram necessários três Ciclos para obtenção do Objetivo geral.

Cada Ciclo é guiado pelas atividades: Planejar, Agir, Monitorar. O Ciclo também tem como entrada Objetivo (s) Específico (s) e tem como saída Ponto (s) de Análise.

A seguir é mostrado a Fase 2 que engloba o Ciclo 01.

5.3 FASE 2 – CICLO 01 DA PESQUISA–AÇÃO

Esta fase tem como foco uma avaliação empírica de uma aplicação web escolhida como AWA. Esta AWA escolhida será chamada por SISTEMAWEB a partir deste ponto. Nessa avaliação foi explorada a segurança de acesso de maneira aleatória apenas com a visão de *hacker*. A Figura 5.7 mostra os objetivos específicos desta fase, a proposição, o ponto de análise e os entregáveis.

Figura 5.7 – Estrutura da Fase 02

Os passos dentro do ciclo:

5.3.1 Planejar

O SISTEMAWEB é um ambiente computacional que permite a interação dos membros de uma equipe dedicada à produção de um determinado resultado, por meio do qual se pode registrar e trocar informações assim como ter acesso a ferramentas computacionais. O ambiente de trabalho pode ser criado e configurado para cada tipo de resultado produzido pela instituição. O sistema é voltado para a gestão dos resultados de instituições de pesquisa de órgãos federais, e foi concebido e desenvolvido por uma equipe do CTI.

Os motivos/razão da sua escolha foram:

- A proximidade da equipe responsável pela aplicação;
- Esta aplicação atende a onze Instituições do MCTI em todo o país sendo acessível através da web com hospedagem no CTI;
- Esta aplicação nos é familiar há muitos anos, desde sua primeira versão *stand alone*;

- Para a versão Web, foi publicado um Edital e continha especificações de requisitos, incluindo os de segurança. Na aceitação do produto foram realizados testes de software e segurança.

5.3.2 Agir

Foi realizada uma primeira avaliação, com abordagem exploratória para conhecer o comportamento do SISTEMAWEB perante alguns atributos de segurança. Um método informal foi um teste de acesso à aplicação por meios não convencionais de um usuário típico.

A avaliação empírica contou com o apoio de um profissional de segurança especialista em análise de vulnerabilidades.

A equipe responsável pelo SISTEMAWEB disponibilizou uma versão específica para esta avaliação, ou seja, isolada do ambiente da versão de produção.

O foco da avaliação foi o requisito Autenticação de usuário, pois este é o primeiro requisito utilizado no acesso a uma aplicação web. Os achados/resultados desta avaliação foram documentados em Relatório enviado à equipe responsável. Este relatório está no APÊNDICE 1.

A avaliação constatou vários defeitos/vulnerabilidades relacionados a autenticação de usuário, defeitos que podem ser considerados típicos em aplicações web e também defeitos originados por uma simples falta de conhecimento e visão para assegurar segurança em uma aplicação que é disponível na web.

5.3.3 Monitorar

Foi realizada uma reunião entre a equipe de avaliadores e a equipe responsável pelo SISTEMAWEB para a exposição dos problemas encontrados. O relato foi reconhecido pela equipe responsável.

Foi discutido também com a equipe responsável questões com o propósito de fazer uma análise ampla das causas e dos desdobramentos das vulnerabilidades encontradas no sistema.

As questões foram:

Em relação aos problemas encontrados e relatados no relatório da avaliação, qual a sua visão:

- A vulnerabilidade é nova ou já conhecida por vocês?
- A gravidade da vulnerabilidade é (Pequena, Média, Alta)?
- A fonte/causa do problema é de segurança na Rede, Servidor, Aplicação-Código, Arquitetura?
- Tem outros desdobramentos de correções no sistema?
- Quem é o responsável por corrigir?
- Qual o prazo estimado para corrigir?
- Que problemas podem gerar ao usuário do sistema?
- Que ações devem ser geradas pela equipe de desenvolvimento?
- Que ações devem gerar aos responsáveis pelo SISTEMAWEB?
- Na especificação de requisitos existia algum requisito para evitar esta vulnerabilidade?

Foi interessante estes questionamentos, pois percebeu-se que em geral são realizados testes e correções dos defeitos, mas sem uma análise mais ampla das ocorrências.

5.3.4 Entregável

1- Artigo publicado no evento de Portugal, IADIS 2010 Actas da Conferência IADIS IBERO-AMERICANA WWW/INTERNET 2010 – ALGARVE, PORTUGAL, DEZEMBRO 10-11 2010. Organizado por *IADIS International Association for Development of the Information Society* Com apoio FCT Fundação para Ciência e a Tecnologia – Consórcio Doutoral.

2 - Relatório da avaliação do SISTEMAWEB, ver APÊNDICE 1.

3 – Identificação da adequação de focar a pesquisa para avaliar autenticação de usuário

5.3.5 Ponto de Análise

Os resultados desta avaliação mostraram as fraquezas e vulnerabilidades associadas às aplicações web de modo geral. Esta avaliação foi realizada em outras aplicações web governamental e mostraram vulnerabilidades semelhantes.

Estes resultados remetem à lista do OWASP Top Ten (OWASP-TOPTEN, 2010). Esta lista é composta pelas 10 vulnerabilidades que mais ocorreram no último período do ciclo da pesquisa do OWASP, um exemplo disto é o “*Broken Authentication and Session Management*”, que é a quebra de autenticação e consequentemente afeta o gerenciamento da sessão.

A preocupação neste momento era definir um processo de avaliação porque esta primeira avaliação foi realizada de forma empírica e com os conhecimentos dos especialistas em análise de vulnerabilidade.

Esta simulação e experimento serviu para esboçar um modelo de qualidade de segurança de aplicação web, um conjunto de medições para avaliar a segurança e obter a visão gerencial responsável pela aplicação perante o resultado da avaliação realizada.

Como resultado desta fase, o estudo de normas de qualidade de produto e de segurança de software para montar um processo de avaliação foi idealizado. Este estudo resultou em uma proposta para o Consórcio Doutoral da Conferência IADIS Ibero-Americana WWW/Internet 2010 com o título “Avaliação da Qualidade de Produtos de Software com enfoque na Segurança da Informação”

O trabalho desta Fase assegurou o caminho planejado para a pesquisa de avaliar e coletar as evidências, em tempo de execução, de problemas de segurança de aplicações web.

5.4 FASE 3 – CICLO 02 DA PESQUISA-AÇÃO

Esta Fase tem como objetivo desenvolver uma metodologia sistematizada para avaliação do AWA, mostrada na Figura 5.8. O objetivo é desenvolver um modelo de referência para segurança de acesso, um *checklist* e um processo de avaliação.

Ciclo 02

Figura 5.8 - Estrutura da Fase 03

Aqui foi realizada a prova de conceito com o sistema escolhido SISTEMAWEB miscuído com o desenvolvimento do método, foi executada a segunda avaliação do SISTEMAWEB com método pré-determinado.

5.4.1 Planejar

Com este objetivo o estudo passou a ser a elaboração de um Processo de avaliação para segurança de aplicação web. A base teórica para o processo de avaliação foi a norma ISO/IEC 25040 (ISO/IEC 25040, 2011) onde existe um processo genérico para avaliação de software e sistemas. A Figura 5.9 mostra o processo genérico dessa norma.

Figura 5.9 – Processo de Avaliação Genérico ISO/IEC 25040

Estudos desse processo, principalmente no que se refere aos itens “Estabelecer os Requisitos” e “Especificar a avaliação” foram trabalhados para que fossem detalhados com mais profundidade.

Para obter os requisitos de qualidade, que aqui o foco são os requisitos de segurança, esta proposta parte então das propriedades de segurança que são reconhecidas mundialmente, tanto pelas equipes técnicas como pelas equipes gerenciais. A Tabela 5.3 apresenta a correlação entre as propriedades e requisitos de segurança e os referenciais teóricos utilizados resumindo o estudo citado nas referências.

Tabela 5.3 - Correlação das propriedades e requisitos de segurança e as referências

PROPRIEDADES E REQUISITOS	ISO/IEC 25010	ABNT ISO/IEC 27001	ISO/IEC 15408	OWASP ASVS	MS-IWAS	SAVOLA	WANGI
Confidencialidade	X	X				X	X
Integridade	X	X					X
Não-repúdio	X	X				X	X
Responsabilidade	X	X					
Autenticação	X	X	X	X	X	X	X
Autorização					X	X	
Disponibilidade		X				X	X

As propriedades de segurança surgem como um ponto de partida para se estabelecer uma comunicação entre as equipes técnicas e gerenciais, que a partir delas possam aprofundar no interesse e objetivo específico e comum entre estas partes. A Figura 5.10 mostra as quatro propriedades de segurança a serem consideradas nesta pesquisa.

Figura 5.10 – Uso das propriedades de segurança no contexto técnico-gerencial

As propriedades de segurança pelo lado técnico ainda estão em um nível de abstração que não possibilitam obter medidas da segurança, assim é necessário utilizar de requisitos funcionais de segurança que vêm sendo reconhecidos e publicados pela comunidade.

Os requisitos de segurança, por sua vez, podem ser desdobrados em componentes mensuráveis possibilitando assim a obtenção de medidas por meio de ferramentas, listas de verificação e outros meios.

Com a obtenção das medidas de segurança é possível fazer análises e criar métricas que permitam conhecer o nível de segurança de aplicações e a partir deste ponto é possível estabelecer tomada de decisão gerencial para melhorar e assegurar a segurança de aplicações.

A Figura 5.11 mostra os nove (9) requisitos de segurança e como eles podem ser utilizados pelas equipes interessadas.

Figura 5.11 - Requisitos de segurança no contexto técnico-gerencial

Estabelecidas propriedades de segurança e requisitos de segurança será realizada uma investigação sobre a correlação entre estas visões de forma a possibilitar a interpretação da segurança da aplicação em termos de propriedades pela equipe de gestão e em termos de requisitos pela equipe técnica, esta proposta é mostrada na Tabela 5.4, onde somente algumas correlações foram assinaladas.

Tabela 5.4 – Correlação das propriedades com os requisitos

Propriedades Requisitos	Confiden- cialidade	Integrid ade	Disponibili dade	Não - repúdio	Responsab ilidade	Autenticida de
Autenticação	X	X			X	
Autorização						
Gestão de sessão	X	X	X		X	
Controle de acesso					X	
Validação de entrada						
Criptografia					X	
Gestão de configuração			X			
Gestão de exceção	X	X			X	

5.4.2 Agir

A ideia principal veio do estudo da Wang & Wulf e junto com os especialistas de segurança foi elaborado o desdobramento da propriedade de segurança Autenticação para componentes mensuráveis. (WANG; WULF, 1997)

Savola também utilizou os desdobramentos da Wang & Wulf para sugerir equações analíticas na obtenção das medidas (SAVOLA, 2007). Nesse contexto os elementos mensuráveis indicados por Wang puderam ser encontrados nas práticas das comunidades como sendo itens que formam o conjunto de requisitos funcionais de segurança, por exemplo, nos trabalhos da comunidade OWASP, no projeto ASVS (OWASP-ASVS, 2009) eles existem. Este projeto define um conjunto de requisitos para Autenticação, Autorização entre outros.

Um desenvolvimento da primeira versão de um *checklist* passou por três ciclos de elaboração e testes de versões evolutivas até se chegar à sua versão final.

A intenção deste *checklist* é a de oferecer aos avaliadores e auditores uma forma de verificar se uma AWA atende a requisitos de segurança de software para web.

A metodologia utilizada no desenvolvimento do *Checklist* seguiu as seguintes etapas:

1. Realização de um levantamento das melhores práticas para segurança de acesso de aplicações web;
2. Revisão bibliográfica e coleta de recomendações sobre segurança na Web, incluindo a análise do estado da arte no que se refere a *checklist* para qualidade e segurança de software de modo geral;
3. Montagem da primeira versão do *checklist* a partir da reformulação e organização das recomendações selecionadas;
4. Verificação e revisão do *checklist* pela leitura por um grupo de especialistas em segurança de software originando a segunda versão do *checklist*;
5. Validação e revisão do *checklist* pela sua aplicação no SISTEMAWEB originando a terceira versão do *checklist*;

6. Validação e revisão do *checklist* pelo confronto dos resultados de sua aplicação com as observações obtidas numa aplicação web crítica no aspecto da segurança.

As inspeções por *checklist* são técnicas de avaliação capazes de identificar uma grande quantidade de problemas gerais e repetitivos que podem interferir na segurança de uma aplicação web.

O *checklist* se caracteriza por fornecer procedimento de ajuda rápida para a verificação da conformidade de uma aplicação web em referencia à um modelo de referência, por meio de atributos de segurança contidas em uma lista de verificação.

As vantagens da avaliação realizada por meio de *checklist* apresentam a seguintes potencialidades vivenciadas nas avaliações MEDE-PROS (MEDE-PROS®, 2006):

- Redução de custos da avaliação por ser uma técnica de rápida aplicação;
- Facilidade de identificação de problema de segurança, devido à especificidade das questões do checklist;
- Sistematização da avaliação, que garante resultados mais estáveis mesmo quando aplicada separadamente por diferentes avaliadores;
- Avaliação pode ser realizada por profissionais de desenvolvimento de software com conhecimento em segurança.

Os resultados obtidos confirmaram a validade do *checklist* proposto como uma ferramenta de avaliação da segurança de aplicação Web.

Foi desenvolvido o *Checklist* para Autenticidade conforme os níveis da Tabela 5.5

Tabela 5.5 - Cinco níveis da propriedade de Autenticidade

NÍVEL 1	NÍVEL 2	NÍVEL 3	NÍVEL 4	NÍVEL 5
AUTENTICIDADE	AUTENTICAÇÃO	MECANISMO	CARACTERÍSTICAS BÁSICAS	Revela Informações
				No Host Servidor
				Identifica Informações do Cache
				Múltiplos Usuários
				Perda de Credenciais
				Múltiplas Camadas
				URL's Privilegiadas
				Auto-Complete OFF
			REAUTENTICAÇÃO	Reautenticação Exigida
				Reautenticação Navegador
			MENSAGENS	Mensagens de Erro
				Mensagens Não-informativas
			TIMEOUT	Timeout por Inatividade
				Timeout Adequado
				Timeout Cancela Seção
				Cancela Sessões Simultâneas
			CRIPTOGRAFIA	Criptografia de Dados Sensíveis
				Acesso Seletivo
				Serviços (Dados) Externos
				Senha Não-criptografada
			LOGOUT	Criptografia na Rede
				Logout Usuário
				Cancela Todas as Sessões
			BLOQUEIO	Refresh preserva Logout
				Bloqueio de Usuário
				Máximo de Tentativas
				Detem Força-bruta
			CARACTERÍSTICAS ADICIONAIS	Bloqueio de Host (IP)
				Desabilita Usuário
				Login Resiste a SQL Injection
				Senhas Temperadas
			IDENTIDADE	Páginas de Senhas em HTTPS
				Páginas (Dados) Sensíveis em SSL
			CARACTERÍSTICAS BÁSICAS	Política para ID
				ID no Host-cliente
				ID no Host-servidor
				Força-bruta na Autenticação possível
				Adivinhação de Credenciais possível
			ID/SENHA	Política (Regras) para Senhas Fortes
				Senha Anterior em Mudanças
				Reutiliza Senhas Anteriores
				Muda Senha no 1o Login
				Recurso para Recuperar Senha
				Recurso CAPTCHA
				Usuário Muda Detalhes (Senha)
				Senha apresentada em Plain Text

5.4.3 Monitorar

Na tentativa de utilizar o *checklist* na obtenção de medidas foi detectado que não haveria possibilidade de responder ao *checklist* somente com a execução do aplicativo web. Então foram realizadas reuniões com a equipe responsável pelo aplicativo que conseguiam responder as questões e indicavam as evidências comprobatórias das respostas.

A partir desta constatação o *checklist* não seria útil para uma avaliação do aplicativo em tempo de execução e sim para uma auditoria no produto com comprovações em tempo de execução e com o apoio da equipe responsável pelo produto.

5.4.4 Entregável

1-A visão da estruturação de modelo de referência para segurança de acesso, como mostrado nas Figuras 5.10 e 5.11.

2-Método sistematizado – *Checklist de Avaliação de Autenticidade*, APÊNDICE 3.

3-Artigo ICSSEA França, 2011.

5.4.5 Ponto de Análise

Foi elaborado um exemplo de Modelo de referência de segurança com quatro (4) propriedades. Este modelo é apenas um exemplo do que um modelo de referência pode ser. Ele pode depender da categoria de software onde está inserido. Por exemplo, um software da categoria gerencial tem um modelo de referência diferente de um software da categoria financeiro ou de um software crítico. Os modelos dependem do contexto da aplicação e de suas especificidades.

Existe no processo de avaliação uma atividade que é a especificação do modelo de qualidade, que consiste em um conjunto de requisitos de segurança para o AWA. Estes requisitos são derivados de literatura e outros trabalhos relacionados, enquanto as necessidades específicas são definidas pelo AWA e pelo requerente da avaliação.

Os resultados da avaliação podem ser apresentados de forma qualitativa ou qualquer forma quantitativa. Na forma qualitativa, descreve-se o atendimento

aos requisitos de segurança e indica os pontos de melhoria a serem realizados no produto. Na forma quantitativa, as medidas são convertidas em valores numéricos e normalizadas. Com este procedimento é gerado uma pontuação para se estabelecer o nível de segurança. Este resultado contribui na tomada de decisão sobre o AWA.

Finalmente, a parte quantitativa que auxilie na priorização e pontuação dos atributos de segurança precisa ser mais bem estudada para que os objetivos sejam melhores visualizados, analisados e alcançados.

5.5 FASE 4 – CICLO 03 DA PESQUISA-AÇÃO

Esta fase novamente tem-se uma prova de conceito com a utilização do Modelo da Wang & Wulf (WANG; WULF, 1997), com método AHP (SAATY, 2008) e calculado em uma planilha de cálculo, por exemplo, em Excel.

A Figura 5.12 mostra os objetivos, a proposição, o ponto de análise e os próximos passos.

Figura 5.12 – Estrutura da Fase 04

Objetivo Específico 03 – Transformar propriedades de segurança intangíveis em atributos de segurança tangíveis e quantificar atributos tangíveis de segurança.

Os passos dentro do ciclo:

5.5.1 Planejar

Este Ciclo tem como foco a utilização de um método para auxiliar na questão de pontuar e classificar os tipos de respostas do *checklist*.

Wang & Wulf (WANG; WULF, 1997) sugere, mas não demonstra a utilização do método multicritério AHP, nos componentes mensuráveis que tiveram origem em uma decomposição dos requisitos de segurança. É necessário diferenciar a importância relativa ou pesos entre esses componentes. Estudando e conhecendo o método AHP, este se mostrou muito apropriado, pois:

- O método AHP divide o problema em níveis hierárquicos;
- Fornece uma escala onde especialistas quantificam os julgamentos;
- Julgamentos par a par entre os múltiplos critérios;
- Usa método matemático (baseado na utilização de autovalores e autovetores);
- Estabelece prioridades, prioriza as alternativas;
- Permite a correção de certo grau de inconsistência nos julgamentos;
- Possui a abordagem Ratings;
- Faz análise de sensibilidade, isto é, grau de robustez do modelo.

Com este planejamento foi possível definir o processo de avaliação e a atividade relacionada a “Especificação da avaliação”.

Assim, foi feita uma adaptação do processo de avaliação para um processo de avaliação de segurança de aplicação web, como mostra a Figura 5.13.

Figura 5.13 – Processo de Avaliação de Segurança de aplicação

Mapeamento dos sete passos do AHP para Medição da Segurança de Acesso da AWA:

Etapa 1: Compreender as propriedades de segurança de aplicações Web. O sistema é estudado em detalhes com o foco na identificação de critérios de segurança, nos critérios/sub-critérios com base em informações de segurança, crenças e convicções dos desenvolvedores, e alternativas para resolver o problema. Conhecer as propriedades e requisitos de segurança de software, as boas práticas para serem implementadas em aplicações Web, trabalhos, orientações e discussões em medição de segurança de software que é uma área em pesquisa e que está começando a ser explorada.

Escolher uma aplicação web alvo (AWA) e verificar o seu comportamento perante explorações de vulnerabilidades e aplicações de ataques que são comuns na web.

Etapa 2: Hierarquia Problema de Decisão - O problema de decisão é dividido em níveis hierárquicos, a fim de facilitar a compreensão e avaliação. A Figura 2.3 – Estrutura Hierárquica com *Ratings*, ilustra a estrutura de critérios hierárquicos na sua formulação.

O conhecimento teórico e prático obtido do passo anterior possibilita a criação de uma estrutura hierárquica que retrata propriedades, requisitos e atributos

que uma AWA deve ter para assegurar níveis de segurança. Esta estrutura hierárquica denomina-se Modelo de Referência de Segurança.

Etapa 3: Coletar julgamentos par à par dos especialistas. Uma vez que a estrutura esteja montada é necessário coletar dados sobre os julgamentos de especialistas ou tomadores de decisão em pares de comparação, tanto das alternativas como o foco de cada sub-critério, como os sub-critérios e critérios em relação ao imediatamente nível superior (BOLDIN & GASS, 2003).

Um grupo de especialistas em segurança de software (3 pessoas), em desenvolvimento de aplicação web (2 pessoas), na aplicação da metodologia AHP (1 pessoa) reuniu-se para validar o Modelo de Referência de Segurança para AWA e para estabelecer os pesos de importância para os critérios que compõem o Modelo na forma de comparação par a par entre os critérios nos diferentes níveis da estrutura hierárquica.

Etapa 4: A construção das matrizes de decisão. Cada resposta ao questionário desenvolvido na etapa anterior deve ser organizada em uma matriz quadrada, chamada a matriz de decisão, de modo igual ao número de elementos de comparação.

Com os pesos de importância estabelecidos no passo anterior realiza-se a montagem das matrizes de decisão que são oriundas de cada nível hierárquico com suas respectivas comparações entre si. Estas matrizes tem as características de serem matrizes quadradas, de diagonal 1, que possibilitam extrair valores e vetores com significado para definir prioridades para o problema em questão.

Etapa 5: Obtendo os valores e vetores próprios de decisão das matrizes. Pode-se calcular o autovalor e autovetor de qualquer matriz por meio de dois métodos: algébrico e numérico. O cálculo algébrico é feito a partir da equação característica da matriz. O numérico envolve, por exemplo, o cálculo pelo método da Potência. O cálculo algébrico foi mostrado no capítulo II e calculada no modelo da Wang em uma planilha excell. No SuperDecision® é utilizado o método da Potencia.

Com o auxílio de ferramenta para realizar cálculos numéricos, neste caso é adotado a planilha Excel, é possível obter os autovalores e os autovetores que nos dão as prioridades entre os critérios.

Etapa 6: A Razão de Consistência da matriz de decisão. Quando se realiza os julgamentos entre critérios de avaliação é inerente que haja alguma inconsistência, desta forma a metodologia possibilita o cálculo de Razão de Consistência (RC), que permite aos especialistas reverem seus julgamentos para garantir esta consistência. O RC deve ser menor que 0,1.

Etapa 7: Processo de Agregação dos Vetores de Prioridade. Após a obtenção dos vetores de prioridades das matrizes de decisão referentes às alternativas sob cada subcritério, dos subcritérios em relação aos critérios superiores e dos critérios para a relação com o objetivo principal devem ser gerados os valores finais das alternativas.

Com os critérios e os seus respectivos pesos estabelecidos para o problema em questão, com sua validação pelos especialistas, a metodologia fornece o vetor de prioridade que possibilita conhecer o que é mais relevante para atender ao problema.

Nesta Fase o objetivo foi de conhecer o nível de segurança das propriedades de segurança estabelecidas no modelo da Wang para uma AWA, isto é, com a aplicação da metodologia AHP é possível estabelecer uma hierarquia de prioridades da AWA.

A priorização de atributos intangíveis de segurança de software proporciona à nossa proposta a medição das propriedades de segurança de acesso, e isso é incorporado em uma visão mais ampla tratada no processo de avaliação de segurança de aplicações web em tempo de execução (COLOMBO; GUERRA, 2009).

O processo de avaliação descrito consiste em cinco fases, cada uma delas apresenta uma estrutura bem definida. A Figura 5.13 mostra o processo para avaliar a segurança de software e as suas atividades.

Esta Fase detalha e foca nas duas fases do processo de avaliação de software de segurança mostrada na Figura 5.13 (WANG; WULF, 1997).

Na primeira fase do processo, "Estabelecer os requisitos de avaliação", a atividade "Definição de requisitos de segurança" resulta na saída do modelo de segurança de acesso adotada nesta Fase, como mostrado na Figura 5.13.

Na segunda fase do processo, "Especificar a avaliação", a atividade "Pontuar e definir prioridades" resulta na saída da coluna de vector W de uma matriz quadrada, mostrada na fórmula (1). O modelo para segurança de acesso proposto pela Wang & Wulf resulta na Figura 5.14.

Figura 5.14 - Modelo de Qualidade de Segurança de Acesso – (WANG; WULF, 1997)

Outro tópico a ser planejado é a composição da equipe de especialistas que irão aplicar a escala de Saaty (SAATY, 2008) para os atributos de segurança. Esta equipe é formada por especialistas em segurança e especialistas do negócio da aplicação web.

5.5.2 Agir

Aplicar o método AHP de forma mais sucinta:

- 1) Definição do problema,
- 2) Estruturação da hierarquia de decisão,
- 3) Construção da matriz de decisão, como um conjunto de matrizes de comparação de pares, onde cada Banco, em nível de elemento ano superior é usada para comparar os elementos no nível abaixo imediatamente com relação a isso ,
- 4) Sintetização final, obtenção da taxa global ou prioridade global usando as obtenues Prioridades das comparações de peso para as prioridades no nível abaixo imediatamente, eficaz e fazendo isso para cada elemento.

Neste ciclo, o modelo contém quatro propriedades de segurança: Autenticação, Confidencialidade, Integridade, e Não repúdio. O Modelo de Segurança pode ser construído com variações dessas propriedades dependendo do contexto e padrão adotado. Com base na decomposição de atributos de segurança proposta por Wang (WANG; WULF, 1997) que tem sido utilizada por Savola (SAVOLA, 2007) e (SAVOLA; ABIE, 2009a) e com a experiência das decomposições feitas nos Modelos de Qualidade do MEDE-PROS® (MEDE-PROS, 2006), pode-se estruturar a decomposição de requisitos de segurança para identificar medidas de segurança para conhecer o status da Segurança de acesso. Esta decomposição segue as quatro (4) atividades do método AHP.

A metodologia AHP é aplicada ao modelo de segurança de acesso, o modelo é composto de atributos intangíveis e necessita obter os componentes mensuráveis e estabelecer um critério de decisão - função relacionada, pesos e prioridades dos componentes mensuráveis de cada atributo de segurança. Esta decomposição considera a relação funcional na hierarquia. Como um exemplo, a Tabela 5.3 mostra três (3) matrizes de decisão de 3x3 que foram construídas com a ajuda de especialistas, foi aplicado a escala de Saaty para priorizar os atributos de segurança. Para os cálculos, foram produzidos treze (13) matrizes, sendo que dez (10) delas são matrizes 2x2 e as três restantes 3x3 são apresentadas na Tabela 5.3.

A equipe de especialistas foi formada por um gerente, dois projetistas e dois desenvolvedores com experiência de desenvolvimento de software e com conhecimento dos atributos de segurança. Eles foram entrevistados e atribuíram valores da escala de Saaty com base em suas experiências individuais. Os resultados obtidos são apresentados na coluna "Prioridade" da Tabela 5.4.

O método AHP também pode evitar erros de julgamento subjetivo e aumentar a probabilidade de que os resultados sejam confiáveis. Na tabela 5.6 pode-se ver o IC é o Índice de Coerência/ Consistência e RC é a Razão de Consistência (SAATY, 2008). A Razão de Consistência (RC) é obtida através da formação da razão entre o Índice de Consistência (IC) de uma matriz de comparação indicada por $((\lambda_{\max}) - n) / (n - 1)$, e um conjunto de números apropriados, cada um dos quais é um cálculo médio aleatório definido por Forman (Saaty, 2006 apud Forman, 1990).

Esta média é utilizada para formar o Índice de Consistência (IC) aleatório. O Índice de Consistência (IC) calculado pela matriz de decisão é comparado com o valor de IR (?) para fornecer a Razão de Consistência (RC), de modo que:

$$RC = IC/IR.$$

TABELA 5.6 - Matriz A Para o Modelo de Segurança de Acesso

Critérios do Objetivo					
Segurança de Acesso	A	CI	NR	Prioridade	Norml
1. Autenticação (A)	1	5	7	3,1237	0,7223
2. Confidencialidade e Integridade (CI)	1/5	1	4	0,8865	0,2050
3. Não Repúdio (NR)	1/7	1/4	1	0,3145	0,0727
ordem da matriz = 3		IC = 0,0412		RC = 0,0711	
Subcritérios 2					
Confidencialidade e Integridade	PC	SF	CASw	Prioridade	Norml
2.1. Proteção Criptográfica (PC)	1	1	7	3,0000	0,4667
2.2. Segurança Física (SF)	1	1	7	3,0000	0,4667
2.3. Controle de Acesso do Sw (CASw)	1/7	1/7	1	0,4286	0,0667
ordem da matriz = 3		IC = 0,0000		RC = 0,0000	
Mecanismo	CNST	CONF	INT	Prioridade	Norml
3.1.1. Consistência (CNST)	1	1/7	1/5	0,3396	0,0719
3.1.2. Confiabilidade (CONF)	7	1	3	3,0649	0,6491
3.1.3. Integridade (INT)	5	1/3	1	1,3171	0,2790
ordem da matriz = 3		IC = 0,0216		RC = 0,0373	

Se RC é menor que 0,1, então, os julgamentos da matriz de decisão são considerados consistentes, caso contrário há alguma inconsistência nos ensaios e especialistas podem ser convocados a reverem seus julgamentos.

A Tabela 5.6 destaca as matrizes 3x3 que são apresentados na Tabela 5.4 A primeira refere-se ao objetivo principal que é Segurança de acesso. A segunda é Confidencialidade e Integridade e a terceira refere-se ao mecanismo Não-repúdio.

A interpretação do resultado na Coluna "Prioridade" é que a Integridade da Identidade de Autenticação, o componente (1.2.2) é o atributo mais importante para os critérios de autenticação como o seu valor é 0,5267, como Tabela 5.7. Este resultado encontra o "sentimento" dos especialistas entrevistados sobre o problema.

A pontuação da Segurança de acesso da aplicação web alvo – AWA é calculada como a soma das dezoito (18) folhas mostradas na Figura 5.11 e os seus respectivos pesos prioritários mostrados na coluna "Prioridade" da Tabela 5.7. Também é possível realizar uma análise de sensibilidade.

Este tipo de análise dá uma ideia sobre a robustez do modelo e a estabilidade dos resultados (devido a alterações nos níveis de ensaios), e mostra o limite/thresholds no qual um critério teria prioridade sobre os outros

TABELA 5.7 – Resultados do AHP

Critério	Subcritério 1	Subcritério 2	Subcritério 3	Prioridade
1. Autenticação	1.1. Mecanismo	1.1.1. Confiabilidade		0,0150
		1.1.2. Integridade		0,1053
	1.2. Identidade	1.2.1.1. Unicidade	1.2.1.1. Unicidade	0,0564
		1.2.1.2. Estrutura	1.2.1.2. Estrutura	0,0188
		1.2.2. Integridade		0,5267
2. Confidencialidade e Integridade	2.1. Proteção Criptográfica	2.1.1. Algoritmo	2.1.1.1. Implementação	0,0717
			2.1.1.2. Grau de teste	0,0102
		2.1.2. Chaves	2.1.2.1. Comprometimento da Chave	0,0014
			2.1.2.2. Armazenamento da Chave	0,0123
	2.2. Segurança Física	2.2.1. Mídias Físicas		0,0159
		2.2.2. Acessibilidade		0,0797
	2.3. Controle de Acesso do	2.3.1. Eficácia		0,0020
		2.3.2. Confiança		0,0117
3. Não Repúdio	3.1. Mecanismo	3.1.1. Consistência		0,0044
		3.1.2. Confiabilidade		0,0393
		3.1.3. Integridade		0,0169
	3.2. Prova de Identificação	3.2.1. Integridade		0,0106
		3.2.2. Confiabilidade		0,0015

Este tipo de análise dá ideia sobre a robustez do modelo e a estabilidade dos resultados (devido às alterações nos níveis de ensaios), e mostra o limite/thresholds no qual um critério teria prioridade sobre os outros.

5.5.3 Monitorar

Este método que transforma os atributos intangíveis em atributos tangíveis como mostra a Figura 5.15, tem a peculiaridade que a distingue de outros métodos de tomada de decisão, que é a possibilidade de avaliar os julgamentos feitos entre os elementos de uma matriz por seu autovalor máximo, e verificar algum nível de inconsistência, segundo Saaty (SAATY, 2008), a Razão de Consistência (RC) pode assumir valores até 0,10, sem comprometer a integridade do modelo. No final, a matriz gerada tem um autovalor, que produz um peso para o elemento em questão através das equações (1) e (2):

$$AW = \lambda_{\max} W \quad (1)$$

$$w = 0 \text{ or } \text{Det}(A - \lambda I) = 0$$

(2)

Figura 5.15 – Como passar dos intangíveis para os tangíveis

Por exemplo, no caso de uma matriz 3x3, existem três valores de λ que satisfazem a equação (2). O maior valor é utilizado para produzir o vetor de normalização, a partir da qual é possível obter o peso dos elementos que pertencem ao objetivo.

5.5.4 Entregável

1- Constatação da adequação da metodologia AHP para uma resposta a questão da pesquisa, o processo da metodologia AHP apoiou o desenvolvimento das fases da pesquisa-ação.

2 - Artigo publicado no WoQS2012 e na *journal* ACM SIGSOFT Software Engineering Notes, November 2012 Volume 37 Number 6, DOI: 10.1145/2382756.2382781 Copyright is held by author.
<http://doi.acm.org/10.1145/2382756.2382781>

3-Experimento com Modelo da Wang & Wulf utilizando o método AHP e a ferramenta Excel.

5.5.5 Ponto de Análise

Concluindo sobre o AHP – os conceitos abaixo foram utilizados e os resultados foram validados por meio da publicação do Artigo:

- Modelo hierárquico

- Pontuação com escala de Saaty
- Cálculo das prioridades com Excel
- Razão de consistência
- *Ratings*.

Este processo de avaliação de segurança de software define um modelo de segurança de acesso que é composto de requisitos de segurança. Este ciclo se decompõe em componentes mensuráveis, resultando em medidas de segurança. Esta abordagem também pode ser utilizada para especificar requisitos durante o ciclo de vida de desenvolvimento de software (SDLC) (McGRAW,2006).

O uso de modelos multi-critérios para tomada de decisão ainda é raramente observada em engenharia de software e na avaliação de segurança de software. Este trabalho contribui para ampliar o âmbito de aplicações do método AHP, e disseminação de seu uso como uma metodologia transparente, eficaz e objetiva para resolver problemas de medição de atributos intangíveis, especialmente aqueles relacionados à pontuação e classificação.

5.6 FASE 5 – CONCLUSIVA

A fase final e conclusiva apresenta a metodologia para medição de atributos intangíveis incluindo os modelos de referência para as propriedades de segurança e a sua implementação da propriedade Autenticidade, aplicada para o SISTEMAWEB como mostra a Figura 5.16.

Figura 5.16 – Estrutura da Fase 05

Nesta fase foram desenvolvidos os quatro (4) modelos de referência para segurança de acesso comumente chamado de C.I.D.A, isto é, Confidencialidade, Integridade, Disponibilidade e Autenticidade como pode ser visto na Figura 5.17

Figura 5.17 – Modelo de Referência para Segurança de acesso

A partir das propriedades de segurança – C.I.D.A. foram criadas as árvores e suas definições (Modelos de referência) com base no estudo das referências adotadas; são mostrados nas Figuras 5.18,5.19,5.20 e 5.21.

Confidencialidade - Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. O conceito de garantir a informação sensível confidencial, limitada para um grupo apropriado de pessoas ou organizações (ISO/IEC 13335-1:2004).

Integridade - Propriedade que salvaguarda a exatidão e completeza de ativos. (ISO/IEC 13335-1: 2004).

Disponibilidade - Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada. A informação deve ser entregue para a pessoa certa, quando ela precisar.

Autenticidade - Propriedade que uma entidade é o que afirma ser (ISO/IEC FDIS 27000, 2009).

A propriedade de segurança Autenticidade é composta por dois (2) componentes: Autenticação e Rastreabilidade. Cada um deles é desdobrado mais uma vez e sucessivamente até obter os atributos mensuráveis.

Figura 5.18 – Modelo de Referência para Autenticidade

A propriedade de segurança Confidencialidade é composta por três (3) componentes: Controle de acesso, Gerência de sessão e Sigilo da informação. Cada um deles é desdobrado mais uma vez e sucessivamente até obter os atributos mensuráveis.

Figura 5.19 – Modelo de Referência para Confidencialidade

A propriedade de segurança Disponibilidade é composta por três (3) componentes: Rede de comunicação, Aplicação web, Servidores de serviço. Cada um deles é desdobrado mais uma vez e sucessivamente até obter os atributos mensuráveis.

Figura 5.20 – Modelo de Referência para Disponibilidade

A propriedade de segurança Integridade é composta por um (1) componente: Entrada e saída de dados. Este é desdobrado mais uma vez e sucessivamente até obter os atributos mensuráveis.

Figura 5.21 - Modelo de Referência para Integridade

Das quatro propriedades de segurança de acesso, a propriedade Autenticidade foi escolhida para ser detalhada com a metodologia.

Não importa o tipo de sistema de segurança de computador que seja, a primeira etapa a ser executada é a identificação e autenticação: Quem é você? Como provar isso? (SCHNEIER, 2001)

A Figura 5.22 mostra a configuração do Modelo de Autenticidade na ferramenta SuperDecision@s

Da mesma forma, a componente Identidade é desdobrada em dois (2) atributos e cada um deles é desdobrado nos seus respectivos itens mensurável.

A base para o desenvolvimento do *Checklist* está mostrada na Figura 5.23.

Após o término da utilização do *checklist* é realizado o julgamento para par para se estabelecer os critérios de prioridades entre os atributos de segurança.

Figura 5.23 – Base para formalização do Checklist

Para auxiliar no julgamento do SISTEMAWEB foi utilizada a tabela mostrada na Tabela 5.8 com os atributos de Mecanismo. Ela é utilizada pela equipe para fazer a comparação para a par entre os critérios. Esta fase é bastante debatida, mas é necessário que haja um consenso final pela equipe.

Tabela 5.8 – Tabela de auxílio aos critérios

CRITÉRIOS	ESCALA DE SAATY (valores de 1 a 9)	CRITÉRIOS
CARACTERÍSTICAS BÁSICAS		REAUTENTICAÇÃO
		MENSAGENS
		TIMEOUT
		CRIPTOGRAFIA
		LOGOUT
		BLOQUEIO
		CARAC.ADICIONAL
REAUTENTICAÇÃO		MENSAGENS
		TIMEOUT
		CRIPTOGRAFIA
		LOGOUT
		BLOQUEIO
		CARAC.ADICIONAL
MENSAGENS		TIMEOUT
		CRIPTOGRAFIA
		LOGOUT
		BLOQUEIO

CRITÉRIOS	ESCALA DE SAATY (valores de 1 a 9)	CRITÉRIOS
		CARAC.ADICIONAL
TIMEOUT		CRIPTOGRAFIA
		LOGOUT
		BLOQUEIO
		CARAC.ADICIONAL
CRIPTOGRAFIA		LOGOUT
		BLOQUEIO
		CARAC.ADICIONAL
LOGOUT		BLOQUEIO
		CARAC.ADICIONAL
BLOQUEIO		CARAC.ADICIONAL

Resultados obtidos do Modelo e de medição

- Foi identificado os atributos mensuráveis e criado o *checklist* para a propriedade de Autenticidade;
- Utilização do método AHP na ferramenta SuperDecision®
- Foi mapeado o Modelo, mapeado os *checklists*, atribuído os pesos com a escala de Saaty para as comparações par-a-par das matrizes, e o SD faz os cálculos. A equipe interpreta os resultados;
- Fiz a entrevista com a equipe e avaliamos o AWA utilizando o checklist de Autenticidade;
- Mapeei os dados na ferramenta SuperDecision®;
- Gera o relatório com os resultados da medição sobre o estado da segurança do aplicativo web alvo.

Um dos resultados que aparecem no relatório é a Tabela de pontuação com os níveis de hierarquia de decomposição da propriedade Autenticidade para o SISTEMAWEB calculado pela ferramenta SuperDecision®. Os valores apresentados na Tabela 5.9 estão normalizados entre (0 e 1) zero e um. Estes valores foram os atributos que os especialistas esperavam para o sistema. Pois o sistema em questão não possui a classificação dos dados quanto à

segurança, o que ocasiona uma necessidade mais rigososa para a propriedade de Autenticidade.

Tabela 5.8 - Matriz de Decisão

	Cg	Re	Me	Ti	Cri	Lo	BI	Ad
Cg	1	7	5	1	1	5	1	1
Re	1/7	1	3	3	3	3	3	3
Me	1/5	1/3	1	3	3	3	3	3
Ti	1	1/3	1/3	1	1	5	1	3
Cri	1	1/3	1/3	1	1	5	5	3
Lo	1/5	1/3	1/3	1/5	1/5	1	5	1
BI	1	1/3	1/3	1	1/5	1/5	1	5
Ad	1	1/3	1/3	1/3	1/3	1	1	1

Tabela 5.9 - Resultado da Autenticação no AHP para o SISTEMAWEB

Nível 2	Nível 3	Nível 4
Autenticação 0,87	Mecanismo 0,83	Características básicas 0,16
		Reautenticação 0,06
		Apresentação de mensagens 0,02
		Tempo-limite 0,03
		Criptografia 0,40
		Logout 0,18
		Bloqueio 0,10
	Identidade 0,16	Características adicionais 0,83
		Login/Password 0,16

As pontuações apresentadas na Tabela 5.9 para o SISTEMAWEB indicam o grau de atendimento aos critérios, ou seja, aos atributos de segurança e a sua importância relativa na distribuição de pesos entre os componentes de segurança, dentro do modelo de referência utilizado.

5.6.1 Entregável

- Modelo de referência para segurança de acesso de Aplicação Web, que relaciona Propriedades (intangíveis) em atributos mensuráveis;
- O método MED-SEC-AWA para a propriedade Autenticidade;
- Pontuação e priorização com um método de apoio a decisão;
- Abordagem sistemática de modelagem e medição da segurança de acesso de aplicação web;
- Artigo submetido ao *Journal Computers&Security*.

5.6.2 Ponto de Análise

A equipe responsável pela segurança da aplicação pôde usar esse resultado no planejamento de atributos de segurança do SISTEMAWEB e em outros produtos para melhorar a segurança de seus produtos.

Um outro exemplo deste uso é descobrir o que priorizar em testes de software de segurança.

Próximos passos:

Escolha de uma AWA onde a segurança seja um fator crítico; numa futura tese de mestrado.

5.7 RESULTADOS OBTIDOS

Esta pesquisa parte de uma questão central de indagação:

Como medir e conhecer o nível de segurança de acesso de aplicação web?

E traz como premissa a especificação e avaliação de propriedades e requisitos de segurança que possam ser medidos para conhecer o nível de segurança de aplicativos Web.

Para responder essa pergunta, a pesquisa foi estruturada conforme a Tabela 5.1- Estruturação geral da Pesquisa.

A pesquisa estabeleceu o **Objetivo Geral** – Desenvolver uma metodologia de avaliação da segurança de acesso de aplicações web.

Este objetivo desdobrou-se em **Objetivos específicos**.

As **Proposições** foram estabelecidas para atenderem aos objetivos específicos;

Pontos de análise foram colocados para verificarem se houve o atendimento das proposições aos objetivos específicos e para dar o sequenciamento das fases da pesquisa-ação para o atendimento ao objetivo geral da pesquisa.

A Fase 01 possibilitou o estudo teórico dos atributos de segurança de aplicações WEB, esse estudo foi classificado por meio de Bibliometria das publicações utilizadas que são mostradas nas Figuras 5.5 e 5.6 e na Tabela 5.2.

Na Fase 02 foi escolhida a AWA e aconteceram as reuniões com o grupo responsável por esse aplicativo. Foram detectadas as vulnerabilidades da aplicação de forma exploratória. Observaram-se muitas vulnerabilidades relacionadas com a Autenticação de usuário do AWA. Foi decidido por um estudo mais aprofundado sobre a propriedade de segurança Autenticidade.

Na Fase 03 tomou como base o processo de Avaliação para Segurança de Software, foi desenvolvido o *Checklist* de Autenticidade que possibilitou obter as medidas previstas no processo. O resultado da avaliação do AWA com o *Checklist* foi estruturado de forma qualitativa gerando um relatório com o resultado do atendimento ou não da propriedade Autenticidade.

A Fase 04 teve como foco o processo de avaliação com resultados quantitativos, provenientes da Metodologia AHP. Como experimento foi aplicada a metodologia AHP no Modelo de Segurança de software proposto pela Wang & Wulf, em 1997. A ferramenta Excell foi utilizada para os cálculos matemáticos.

Na Fase 05 foi realizada a extensão dos modelos de referências para Confidencialidade, Integridade e Disponibilidade. Foi executada a avaliação da propriedade Autenticidade da AWA com a ferramenta SuperDecision® e os resultados foram acordados com a equipe responsável.

Estes resultados são mostrados de forma sucinta na Tabela 5.10.

Tabela 5.10 – Resumo dos resultados da Metodologia de medição e priorização de Segurança de Acesso de Aplicações Web

Fase 1- Exploratória	
Objetivos Especificos	OE 01
Proposição	P01

Resultado da Fase	Levantamento bibliográfico. Estudo dos conceitos de segurança Web. Classificação dos principais conceitos do tema.
Fase 2 – Ciclo 1 – Avaliação empírica da AWA	
Objetivos Específicos	OE 01 e OE 02
Proposição	P01
Resultado da Fase	Escolha da AWA. Exploração de vulnerabilidade da AWA. Identificação da Propriedade Autenticidade, essencial para AWA.
Fase 3 – Ciclo 2 – Avaliação estruturada da AWA	
Objetivos Específicos	OE 03
Proposição	P02 e P03
Resultado da Fase	Adoção de um processo de Avaliação. Desenvolvimento do <i>Checklist</i> para Autenticidade. Aplicação do <i>Checklist</i> para a AWA. Resultado Qualitativo da Avaliação.
Fase 4 – Ciclo 3 – Transformação dos atributos intangíveis em atributos tangíveis	
Objetivos Específicos	OE 04 e OE05
Proposição	P04 e P05
Resultado da Fase	Aplicação da Metodologia AHP para medição de segurança. Aplicação da AHP para Modelo de Segurança da Wang & Wulf. Utilização da Ferramenta Excell para cálculos matemáticos. Resultado Quantitativo da Avaliação.
Fase 5 – Metodologia de Avaliação de Aplicação Web	
Objetivos Específicos	OE 06
Proposição	P07
Resultado da Fase	Modelo de Segurança de Acesso – C.I.D.A. Ampliação do Checklist de Autenticidade. Modelar a Autenticidade no SuperDecision® e aplicar a escala de Saaty para o AWA. Resultado Qualitativo e Quantitativo da AWA. Relatório final da Avaliação.

Neste Capítulo foi estruturada a pesquisa e foram obtidos os resultados parciais em cada fase da pesquisa. Neste momento obteve-se a resposta da pergunta central.

Para validar essa metodologia foi realizada a avaliação do portal “COMPRAS-ONLINE” que será apresentado no próximo Capítulo que tem o nome de Prova de Conceito.

6. PROVA DE CONCEITO

Este Capítulo apresenta a conceituação de Prova de Conceito e sua aplicação nesta pesquisa.

Uma prova de conceito, ou PoC (sigla do inglês, *Proof of Concept*) é um termo utilizado para denominar um modelo prático que possa provar o conceito (teórico) estabelecido por uma pesquisa.

A prova de conceito permite demonstrar na prática a metodologia, os conceitos e as tecnologias desenvolvidas em um projeto. Trata-se, pois, de uma iniciativa de curto prazo, incluída no desenvolvimento do projeto e orientada de forma restrita ou de acordo com a viabilidade do cenário a disposição. Tem natureza colaborativa, envolvendo a expertise do desenvolvedor e fornecedores e as competências do cliente.

A partir da prova de conceito é possível avaliar os resultados dos testes de aplicação e aceitação, e usar esses resultados para balizar as alterações que se fizerem necessárias na estrutura (lógica e física), antes de gerar uma proposta final.

Em segurança da informação, o termo Prova de Conceito geralmente refere-se ao desenvolvimento de uma ferramenta prática para provar a vulnerabilidade teórica de um sistema de informação (PINHEIRO, 2013).

Aqui se considerou uma aplicação da metodologia desenvolvida para medição e priorização da segurança de acesso para uma aplicação WEB em que a segurança de acesso é um elemento crítico, e com o propósito de verificar que a metodologia em questão é suscetível de serem aplicadas de uma maneira útil para ambas as partes, para a primeira, a validação desta pesquisa e para a segunda, um exemplo prático e real de medir a segurança da sua aplicação WEB.

Os passos dentro deste Ciclo são:

6.1 PLANEJAR

O COMPRAS-ONLINE, nome fictício, é um portal na WEB que permite consultas e compras de Produtos em geral. Este portal é desenvolvido e mantido pela Empresa A.

A Empresa A é uma das principais empresas de TI no mercado Brasileiro, a Empresa atua há mais de 37 anos no desenvolvimento de soluções e serviços. Fornece serviços customizados de TI ao mercado corporativo, orientados às necessidades dos clientes, desenvolve aplicações seguras e integradas para negócios on-line. Ela conta com mais de 3.600 mil colaboradores. A Empresa tem como valores: Inovação, Foco no cliente, Responsabilidade, Competência e Ética. A Empresa tem várias certificações, como: Certificação ISO 9001, desde 1995, certificação ISO 14001, desde 2012, Nível 3 do CMMI, atingido este ano; e já recebeu vários Prêmios, como: *E-Finance* 2009 - 7 prêmios, Prêmio Relatório Bancário nos anos 2007 a 2009; dentre vários outros.

O COMPRAS-ONLINE oferece grande variedade de produtos com descontos, além de ofertas. O Cliente do COMPRAS-ONLINE tem uma grande variedade de produtos, incluindo passagens aéreas e reservas em hotéis com descontos e benefícios exclusivos. É um buscador de ofertas que permite procura e comparação de preços com diversas lojas da internet; oferece parcelamento de pagamento em até 12 vezes sem juros.

Os motivos/razão da escolha do portal COMPRAS-ONLINE foram:

- É uma aplicação WEB em que a segurança de acesso é um elemento crítico;
- Já havia um contato com um Diretor da Empresa e que patrocinou este trabalho com os responsáveis pela aplicação;
- Esta aplicação WEB está disponível, em modo produção e continua em plena evolução.

6.2 AGIR

Foi realizada uma primeira reunião na Empresa A, com dois gestores de Desenvolvimento de Soluções & Sistemas para apresentar a metodologia e os recursos necessários para realizar a prova de conceito. Desta reunião foi escolhida a aplicação WEB alvo (AWA) a ser utilizada para este ciclo.

Após algumas semanas, foi realizada uma segunda reunião na Empresa A, com o gestor responsável, que é PMP (*Project Management Professional*) e CSM (*Certified Scrum Master*), e com o gestor técnico de desenvolvimento e segurança do COMPRAS-ONLINE, para eu conhecer o portal COMPRAS-

ONLINE e apresentar a Lista de verificação MED-SEC-AWA que eles deviam preencher. Foi apresentado o Modelo de referência de Autenticidade e a Lista de Verificação de Autenticidade mostrada no Apêndice 3.

Eles responderam a Lista de Verificação e me enviaram.

Eu analisei a Lista de Verificação preenchida, identifiquei algumas inconsistências e fizemos os acertos.

Em seguida utilizei a ferramenta *SuperDecision®* para inserir o Modelo de referências Autenticidade, as respostas da Lista de verificação e o julgamento dos critérios que compõem o Modelo de referência, este julgamento foi realizado por dois especialistas em segurança de software e que conhecem o COMPRAS-ONLINE como usuários da aplicação.

Com a ferramenta *SuperDecision®* é possível:

- validar o Modelo e suas relações;
- calcular o número de critérios atendidos perante o Modelo, que fornece a medição do COMPRAS-ONLINE perante o Modelo;
- calcular o vetor Prioridade que fornece a priorização entre os critérios do Modelo para o COMPRAS-ONLINE.

Os achados/resultados desta avaliação de segurança de acesso foram documentados em Relatório de Avaliação, que foi enviado à equipe responsável pelo COMPRAS-ONLINE. O Relatório de Avaliação mostra o quanto o produto atendeu ao Modelo de referência para Autenticidade e a priorização dos seus atributos de segurança. Esse relatório auxilia a área de Gestão do COMPRAS-ONLINE a refletir e tomar ações em relação à aplicação WEB.

O relatório é mostrado no Apêndice 4 que contém os tópicos mencionados neste item.

6.3 MONITORAR

Após o envio do Relatório da Avaliação(Ver Apêndice 4) à equipe responsável pelo COMPRAS-ONLINE, eles fizeram algumas considerações e estas foram comentadas por mim, conforme abaixo:

Legenda:

GR - Gestor Responsável pelo COMPRAS-ONLINE;

RC – Autora desta pesquisa.

GR - Página 2/11: O COMPRAS-ONLINE é um portal na web que permite consultas e compras de Produtos, Viagens e Veículos.

Desta forma não é difícil identificar o portal analisado, existem poucos que atendem a esta descrição. Sugiro tornar mais genérica.

RC - Ok, será reescritor.

GR - Página 8/11: ainda não tem os valores para as pontuações, serão apresentados para a gente? Acho interessante dizer quais os impactos desta avaliação, quer dizer, uma pontuação baixa é sinônimo de possível problema?

RC - Falta só esta parte para vocês fazerem. No relatório, nas páginas 6 e 7 tem a Tabela 2. Esta Tabela contém em cada linha um par de critérios que deve ser comparado e preenchido com a Escala de Saaty (pag. 6). Esta comparação é sobre a importância de um critério em relação ao outro. Após o preenchimento por vocês é que terei uma Pontuação final.

GR - Página 9/11, poderia acertar a concordância na frase: “a equipe responsável tem um indicador de onde é prioritário ações para correção”

RC - Ok, será reescrita.

GR - Página 9/11: função auto complete pode ser no navegador do cliente, onde não temos controle.

RC - É possível desabilitar a função autocomplete do navegador por meio de tags HTML (http://www.w3schools.com/tags/att_input_autocomplete.asp). O COMPRAS-ONLINE está de acordo.

GR - Página 9/11: compartilhamento de um mesmo usuário: apesar do ideal ser não permitir, em muitos casos isto pode ser aceito

RE - De acordo com o requerimento 8.5.8 do PCI-DSS (Payment Card Industry - Data Security Standard) o compartilhamento de credenciais não é aceito, pois com isso não é possível identificar um indivíduo unicamente. (<http://www.manageengine.com/products/eventlog/eventlog-other-pci-requirements.html#requirement858>) . O PCI é uma boa referência.

GR - Página 9/11: autenticação antes de operações críticas: em geral é um requisito de negócio neste tipo de aplicação, se o usuário já se logou, não pede nova autenticação no pagamento, para não desestimular compras

RC - O processo de re-autenticação é um requisito importante que pode mitigar ataques a sessão do usuário. Fica o alerta para ser ponderado por vocês.

GR - Página 9/11: bloqueio por IP: este é um site de vendas

RC - Sim, mas um site de vendas pode estar sofrendo ataques, desta forma é necessário separar e bloquear os usuários ilícitos dos usuários legítimos. Fica o alerta para ser ponderado por vocês.

GR - Página 10/11: desabilitar cliente: precisa ver outros aspectos, tipo Código de Defesa do Consumidor, ao qual o site está sujeito.

RC - Ok, Fica o alerta para ser ponderado por vocês.

GR - Página 10/11: SQL injection: seria possível passar onde isto pode ser feito?

RC - Na questão 1.1.8.1 menciona XSS e/ou SQL. O que foi testado foi um XSS e funcionou no campo de busca, porém como os filtros de XSS foram burlados é possível que ataques de SQL Injection possam ser executados com sucesso.

GR - Página 10/11: uso de força bruta: lembrar que é um site de vendas, incluir mecanismos tipo Captcha pode impactar vendas

RC - O Captcha não necessariamente precisa ser utilizado na primeira tentativa do usuário, diversas aplicações a partir da terceira tentativa ativam o Captcha, para trazer mais usabilidade na aplicação e evitar ataques automatizados.

GR - Página 11/11: pedir senha anterior para troca, reuso de senhas: isto é uma regra de negócio, precisa validar com gestores

RC - Sim, é uma regra do negócio, porém fica o alerta para ser ponderado por vocês e gestores, uma senha de somente 3 caracteres aumenta o risco de segurança de senhas.

GR - Página 11/11: recuperação e análise de logs: tem a ver com processos de negócio, o site deve disponibilizar os logs, análise e ações dependem do gestor

RC - É recomendado que os logs devam ser analisados constantemente, tanto para avaliar a "saúde" da aplicação como para identificar anomalias que podem sugerir fraudes ou ataques. Fica o alerta para ser ponderado por vocês e os gestores.

GR - Página 11/11: no caso de reflexões sobre próximas ações, sugiro incluir os gestores de negócio em algum momento (não necessariamente no primeiro)

RC - Com certeza os gestores devem ser envolvidos na conversa, pois eles conhecem as regras do negócio e devem ponderar os riscos, por exemplo, até onde vale a pena correr o risco para vender mais.

Após esta monitoração, outra foi colocada para fechamento desta Prova de conceito.

Foi apresentada a equipe responsável pelo COMPRAS-ONLINE as questões abaixo com o propósito de fazer uma análise do resultado da avaliação, como exemplo, as causas e os desdobramentos das vulnerabilidades encontradas no sistema.

As questões foram:

Em relação aos aspectos a serem revistos e relatados no relatório da avaliação, qual a sua visão:

- A vulnerabilidade é nova ou já conhecida por vocês?
- A gravidade da vulnerabilidade é (Pequena, Média, Alta)?
- A fonte/causa do problema é de segurança na Rede, Servidor, Aplicação-Código, Arquitetura?
- Que ações devem ser geradas pela equipe de desenvolvimento?
- Tem outros desdobramentos de correções no sistema?
- Quem é o responsável por corrigir?
- Qual o prazo estimado para corrigir?
- Que problemas podem gerar ao usuário do sistema?
- Que ações devem gerar aos responsáveis pelo COMPRAS-ONLINE?

Estes questionamentos podem auxiliar a equipe responsável, pois se percebe que em geral são realizados testes e correções dos problemas, mas sem uma análise mais ampla destas ocorrências.

6.4 ENTREGÁVEL

Relatório da avaliação do COMPRAS-ONLINE que mostra de forma quantitativa e qualitativa do desempenho da aplicação WEB, destacando os aspectos positivos e os a serem revistos em relação ao Modelo de referência.

6.5 PONTO DE ANÁLISE

A avaliação constatou vários defeitos/vulnerabilidades relacionados à propriedade Autenticidade, defeitos que podem ser considerados típicos em aplicações web e também defeitos originados por uma simples falta de conhecimento e visão para assegurar segurança em uma aplicação crítica em segurança e que é disponível na WEB.

Como conclusão da aplicação da Prova de conceito, posso ressaltar:

- a importância de ter realizado esta prova de conceito, pois possibilitou algumas correções na própria Lista de verificação;
- a aplicação real da metodologia desenvolvida e indicações de trabalhos futuros para ela;
- a importância e a necessidade de incluir a Análise de risco na metodologia para expandir o Processo de avaliação da segurança de acesso de aplicação WEB alvo, perante o Modelo de referência. A análise de risco em segurança da informação resulta no mapeamento dos riscos relacionados aos ativos (pessoas, processos e tecnologias) pertencentes ao escopo definido pela organização. Esta atividade permite ao cliente, tomar decisões de segurança, que resultará no tratamento priorizado de riscos, aplicando novos controles de segurança ou readequando os controles já existentes e necessários para sua organização (ISO/IEC 27004, 2009)
- Nesta análise de risco pode considerar variáveis como:
  - Ameaças existentes ao plano de negócio;
  - Probabilidade de ocorrência de ameaças;
  - Controles de segurança já existentes e sua respectiva eficácia; e
  - Impacto da concretização dos riscos aos negócios.
- Benefícios da Análise de risco:
  - Visão atualizada dos riscos em segurança que podem expor a aplicação WEB e sua organização.
  - Base para decisões em segurança apoiado em visão isenta e externa à sua empresa.
  - Estabelecimento de indicador de segurança necessário para atendimento ao Modelo de referência.
- Relatório executivo e técnico indicando os riscos mais críticos; descrevendo os riscos identificados e como um plano e recomendações de mitigação dos riscos.

Finalizando este Capítulo, quero ressaltar a importância da realização da ferramenta Prova de conceito nesta pesquisa, pois assegurou o caminho

planejado e desenvolvido para a metodologia desenvolvida pelo método de pesquisa “Pesquisa-ação”.

7. DISCUSSÕES E TRABALHOS FUTUROS

Foi apresentada uma proposta de metodologia para medição e priorização de atributos intangíveis para segurança de software em aplicativos para web, com uma visão sistêmica para segurança de acesso.

Esta proposta foi desenvolvida de acordo com a metodologia de pesquisa “pesquisa-ação” que possibilitou o desenvolvimento da metodologia de forma acadêmica e prática. E a sua evolução foi visivelmente documentada, pois cada Ciclo/Fase os objetivos específicos foram alcançados e os resultados parciais foram obtidos.

O objetivo da pesquisa foi propor uma metodologia de avaliação da segurança de acesso de aplicações web, tendo como foco a definição de um modelo de referência para segurança de acesso.

Por meio de um processo de análise hierárquica que engloba a estruturação do problema pôde ser obtido o modelo de referência e seu desdobramento, assim a medição de atributos intangíveis e a priorização desses atributos. Foi formalizada matematicamente a avaliação para obtenção de medidas que pudessem auxiliar os envolvidos na tomada de decisão sobre segurança de software.

Esta metodologia teve uma abordagem “*top down*”, pois partiu de uma visão macro para segurança de acesso e atingiu atributos que puderam ser medidos de forma objetiva.

Foi elaborado um *checklist* para auxiliar a obtenção das medidas, este *checklist* foi aplicado em forma de auditoria e respondido pela equipe responsável pela AWA.

Com os resultados obtidos no checklist e com o julgamento dos critérios acordado pela equipe responsável, eles são inseridos na ferramenta SuperDecision®, que embute os cálculos matemáticos para obter o vetor prioridade e verificar o atendimento ao modelo de referência. Este resultado apresenta de forma clara o estado sobre a segurança da aplicação web para os interessados (*stakeholders*). A instituição conhece o nível de segurança e as prioridades no seu contexto de negócio podem ser alinhadas.

Esta pesquisa contribui nas seguintes abordagens:

- Definição de Modelo de referência para segurança de aplicação web, que relaciona propriedades (intangíveis) em atributos mensuráveis, de uma forma organizada;
- Pontuação e priorização com método matemático;
- Abordagem sistemática de modelagem e medição de segurança;
- Auxílio nível gerencial da instituição;
- Metodologia com aplicações diversas – no Desenvolvimento, Avaliação e Seleção de AWA's;
- Expansão da metodologia para outras propriedades de segurança de software.

Este trabalho foi motivado pela dissertação de mestrado da autora que tinha como objetivo avaliar a qualidade de pacotes de software, foi modelado, medido e pontuado de modo empírico na pesquisa de mestrado. Nesta pesquisa de doutorado foi possível desenvolver matematicamente a medição de atributos intangíveis na área de segurança de software.

O processo utilizado para o cálculo do AHP mostrou-se muito coerente e apropriado, pois faz a estruturação do problema, e a partir disso auxilia o entendimento do modelo de segurança e dos critérios da Aplicação Web Alvo (AWA). Com o modelo definido é realizado o julgamento por especialistas definindo o nível de importância de cada critério por meio da escala de Saaty. O julgamento dos especialistas é computado matematicamente por meio das Matrizes de Decisão do método AHP e desse cálculo é gerado o vetor prioridade que possibilita a priorização dos critérios.

Inicialmente foi feita uma avaliação da segurança para o modelo de referência da Wang & Wulf e utilizando uma planilha Excell para cálculos – Fase 4/Ciclo3. Depois desse experimento foi escolhido o modelo de Autenticidade desenvolvido pela autora e aplicado ao sistema web SISTEMAWEB de acordo com a metodologia de pesquisa. Este modelo foi calculado na ferramenta de software SuperDecision®, desenvolvida para aplicação automática do AHP.

Os resultados obtidos são analisados primeiramente, pela ferramenta e em seguida pela equipe responsável. Na maioria das vezes é necessário verificar a Razão de consistência e se for o caso, rever o julgamento. No final é possível acordar as prioridades e assim obter os resultados de forma coerente.

Uma limitação encontrada na aplicação deste estudo, diz respeito à utilização do software Super Decisions® (CREATIVE DECISIONS FOUNDATION, 2012). Este software ainda se encontra na versão Beta, o que trouxe algumas dificuldades para utilização, pois o mesmo frequentemente apresenta erros de funcionamento, como por exemplo, para salvar os modelos utilizados.

Também houve dificuldade na formulação dos modelos, pois apesar de o método e o software terem uma lógica de utilização compreensível, na prática houve muitas dúvidas quando do estabelecimento dos *clusters* e das interações entre os elementos. Por vezes, as dúvidas foram sanadas por tentativa e erro, com base no estudo de tutoriais e de pesquisas publicadas.

A metodologia AHP apresenta uma limitação com respeito aos critérios a serem julgados. O número de critérios estão limitados à 7 + ou – 2 pois na comparação par a par mais que isso se torna inviável aos especialistas na hora do julgamento.

Considerando a importância das metodologias de apoio à decisão para as organizações, verifica-se a grande versatilidade e flexibilidade do AHP (*Analytic Hierarchy Process*). Mesmo devendo ser considerada algumas críticas quanto ao seu uso, a utilização do AHP pode representar um diferencial competitivo frente à concorrência, além de estimular a interação de várias pessoas, de diversas áreas, envolvidas na estratégia em questão, o que torna o modelo desenvolvido muito mais sólido e completo.

A aplicação deste método em engenharia de software de modo geral ainda é bem limitada tendo sido tratada na revisão bibliográfica. Apesar de ter sido citada em 1997 pelos pesquisadores Wang & Wulf somente agora em 2013 foi realizado o primeiro cálculo. Não foi encontrado na literatura nenhum autor trabalhando diretamente com AHP na área de medição para software e segurança.

O processo de Avaliação aqui apresentado como uma contribuição do trabalho se mostrou adequado e juntamente com a metodologia AHP pode ser útil para avaliar a segurança de aplicações WEB. Na fase especificação da Avaliação o processo diz para selecionar as medidas e definir os critérios de decisão. Com a metodologia do AHP foi possível transformar as propriedades intangíveis em atributos mensuráveis e adicionalmente a metodologia AHP mostra a

priorização dos atributos. Dessa forma a metodologia AHP veio completar a fase de especificação do processo de avaliação.

O trabalho contribui para eliminar a subjetividade das propriedades intangíveis, que precisam ser mensuradas para o nível gerencial ter uma visão global da segurança de suas aplicações. Os especialistas contribuem com suas experiências tácitas que precisam ser explicitadas de forma objetiva. Eles podem fazer isso com segurança de software, pois a metodologia do AHP tem seus recursos para verificar se existem incoerências nesses julgamentos.

Contudo, é importante frisar que, independente de se adotar um método formal ou informal, é de extrema importância ter certeza de que as partes interessadas forneçam os dados necessários e que os critérios estabelecidos estejam completos e não redundantes e, para isso, os participantes do processo decisório devem conhecer as necessidades da empresa, sua estratégia e objetivos dentro do contexto especificado.

É importante frisar também que, apesar dos autores que tratam da utilização do método o considerar de fácil aplicação, o AHP utiliza-se de conceitos matemáticos que não são utilizados no dia-a-dia das empresas em geral, por isso se faz necessário que seja desenvolvido conhecimento prévio do método antes de aplicá-lo, mesmo quando for utilizada alguma ferramenta de apoio à fase de desenvolvimento algébrico e numérico.

Com o intuito de contribuir para o tratamento da subjetividade e intangibilidade de atributos que necessitam ser medidos para um processo decisório, e com a observação de uma lacuna no processo de medição de segurança de aplicações web que são desenvolvidos sem a devida preocupação. Observou-se a oportunidade de aplicação de um Método Multicritério de Apoio à Decisão que possa auxiliar o complexo processo de medição e de tomada de decisão.

A Razão de Consistência evidencia a consistência sobre as notas de julgamento propostas pelo decisor, pois dependendo da nota proposta, o resultado indicará se os critérios estão consistentemente relacionados.

Neste trabalho foi aplicado para propriedade de segurança Autenticidade. Dentro do contexto da pesquisa de tese, observou-se que a metodologia desenvolvida para medição e priorização da propriedade Autenticidade, mostrou-se como uma prova de conceito para essa pesquisa. Para as demais

propriedades, Confidencialidade, Disponibilidade, e Integridade o processo se repete com as devidas particularidades. Se houver o intuito de ser desenvolvido um produto para avaliação comercial seria necessário completar a metodologia para as outras três propriedades.

A estimativa de tempo para aplicação da metodologia para propriedade Autenticidade foi de 14 horas, sendo 6 horas para o preenchimento do checklist, 3 horas para a auditoria, 3 horas para o julgamento dos critérios, e 2 horas para validação do relatório de medição do AWA. Estimativa essa calculada para os especialistas responderem o *cheklist* e para o julgamento das matrizes de decisão. Este tempo pode ser considerado relativamente pequeno para os resultados obtidos com a metodologia. Dessa forma consideramos uma maneira rápida para conhecer os níveis de segurança de uma aplicação Web. Esses dados ajudam os gestores à priorizar as ações necessárias para melhoria das aplicações.

Em relação à avaliação de segurança de aplicações web, este é um recurso desenvolvido tanto para empresas desenvolvedoras de softwares quanto para empresas que os utilizam em seus processos de negócio. As avaliações de segurança podem ser realizadas pela equipe especialista, visando identificar possíveis falhas de segurança tanto na visão de usuários, administradores ou agentes externos não autorizados. A verificação pode ser realizada em sistemas em fase de projeto, desenvolvimento ou já em funcionamento em seu ambiente. Ao final da avaliação de segurança é fornecido ao cliente relatório informando as falhas de segurança encontradas e sugestões para corrigi-las.

Esta metodologia pode englobar diferentes Modelos de referência, pois existem diferentes categorias de software.

8. REFERÊNCIAS BIBLIOGRÁFICAS

BARBATO L. G. C., Metodologia de Identificação de Vulnerabilidades em Aplicações de Pagamento utilizado Cartões de Crédito – Tese de doutorado INPE São José dos Campos, 2009.

BARNUM S., SETHI A., Attack Pattern Glossary - Copyright © Cigital, Inc.- <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/attack/590-BSI.html>, 2006

BARTOL N., BATES, B., GOERTZEL K. M., WINOGRAD, T. - Measuring – Cyber Security and Information Assurance, SOAR – State of the Art Report, Information Assurance Technology Analysis Center (IATAC), 2009.

BASTOS A L A. et al. Modelo Multicritério de Apoio à Decisão para Seleção de Fornecedores. VII Congresso Nacional de Excelência em Gestão, 2011.

BAYUK J., HOROWITZ B. M. An Architectural Systems Engineering Methodology for Addressing Cyber Security, This work was supported in part by the U.S. Department of Defense under contract H98230-08-D-0171, 2010

BAYUK J., Measuring System Security: An initial security theoretical construct framework, A dissertation of Doctor of philosophy, Stevens Institute of Technology, Hoboken, NJ 07030, 2011

BELLOVIN S. M., “On the brittleness of software and the infeasibility of security metrics,” IEEE Security & Privacy, p. 96, Jul./Aug. 2006

BELLOVIN S. M.,STOLFO S. “Measuring Security” Copublished by the IEEE Computer and Reliability Societies, On the Horizon,2011

BIBLE M. J. , BIVINS, S S. Mastering Project Portfolio Management: A Systems Approach to Achieving Strategic Objectives. J. Ross Publishing, 2011.

BLACK P E, SCARFONE K, SOUPPAYA M CYBER SECURITY METRICS AND MEASURES, in Handbook of Science and Technology for Homeland Security, Vol. 5, Edited by John G. Voeller, NIST, Gaithersburg, Maryland, 2008

BOEHM Barry, BASILI V. R., “Software Defect Reduction Top 10 List”, Software Management, Jan 2001, pp 135-137.

BOLDIN, L. & GASS, S. I., On Teaching the analytic hierarchy process, Computers & Operations Research 30, pp. 1487-1497, 2003

BSIMM Building Security In Maturity Model <http://www.bsi-mm.com/>

Acesso em Julho 2013

BRONSON R., Matrices, McGraw-Hill – New York 1989.

BUTLER S. A., Security Attribute Evaluation Method: A Cost-Benefit Approach, Proceedings of the 24th International Conference on Software Engineering, 2002, pp. 232-240.

CC - Common Criteria, 2001 <http://www.commoncriteriaportal.org/cc/>, acesso em junho de 2011.

CERT.BRa Estatísticas dos Incidentes Reportados - Valores acumulados: 1999 a junho de 2011, <http://www.cert.br/stats/> (accessed september 2011).

CHANDRA S., KHAN, R. A. – Software Security Matric Identification Framework (SSM) OCAC3'09, Mumbai, Maharashtra, India. Copyriht ACM 978-160558-351-8, 2009

CHAULA J. A., Yngström, L., Kowalski, S.- Security Metrics and Evaluation of Information Systems Security - Department of Computer and Systems Sciences, Stockholm University, 2004

CHEW E., SWANSON M., STINE K., BARTOL N., Brown A., Robinsonet W., Performance Measurement Guide for Information Security, NIST 800-55, 2008.

CONALLEN J., Building Web Applications with UML, Addison-Wesley Publishing Company, Reading, MA, 2000.

COSTA J F. S.; CORREIA, M G.; SOUZA, L T.T. Utilizando o Método de Análise Hierárquica na Escolha de Software Estatístico para a Demanda de uma Universidade Pública. Produto & Produção, vol. 12, n. 1, p. 42 - 59, 2011.

COUGHLAN P., COUGHLAN D. Action research for operations management. IJOPM International Journal of Operations & Production Management, v. 22, n. 2, p. 220-240, 2002. <http://dx.doi.org/10.1108/01443570210417515>

CVE - Common Vulnerabilities and Exposures
<http://www.cve.mitre.org/about/terminology.html>

Acesso em 30 agosto, 2010.

CVSS - Common Vulnerability Scoring System (v2), NIST, Peter Mell, Karen Scarfone, Sasha Romanosky, A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007

CWE Common Weakness Enumeration: cwe.mitre.org/ CWE is a list of software weaknesses. CWE-2000 - 2011 CWE/SANS Top 25, Acesso em 28/08/2013

CWSS <http://cwe.mitre.org/cwss/> Common Weakness Scoring System, acesso em 2013

DICTIONARY Dictionary of Scientific & Technical Terms, 6E, Copyright © by The McGraw-Hill Companies, Inc. - <http://encyclopedia2.thefreedictionary.com/Software+security>, 2003

DIONNE H, A Pesquisa Ação para o Desenvolvimento local. Trad. Michael Thiollent. Brasília: Liber, 2007, p. 26-27

DOWD M, McDONALD J, SCHUH J, Art of Software Security Assessment, The: Identifying and Preventing Software Vulnerabilities, by Addison-Wesley Professional. ISBN-10: 0-321-44442-6 ISBN-13: 978-0-321-44442-4, 2006

DUARTE L. O., Desenvolvimento de um ambiente para análise de códigos-fonte com ênfase em segurança. Dissertação de Mestrado, São José dos Campos: INPE, 2008.

EISENHARDT K., Building Theories from Case Study Research, Academy of Management Review, 1989, Vol 14, No 4, 533-550, 1989

ERNST&YOUNG Outpacing change - Ernst & Young's 12th annual global information security survey, 2009

FORZA C. Survey research in operations management: a process-based perspective. International Journal of Operations & Production Management, v. 22, n. 2, p. 152-194, 2002.

FOSSI et al. Symantec Global Internet Security Threat Report. Trends for 2010, Published April 2011.

GEER, D., Tutorial measuring security, 1.617.492.6814 / dan@geer.org v2.1:16x07 (2007) <http://all.net/Metricon/measuringsecurity.tutorial.pdf>

GLISSON W., BRADLEY g. Welland R. Web Engineering Security: Essential Elements In: The Second International Conference on Availability, Reliability and Security (ARES'07), 10-13 April 2007, Vienna, Austria.

GOERTZEL K.M. et al. - Software Security Assurance State-of-the-Art Report (SOAR) Information Assurance Technology Analysis Center (IATAC), Data and Analysis Center for Software (DACS), Joint endeavor by IATAC with DACS, DOI=10.1109/52.646883, 2007

GOERTZEL K, WINOGRAD T et al. for Department of Homeland Security and Defense Data and Analysis Center for Software. Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance, 2008.

GOMES C.G., SILVA A.C.S., CHAGAS M.F. Seleção de Projetos com Decisão Multocritérios - Uma Proposta de Modelo Para Seleção e Priorização de Projetos com a Aplicação do Método AHP e Utilização de Ratings Local Ano da publicação, XXVII Simpósio de Engenharia de Produção, 2010.

GOMES C.G. Proposta de um Modelo para Seleção e Priorização de Projetos com a Aplicação do Método AHP e Utilização de Ratings, dissertação de mestrado no ITA, 2011

GREENWALD M., C. A. GUNTER, B. KNUTSSON, A. Scedrov, J. Smith, S. Zdancewic, Computer security is not a science (but it should be), <http://www.cis.upenn.edu/bgreen/papers/Ins03-securityscience-whitepaper.pdf>, 2003

HINSON G. Seven myths about information security metrics, 2006 - disponível em www.isect.com

HO W Integrated analytic hierarchy process and its applications – A literature review, European Journal of Operational Research 186 211–228 available online at www.sciencedirect.com, 2008

HOUMB S.H. et al - Eliciting security requirements and tracing them to design: an integration of Common Criteria, heuristics, and UMLsec In Requirements Eng. 15:63-93 DOI 10.1007/s00766-009-0093-9, 2010.

IEEE Std 610 - IEEE Standard Glossary of Software Engineering Terminology, 1990

IMPERVA <http://www.imperva.com/index.html> último acesso em junho de 2013.

ISO/IEC 13335-1 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management, 2004

ISO/IEC 15408-1 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, International Standards Organization, Geneva, 2009.

ISO/IEC 15408-2 - Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements, Geneva, 2008.

ISO/IEC 15408-3 - Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components, Geneva, 2008.

ISO/IEC 15939 Systems and software engineering -- Measurement process. 2007.

ISO/IEC 21827 Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®) , 2002

ISO/IEC 25000 - Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE, 2005.

ISO/IEC 25010 - Software Engineering - Software product Quality Requirements and Evaluation (SQuaRE), 2011.

ISO/IEC FDIS 25020 - Software and system engineering . Software product Quality Requirements and Evaluation (SQuaRE) . Measurement reference model and guide, 2006.

ISO/IEC 25030 - Software Engineering – System and Software product Quality Requirements and Evaluation (SQuaRE), Quality Requirements, 2008.

ISO/IEC 25040 - Systems and software Engineering-Systems and Software Quality Requirements and Evaluation (SQuaRE)-Evaluation Process,Geneva, 2011.

ISO/IEC FDIS 27000 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, 2009.

ISO/IEC 27001 - Information technology - Information technology -- Security techniques – Information security management systems - Requirements, 2005.

ISO/IEC 27002 - Information technology - Code of practice for information security management, 2005.

ISO/IEC FDIS 27004 -- Information technology -- Security techniques -- Information security management – Measurement, 2009

ITSEC - Information Technology Security Evaluation Criteria (ITSEC) , EC advisory group, SOG-IS (Senior Officials Group - Information Systems Security), 1991

JANSEN, W., Directions in security metrics research, U.S. National Institute of Standards and Technology, NISTIR 7564, 21 p. ,2009.

JAQUITH A., “Security metrics: replacing fear, uncertainty and doubt”, Addison-Wesley, 2007.

JELEN G F.; JEFFREY R. W; A Practical Approach to Measuring Assurance, 1997.

LIPNER S, HOWARD M, “The Trustworthy Computing Security Development Lifecycle”, Microsoft Corporation, 2006.

McCALLAM D., The case against numerical measures of information assurance, in: Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, 2001.

McGRAW G, Software Security Building security in, Addison-Wesley, 2006.

McHUGH “Quantitative measures of assurance: prophecy, process or pipedream?”, Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, Virginia, May, 2001 (2002).

MEAD N. R., Security Quality Requirements Engineering (SQuaRE) Methodology, Technical Report, 2005.

MEDE-PROS® Centro de Tecnologia da Informação Renato Archer – CTI/MCT. Divisão de Qualificação em Software. MEDE-PROS® - Método de Avaliação da Qualidade de Produto de Software. Versão 2006.

MEIER J.D., MACKMAN A., VASIREDDY S, DUNNER M., ESCAMILLA R., MURUKAN A., – Improving Web Application Security Threats and Countermeasures – MicroSoft, 2003.

METHA, D M. “Application Security Testing Cheat Sheet”. SmartSecurity.blogspot.com,. 30 08 13 at:
<http://www.edocr.com/doc/264/application-security-testing-cheat-sheet>

MILLER, G A. - The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information - The Psychological Review, vol. 63, pp. 81-97, 1956.

MKS - An Innovative Approach to managing Software Requirement, http://projectmanagement/a.knowledgestorm.com/shared/write/collateral/WTP/49705_52374_26971_MKS.pdf?ksi=1290251&ksc=1298777634 (downloadable, March, 2007)

MORITA H. - “Metodologias para estruturação e avaliação da decisão nas organizações: uma pesquisa”, In: SHIMIZU, T., Decisão nas Organizações: introdução aos problemas de decisão encontrados nas organizações e nos sistemas de apoio à decisão, São Paulo: Atlas, p.286-293,(2001).

NAKANO D. N.; FLEURY, A C. C. - Métodos de pesquisa na Engenharia de produção. In:Enegep, 1998.

NASCIMENTO, L. P. - Aplicação do método AHP com as abordagens ratings e BOCR: o projeto F-X2. 150 f. Dissertação (Mestre em Ciências) - Instituto Tecnológico de Aeronáutica, São José dos Campos,2010.

NBR ISO/IEC 14598-5 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - Tecnologia de Informação – Avaliação de produto de Software – Parte 5: Processo para avaliadores, Rio de Janeiro ABNT, 2002.

NBR ISO/IEC 12119. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 12119: Tecnologia de informação -Pacotes de software - Testes e requisitos de qualidade. Rio de Janeiro: ABNT, outubro 1998. 13 pp. (versão cancelada pela NBR ISO/IEC 25051, 2009).

NBR ISO/IEC 12207 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Tecnologia de Informação – Processos de ciclo de vida de software; Rio de Janeiro ABNT 35 pp. out/1998.

NBR ISO/IEC 25051. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS Engenharia de software – Requisitos e avaliação da qualidade de produto de software (SQuaRE), Rio de Janeiro ABNT, 2008.

NBR ISO/IEC 9126-1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS
Engenharia de software - Qualidade de produto - Parte 1: Modelo de qualidade,
2002

NICHOLS E.A. and PETERSON, G. - A Metrics Framework to Drive Application
Security Improvement, IEEE Security & Privacy, 5(2) March-April 2007, 88-91.
DOI=10.1109/MSP.26, 2007.

OLLMANN, Gunter. "Application Assessment Questioning". acessado 30 08 13
at: <http://www.technicalinfo.net/papers/AssessmentQuestions.html>

OWASP Open Web Application Security Project <http://www.owasp.org/> acesso
em 2013

OWASP-ASVS - Open Web Application Security Project – Application Security
Verification Standard 2009 <http://www.owasp.org/>

OWASP-TOPTEN –The ten most critical web application security risks, 2010
<http://www.owasp.org>

OWASP-SAMM - Open Web Application Security Project – Security Assurance
maturity Model V.1.0, acessado em Julho 2013 em
[https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Mod
el](https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model)

PAYNE S C. - A Guide to Security Metrics, SANS Institute InfoSec Reading
Room, 2006.

PCI-DSS, https://www.pcisecuritystandards.org/security_standards/ 2010

PERRIN, R. Real World Project Management: Beyond Conventional Wisdom,
Best Practices and Project Methodologies. John Wiley & Sons, 2008.

PFLEEGER S. L. , CUNNINGHAM, R. K. , Why Measuring Security Is Hard,
IEEE SECURITY & PRIVACY , JULY/AUGUST 2010

PERRON O., Zur Theorie der Matrices, Math. Ann. 64, 248 – 264, 1907.

PINHEIRO J. M. S. Prova de Conceito (PoC) no Projeto de Redes de
Computadores, 2010. Aceso em abril de 2012

PNAFM - Programa Nacional de Apoio à Gestão Administrativa e Fiscal dos Municípios – 2001. <http://www.ucp.fazenda.gov.br/PNAFM>

PONEMON Institute, State of Web Application Security, by Imperva & WhiteHat Security, 2010.

ROCHA A. R. C.; MALDONADO, J.C.; WEBER, K.C. Qualidade de Software – Teoria e Prática. 1. ed. São Paulo: Prentice Hall, 303 pp, 2001.

SAATY T. L. - The Analytic Hierarchy Process: McGraw-Hill, N. York, USA, 1980.

SAATY T. L. - Decision making with the analytic hierarchy processo n Intenational Journal Services Sciences, vol 1,n.1, 2008.

SAVOLA R M. - Towards a Taxonomy for Information Security Metrics, International Conference on Software Engineering Advances (ICSEA 2007), Cap Esterel, France, August 2007.

SAVOLA R. and ABIE H. - Development of Measurable Security for a Distributed Messaging System, International Journal on Advance Security, vol 2 n.4, <http://www.ariajournals.org/security/>, 2009a.

SAVOLA R. and ABIE H. - Identification of basic Measurable Security Components for a Distributed Messaging System - Third International Conference on Emerging Security Information, Systems and Technologies, 2009b.

SCHNEIER B Segredos e mentiras sobre a proteção na vida digital Editora Campus 2001

SD, SuperDecision® - <http://www.superdecisions.com/>. 2010.

SSE-CMM, System Security Engineering – Capability Maturity Model, 2003 – www.sse-cmm.org, acesso em novembro de 2011.

THIOLLENT M. - Metodologia da pesquisa-ação. 15. ed. São Paulo: Cortez, 2007.

TRIPP D., Pesquisa-Ação: uma introdução metodológica. Tradução publicada por Lólio Lourenço de Oliveira. Educação e Pesquisa São Paulo, v.31,n.3p.443-466 set/dez 2005.

VERENDEL V. - Quantified Security is a Weak Hypothesis, 2009 NSPW'09, September 8–11, 2009, Oxford, United Kingdom ACM 978-1-60558-845-2/09/09.

VERGARA Sylvia Constant. - Projetos e relatórios de Pesquisa em Administração. São Paulo: Atlas, , p. 49, 2007.

VILLALBA M. T., SANZ, L. F., GALLEG0 J. J. C., MARTINEZ J. J. Software Quality Evaluation for Security COTS Products - International Journal of Software Engineering and knowledge Engineering (IJSEKE) - Vol. 20, Issue: 1pp. 27-48 DOI: 10.1142/S0218194010004633, 2010.

VOSS C., Tsikriktsis, N., Frohlich, M. - Case research in operations management. In: International Journal of Operations & Production Management, v. 22, n. 2, pp. 195-219, 2002.

WANG C; WULF W. A. - Towards a framework for security measurement, 20th National Information Systems Security Conference, Baltimore, MD, pp. 522-533, 1997.

WEBAPPSEC <http://www.webappsec.org/> acesso em 2013

WESTBROOK R. - Action research: a new paradigm for research in production and operations management. IJOPM International Journal of Operations & Production Management, v. 15, n. 12, p. 6-20, <http://dx.doi.org/10.1108/01443579510104466>, 1995.

WHITEHEAD <http://wi.mit.edu/> ultimo acesso em junho de 2013.

YIN R. K. - Estudo de Caso – Planejamento e Métodos. Tradução de Daniel Grassi, Brasil: Bookman Companhia Editora, 212 p., 2005.

9. REFERÊNCIAS DO AUTOR

COLOMBO, R. M. T.; GUERRA, A. C. - The Evaluation Method for Software Products. In: ICSSEA 2002 15th International Conference Software & Systems Engineering and their Applications – Paris, France

COLOMBO R. M. T. - Processo de Avaliação da Qualidade de Pacotes de Software. 2004. Dissertação (Mestrado em Engenharia Mecânica) - Universidade Estadual de Campinas.

COLOMBO, R. M. T., GUERRA, A. C., 2009. Tecnologia da Informação: Qualidade de Produto de Software, MCT/SEPIN, Brasília, 2009, 429pp.

COLOMBO, R. M. T., GUERRA, A. C., PESSÔA, M. S., DUARTE, L. O. - 2010 - Avaliação da Qualidade de produtos de Software com enfoque na segurança da Informação - Conferência IADIS Ibero-Americana-Consórcio Doutoral, pag 525.

COLOMBO, R. M. T. et al – Security Evaluation Process of Web Software Applications. In: ICSSEA 2011 23th International Conference Software & Systems Engineering and their Applications – Paris, France

COLOMBO, R. M. T. et al – Prioritization of Software Security Intangible Attributes - ACM SIGSOFT Software Engineering Notes, November 2012 Volume 37 Number 6, <http://doi.acm.org/10.1145/2382756.2382781>

COLOMBO, R. M. T., Guerra, A. C., Pessôa, M. S. P. Models for measuring security Access Web application – ASE/IEEE International Conference on Big Data, aceito mas não publicado em 2013.

COLOMBO, R. M. T., GUERRA, A. C., PESSÔA, M. S. P. – Proposal for measuring Access Security of Web application – submetido em 2013 <http://world-comp.org/elsevier-morgan-kaufman-ICT/>

COLOMBO, R. M. T., GUERRA, A. C., PESSÔA, M. S. P. – Priorization of Software Security Intangible Attributes - Journal Computers & Security – submetido em 2013.

10. APÊNDICES

10.1 APÊNDICE 1 – RELATÓRIO SISTEMAWEB – AVALIAÇÃO EXPLORATÓRIA

Relatório de Pré-Avaliação do Produto de Software

SISTEMAWEB Versão 06/05/2012

Responsável pelo Produto: CTI-DSSD

Campinas, 05 de Setembro de 2012

RELATÓRIO DE AVALIAÇÃO DO PRODUTO <SISTEMAWEB>

1. ESCOPO

Este documento apresenta o resultado da avaliação genérica do produto <SISTEMAWEB>

O SISTEMAWEB é o ambiente computacional que permite a interação dos membros de uma equipe dedicada à produção de um determinado resultado, através do qual podem registrar e trocar informações e também ter acesso a ferramentas computacionais. Os ambientes de trabalho são criados e configurados para cada tipo de resultado produzido pela instituição.

As ferramentas no SISTEMAWEB são agrupadas de acordo com sua natureza e podem ser utilizadas em um ou vários ambientes de trabalho, desde que estejam habilitadas para o tipo de resultado do referido ambiente. Basicamente as ferramentas são classificadas como:

- Consulta
- Gestão
- Registro
- Técnica

O acesso às ferramentas pode ser público, no caso das ferramentas de uso geral, ou restrito, no caso de ferramentas associadas ao tipo de resultado.

2. INTRODUÇÃO

A avaliação genérica do software teve como objetivo inicial observar o comportamento do sistema em relação às características de segurança de uma típica aplicação web.

Através da verificação inicial de segurança foi possível selecionar alguns itens essenciais à identificação do nível de segurança do software

O ambiente de teste e avaliação ocorreu em duas situações:

1 - Um ambiente de teste foi disponibilizado pelos responsáveis pelo produto com as informações necessárias para o acesso.

2 – Outro ambiente de teste e avaliação foi o próprio ambiente de produção em uso na Empresa.

3. O PROCESSO DE AVALIAÇÃO

O processo de avaliação abordou as seguintes etapas:

a- Estabelecer os Requisitos de Segurança

Nesta etapa foi considerada como propósito da avaliação a verificação do comportamento do sistema em relação às intervenções básicas à uma aplicação web. Foi identificado o ambiente de teste.

b- Especificar a Avaliação

Nesta etapa foram definidos alguns casos de teste para explorar possíveis vulnerabilidades conhecidas para este tipo de aplicação de software.

c- Projetar a Avaliação

Nesta etapa é definido o plano de avaliação, com a identificação dos instrumentos a serem utilizados – o ambiente de hardware e software, o sistema alvo de avaliação, os casos de teste e possivelmente alguma documentação de acesso disponível.

d- Executar a Avaliação

Nesta etapa foram efetuadas as verificações planejadas, a coleta dos dados e das informações obtidas durante a avaliação e realizado o procedimento de análise dos resultados obtidos.

e- Concluir a Avaliação

Nesta etapa foi preparado o resultado da avaliação, com conseqüente geração do relatório de avaliação contendo as evidências dos resultados obtidos.

4. ITENS DE AVALIAÇÃO

A seguir é apresentado o resultado da avaliação, destacando os aspectos a serem revistos nos pontos que foram avaliados. Foram identificados nesta fase sete aspectos de segurança de aplicação web.

A. O SISTEMA NÃO EXIGE O USO DO PROTOCOLO HTTPS

Aspectos a serem revistos

Problema: O sistema não exige o uso de HTTPS.

Explicação: Se você estiver em qualquer pagina consegue alterar a requisição de HTTPS para HTTP e poderá depois navegar em qualquer parte do sistema

Sugestão: configuração do servidor ou da aplicação para suportar somente conexões HTTPS

Telas:

B. CONFIGURAÇÃO DO SERVIDOR WEB

Problema: Servidor mal configurado permite a listagem de diretórios

Explicação: Com essa informação se consegue mapear a aplicação e tentar outros tipos de acesso como, ignorar a autenticação. (http://SISTEMAWEB.xxx.xxx /SISTEMAWEB/login/

C. VALIDAÇÃO DE AUTENTICAÇÃO DE USUÁRIO

Problema: Não validação (aparente) de autenticação

Explicação: Baseado no erro anterior, consegue mapear a aplicação completamente e acessar partes da aplicação que não deveriam ser permitidas .

The screenshot shows a web browser window with a menu bar (File, Edit, View, History, Bookmarks, Tools, Help) and a search bar. The address bar shows 'http://'. The browser tabs include 'Sistema de...', 'Directory L...', 'Alteração ...', 'Sistema de...', 'http://...oltar', 'Directory L...', 'http://...o.jsp', and 'Siste...'. The main content area displays a form titled 'Dados Gerais' with a sub-header 'Proposta: 0018.10'. The form contains several input fields and dropdown menus. A red banner at the top right of the form area contains the text 'Salvar | Cancelar | Imprimir'. The form fields include 'H0 AA/00000', 'Gestor:', 'Situação:' (set to 'Proposto'), 'Objeto:', 'Tipo do resultado:' (set to 'Não Consta Na Lista'), 'Novo tipo:', 'Início previsto:', 'Término previsto:', 'Início de execução:', 'Término de execução:', 'Contrato ou convênio associado:', 'TA:', 'Cliente (se houver):', and 'Receita:'. There is also a section for 'Especificação do objeto:' with a large text area below it.

The screenshot shows a web browser window with a menu bar (File, Edit, View, History, Bookmarks, Tools, Help) and a search bar. The address bar shows 'http://'. The browser tabs include 'Sistema de...', 'Directory L...', 'Alteração...', 'Sistema de...', 'http://...oltar', 'Directory L...', 'http://...o.jsp', and 'Siste...'. The main content area displays a form titled 'Alteração de senha'. The form contains three input fields: 'Senha atual', 'Nova senha', and 'Confirmar nova senha'. At the bottom of the form, there are two buttons: 'Salvar' and 'Fechar'.

The screenshot shows a web browser window with the title 'Dados Gerais - H'. The form includes the following fields:

- Gestor:** A dropdown menu with an asterisk.
- Situação:** A text input field.
- Objeto:** A text input field with an asterisk.
- Tipo do resultado:** A text input field with an asterisk.
- Novo tipo:** A text input field.
- Início previsto:** A text input field with an asterisk.
- Término previsto:** A text input field with an asterisk.
- Início previsto do projeto:** A text input field.
- Início Efetivo:** A text input field.
- Término Efetivo:** A text input field.
- Término previsto do projeto:** A text input field.
- Contrato/convenção:** A dropdown menu.
- TA:** A dropdown menu.
- Cliente:** A dropdown menu.
- Receita:** A text input field.
- Especificação do objeto:** A large text area.

•

D. VAZAMENTO DE INFORMAÇÕES

•

Problema: Vazamento de informações (informações desnecessárias aparecendo)

Explicação: O servidor não configurado corretamente mostra dados sobre o servidor e a versão dos produtos instalados. Essa informação é útil para um agente procurar (ou monitorar) as falhas desses softwares e tentar invadí-los.

Server: Apache-Coyote/1.1

X-Powered-By: Servlet 2.4; JBoss-4.0.4.GA (build: CVSTag=JBoss_4_0_4_GA date=200605151000)/Tomcat-5.5

E. IDENTIFICAÇÃO DE VARIÁVEIS DO SISTEMA

Problema: Variáveis com nomes óbvios

Explicação: Variáveis com nomes muito óbvios podem facilitar um ataque

Exemplo: Set-Cookie: ULTIMO_ACESSO=1313002534969; Path=/

F. ACESSO À ARQUIVOS DO SISTEMA

Problema: Proteção incorreta de arquivos e diretórios do sistema

Explicação: Acessando diretamente alguns arquivos pode causar a listagem dos mesmos sem a devida “compilação”

G. GERÊNCIA DE EXCEÇÕES

Problema: Gerenciamento de exceções

Explicação: O gerenciamento incorreto de erros leva a divulgação de informações.

5. OBSERVAÇÕES

Comentários sobre os requisitos não-funcionais(RNF) de segurança apresentados no edital.

Aspectos a serem revistos

- RNF 28 - não foi testado.
- RNF 29 - a recomendação aqui está na garantia de que somente o servidor de aplicação fale com o servidor de banco de dados, porém é possível que baseado nas situações encontradas na aplicação, tenha realmente falhas.

Esse requisito pode estar OK, se olharmos para a camada de rede, porém com a aplicação vulnerável, conseguiríamos ignorar todo o controle de acesso.

- RNF 30 – Foi possível acessar funções do software sem passar pelo processo de autenticação de usuário.
- RNF 31 - O ideal seria que os usuários fossem autenticados via certificado digital, porém não existem indícios visíveis de que isso aconteça ou possa acontecer.
- RNF 32 - somente conseguiremos validar com acesso direto ao banco de dados.
- RNF 33 - somente conseguiremos validar com acesso direto ao servidor da aplicação, ou servidor de *logs* caso exista.
- RNF 34 – não foi testado.
- RNF 35 - não foi testado.
- RNF 36 - não foi testado.
- RNF 37 - não foi testado.
- RNF 38 - não foi testado.
- RNF 39 - somente conseguiremos validar com acesso direto ao servidor da aplicação.
- RNF 40 – Não atendido. No item 4.4 há uma tela mostrando este problema.
- RNF 41 – Possivelmente não atendido baseado nos erros e situações apresentados no item 4, porém não foi coletado evidência.
- RNF 42 - não foi testado.
- RNF 43 - não foi testado.
- RNF 44 - não foi testado.
- RNF 45 - Possivelmente não atendido baseado nos erros e situações apresentados no item 4.7.
- RNF 46 - não foi testado.
- RNF 47 – Este requisito está muito genérico, detalhar “desativação de segurança”. Possivelmente permitiu o problema relatado no item 4.1, 4.6.
- RNF 48 - somente conseguiremos validar com acesso direto a aplicação e acesso ao servidor de banco de dados.
- RNF 49 - Não atendido. No item 4 há uma tela mostrando erros.

6. CONCLUSÕES

O presente relatório apresenta uma prévia da avaliação, não detalhada do SISTEMAWEB. Não foram executados, testes intrusivos visando localizar falhas de injeção (SQL, XSS, Comandos, etc), que poderiam demonstrar mais vulnerabilidades do que as apresentadas nesse documento. Os testes

propostos poderiam mostrar as reais falhas do sistema em situações de uso prático, expostos na internet pública.

Para que o processo de avaliação da segurança do software ocorra em maior detalhe será necessária outra configuração do servidor com os parâmetros de proteção recomendados pelo fabricante do software utilizado para segurança do servidor. Mesmo assim parâmetros adicionais devem ser avaliados ou balizados com as necessidades do sistema.

Não foi possível relacionar alguns problemas encontrados e relatados com os requisitos não-funcionais, por exemplo, 4.2, 4.5.

Alguns requisitos não-funcionais do Edital estão muito genéricos, dificultando a validação dos itens.

O próximo passo sugerido é uma reunião com os responsáveis pelo SISTEMAWEB na Empresa para maiores esclarecimentos sobre o sistema e os resultados obtidos relatados neste relatório e uma estimativa de recursos necessários para possíveis correções relatadas.

Perguntas à equipe responsável pelo SISTEMAWEB

Em relação aos problemas encontrados e relatados neste documento, favor preencher a tabela com estes tópicos:

- Vulnerabilidade nova ou já conhecida?
- Gravidade (Pequena, Média, Alta)
- Fonte/Causa do problema (Rede, Servidor, Aplicação, Arquitetura, ...)
- Tem outros desdobramentos de correções no sistema?
- Responsável/Função por corrigir
- Prazo para corrigir
- Que problemas podem gerar ao usuário do sistema?
- Que ações podem gerar à equipe de desenvolvimento?
- Que ações podem gerar aos responsáveis pelo sistema?
- No Edital tinha algum requisito para evitar este problema?

Em relação aos problemas encontrados e relatados neste documento, favor preencher a seguinte tabela:

Problema/ Tópico				
4.1				
4.2				
4.3				
4.4				
4.5				
4.6				
4.7				

10.2 APÊNDICE 2 – RELATÓRIO SISTEMAWEB – AVALIAÇÃO FORMAL

Relatório de Auditoria da Segurança de acesso do SISTEMAWEB

Responsável pelo Produto:
CTI-Grupo SISTEMAWEB

Campinas, 05 de Setembro de 2013

RELATÓRIO DE AUDITORIA

<SISTEMAWEB>

1. ESCOPO

Este documento apresenta o resultado da auditoria do <SISTEMAWEB>

O *SISTEMAWEB* é o ambiente computacional que permite a interação dos membros de uma equipe dedicada à produção de um determinado resultado, através do qual podem registrar e trocar informações e também ter acesso a ferramentas computacionais. Os ambientes de trabalho são criados e configurados para cada tipo de resultado produzido pela instituição.

As ferramentas no *SISTEMAWEB* são agrupadas de acordo com sua natureza e podem ser utilizadas em um ou vários ambientes de trabalho, desde que estejam habilitadas para o tipo de resultado do referido ambiente. Basicamente as ferramentas são classificadas como:

- Consulta
- Gestão
- Registro
- Técnica

O acesso às ferramentas pode ser público, no caso das ferramentas de uso geral, ou restrito, no caso de ferramentas associadas ao tipo de resultado.

2. INTRODUÇÃO

A auditoria do software teve como objetivo medir a Autenticidade de segurança de acesso do sistema *SISTEMAWEB*.

3. O PROCESSO DE AUDITORIA

O processo de auditoria abordou as seguintes etapas:

a- Estabelecer os Requisitos de Segurança

Nesta etapa foi considerada como propósito da auditoria a verificação da propriedade Autenticidade em relação ao modelo de referência da Figura 1.

A Figura 2 mostra o mesmo modelo com mais níveis de desdobramento e configurado na ferramenta de software SuperDecision®.

Figura 1 – Modelo de Referência para Autenticidade

Figura 2 – Modelo de autenticidade no SuperDecision®

b- Especificar a Auditoria

Nesta etapa foi definido o *checklist* para medir a propriedade Autenticidade para este tipo de aplicação de software. O *checklist* é composto pelos atributos mensuráveis contidos na Tabela 1, na coluna Nível 5.

Tabela 1 - Cinco níveis da propriedade de Autenticidade

NÍVEL 1	NÍVEL 2	NÍVEL 3	NÍVEL 4	NÍVEL 5
AUTENTICIDADE	AUTENTICAÇÃO	MECANISMO	CARACTERÍSTICAS BÁSICAS	Revela Informações
				No Host Servidor
				Identifica Informações do Cache
				Múltiplos Usuários
				Perda de Credenciais
				Múltiplas Camadas
				URL's Privilegiadas
				Auto-Complete OFF
			REAUTENTICAÇÃO	Reautenticação Exigida
				Reautenticação Navegador
			MENSAGENS	Mensagens de Erro
				Mensagens Não-informativas
			TIMEOUT	Timeout por Inatividade
				Timeout Adequado
				Timeout Cancela Seção
				Cancela Sessões Simultâneas
			CRIPTOGRAFIA	Criptografia de Dados Sensíveis
				Acesso Seletivo
				Serviços (Dados) Externos
				Senha Não-criptografada
				Criptografia na Rede
			LOGOUT	Logout Usuário
				Cancela Todas as Sessões
				Refresh preserva Logout
			BLOQUEIO	Bloqueio de Usuário
				Máximo de Tentativas
				Detem Força-bruta
				Bloqueio de Host (IP)
				Desabilita Usuário
			CARACTERÍSTICAS ADICIONAIS	Login Resiste a SQL Injection
				Senhas Temperadas
				Páginas de Senhas em HTTPS
				Páginas (Dados) Sensíveis em SSL
		IDENTIDADE	CARACTERÍSTICAS BÁSICAS	Política para ID
				ID no Host-cliente
				ID no Host-servidor
				Força-bruta na Autenticação possível
				Adivinhação de Credenciais possível
			ID/SENHA	Política (Regras) para Senhas Fortes
				Senha Anterior em Mudanças
				Reutiliza Senhas Anteriores
				Muda Senha no 1o Login
				Recurso para Recuperar Senha
				Recurso CAPTCHA
				Usuário Muda Detalhes (Senha)
				Senha apresentada em Plain Text

c- Projetar a Auditoria

Nesta etapa é definido o plano de auditoria, com a identificação dos instrumentos a serem utilizados – o ambiente de hardware e software, o sistema alvo de auditoria, o *checklist*, a equipe responsável e possivelmente alguma documentação de acesso disponível. A Tabela 1 mostra os atributos mensuráveis do Nível 5. Estes atributos compõem o checklist.

d- Executar a Auditoria

Nesta etapa foram efetuadas as verificações planejadas, a coleta dos dados e das informações obtidas durante a auditoria e realizado o procedimento de análise dos resultados obtidos.

O *Checklist* AUTENTICIDADE foi respondido pela equipe responsável e depois foi realizado o julgamento dos critérios par a par, utilizando a escala de Saaty.

A Tabela 2 os atributos de Mecanismo, isto é, os critérios que são pontuados com a escala de Saaty, por meio do julgamento. Ela é utilizada pela equipe para fazer a comparação par a par entre os critérios. Esta fase é bastante debatida, mas é necessário que haja um consenso final pela equipe.

Tabela 2 – Tabela de auxílio aos critérios

CRITÉRIO	ESCALA DE SAATY	CRITÉRIO
CARAC GERAL- Cg	7	REAUTENTICAÇÃO
	5	MENSAGENS
	1	TIMEOUT
	1	CRIPTOGRAFIA
	5	LOGOUT
	5	BLOQUEIO
	1	CARAC.ADICIONAL - Ad
REAUTENTICAÇÃO-Re	3	MENSAGENS
	3	TIMEOUT
	3	CRIPTOGRAFIA
	3	LOGOUT
	3	BLOQUEIO
	3	CARAC.ADICIONAL
MENSAGENS-Me	3	TIMEOUT
	3	CRIPTOGRAFIA
	3	LOGOUT
	3	BLOQUEIO

CRITÉRIO	ESCALA DE SAATY	CRITÉRIO
	3	CARAC.ADICIONAL
TIMEOUT-Ti	1	CRIPTOGRAFIA
	5	LOGOUT
	1	BLOQUEIO
	3	CARAC.ADICIONAL
	5	LOGOUT
CRIPTOGRAFIA-Cri	5	BLOQUEIO
	1	CARAC.ADICIONAL
	5	BLOQUEIO
LOGOUT-Lo	5	BLOQUEIO
	1	CARAC.ADICIONAL
BLOQUEIO-BI	3	CARAC.ADICIONAL

Após a realização do julgamento, os dados são inseridos na ferramenta SuperDecision® para serem feitos os cálculos das Prioridades. A Tabela 3 mostra a matriz de decisão para os julgamentos realizados.

Tabela 3 - Matriz de Decisão do SISTEMAWEB

	Cg	Re	Me	Ti	Cri	Lo	BI	Ad
Cg	1	7	5	1	1	5	1	1
Re	1/7	1	3	3	3	3	3	3
Me	1/5	1/3	1	3	3	3	3	3
Ti	1	1/3	1/3	1	1	5	1	3
Cri	1	1/3	1/3	1	1	5	5	3
Lo	1/5	1/3	1/3	1/5	1/5	1	5	1
BI	1	1/3	1/3	1	1/5	1/5	1	5
Ad	1	1/3	1/3	1/3	1/3	1	1	1

e- Concluir a Auditoria

Nesta etapa foi preparado o resultado da auditoria com o auxílio da ferramenta SuperDecision®, que realiza os cálculos e nos fornece os resultados obtidos. A Tabela 4 mostra a pontuação para cada componente e atributo de segurança.

Tabela 4 - Resultado da Autenticação no AHP para o SISTEMAWEB

Nível 1	Nível 2	Nível 3
Autenticação 0,87	Mecanismo 0,83	Características básicas 0,16
		Reautenticação 0,06
		Apresentação de mensagens 0,02
		Tempo-limite 0,03
		Criptografia 0,40
		Logout 0,18
	Identidade 0,16	Bloqueio 0,10
		Características adicionais 0,83
		Login/Password 0,16

4. ITENS DE AUDITORIA

A seguir é apresentado o resultado da auditoria, destacando os aspectos a serem revistos nos pontos que foram avaliados. Foram identificados nesta fase os seguintes aspectos de segurança de acesso – Autenticidade de aplicação web.

No primeiro nível vê-se que a pontuação para Autenticidade foi de 0,87, isto significa que ela atendeu 87 % dos atributos de segurança de Autenticidade.

No segundo nível vê-se que entre Mecanismo e Identidade, Mecanismo tem a prioridade de 83 % perante a Identidade com 16 % perante a Autenticidade. No nível 3 vê-se que o atributo Criptografia é 40 % mais importante que os demais atributos de Mecanismo.

Com este resultado, é possível ver o que o SISTEMAWEB atende e não atende ao Modelo de referência e adicionalmente quais as prioridades entre os critérios, dessa forma, a equipe responsável tem um indicador de onde é prioritário ações para correção e melhoria da Autenticidade do SISTEMAWEB.

5. CONCLUSÕES

O próximo passo sugerido é uma reunião com os responsáveis pelo SISTEMAWEB para maiores esclarecimentos sobre o sistema e os resultados obtidos relatados neste relatório e uma estimativa de recursos necessários para possíveis ações a serem tomadas.

10.3 APÊNDICE 3 – CHECKLIST DE AUTENTICIDADE

MED-SEC-AWA 2013

Lista de Verificação

Aluna - Regina M. T. Colombo

Orientador - Marcelo S. P. Pêsoa

FICHA CADASTRAL DA APLICAÇÃO WEB ALVO - AWA

Informações da AWA

Nome:
Versão:
Descrição da Aplicação:
Empresa desenvolvedora:
Contato com responsável (nome, e-mail, fone):

Requisitos de Hardware e Software da AWA

Ambiente de desenvolvimento
Recursos de software (linguagem, sistema operacional, banco de dados):
Arquitetura do software:
Rede/Protocolo:
Ambiente de produção
Plataforma de software:
Faz uso de arquivos de Log? Quais? Outros?
Plataforma de hardware:
Hardware adicional (impressora, <i>scanner</i> , <i>hardlock</i>):

Software adicional:
Observações:

Informações adicionais da AWA

Quais os perfis de usuário?
Número máximo esperado de usuários concomitantes?

AVALIAÇÃO DE AUTENTICIDADE - SEGURANÇA

1. AUTENTICAÇÃO

1.1 MECANISMO DE AUTENTICAÇÃO

A Identidade/Mecanismo de Autenticação pode ser de três categorias:

Autenticação baseada no conhecimento (o que se sabe): o modo mais usado de identificação - senhas, informações pessoais ou qualquer informação não necessariamente secreta, mas que seja considerada desconhecida por outros.

Autenticação baseada na propriedade (o que se tem): caracterizada por um objeto físico que o usuário possui - Smartcard ou Token.

Autenticação baseada na característica (o que é): os métodos de autenticação baseados neste fator são chamados biométricos - sistemas biométricos realizam a verificação ou o reconhecimento de uma pessoa com base em alguma característica física, como impressão digital, íris, voz ou padrão de comportamento característico de uma pessoa.

1.1.1 Mecanismo de Autenticação - Características Gerais

1.1.1.1 A aplicação suporta Autenticação de usuário-cliente? (O/1)

(____) SIM (____) NÃO

Em caso afirmativo (caso haja Autenticação):

1.1.1.2 Como é o Mecanismo de Autenticação, para o usuário e na implementação, regras de ID/senha, ...? (R)

Dentro das categorias de mecanismos de autenticação/identificação, qual (is) é (são) utilizada (s) na aplicação?

Descrever:

1.1.1.3 Como é o processo de fornecimento das credenciais de acesso a aplicação para os novos usuário-cliente? (O/30)

1.1.1.4 Quantas e quais credenciais são exigidas pelo mecanismo para a realização da Autenticação (ID de Usuário e Senha, impressão digital de apenas um dedo ou dos dois dedos, outros....)? (O/6)

Descrever:

1.1.1.5 A aplicação exige Autenticação nos recursos (tarefas) de acesso restrito, exceto o que for destinado especificamente a ser público? (W/1)

(____) SIM (____) NÃO

Descrever:

1.1.1.6 A Autenticação e os seus controles (verificações) são realizados/executados no host-servidor? (O/4) (W/4)

(____) SIM (____) NÃO

Descrever:

1.1.1.7 É possível identificar informações sobre o usuário anterior do host-cliente, a partir de alguma informação do cache ou de outro lugar? (O/14)

(____) SIM (____) NÃO

(OBS: verificar o *cache* do navegador)

1.1.1.8 A Autenticação do usuário-cliente é compartilhada (um usuário pode estar conectado em apenas um único host-cliente, ou em diferentes hosts-cliente ao mesmo tempo)? (O/2)

(____) SIM (____) NÃO

Descrever:

1.1.1.9 Podem múltiplos usuários-clientes serem autenticados e acessar a aplicação ao mesmo tempo? (O/20)

(____) SIM (____) NÃO

Até quanto a aplicação exige e suporta acessos concomitantes (usuários distintos)?

Descrever:

1.1.1.10 A aplicação responde de forma apropriada à perda de credenciais de Autenticação? Há mecanismo de recuperação de credencial, senha, etc.? (O/11)

(____) SIM (____) NÃO

Em caso afirmativo, descrever como recupera a nova senha:

1.1.1.11 O processo de Autenticação foi implementado em múltiplas camadas? (O/8)

(____) SIM (____) NÃO

Em caso afirmativo, descrever como:

1.1.1.12 A Autenticação pode ser contornada pelo uso de URL's privilegiadas? (M/12)

(____) SIM (____) NÃO

1.1.1.13 A função Auto-Complete é desativada por padrão? (M/13)(W/02)

(____) SIM (____) NÃO

1.1.2 Mecanismo de Autenticação - Reautenticação

1.1.2.1 A Reautenticação é exigida antes que sejam permitidas quaisquer operações críticas? (O/10)

(____) SIM (____) NÃO

1.1.2.2 É exigida a Reautenticação do usuário-cliente (p. ex., ID de usuário e Senha têm que ser ressubmetidos) após o acionamento da função "Voltar/Atualizar" do navegador? (M/14)

(____) SIM (____) NÃO

1.1.3 Mecanismo de Autenticação - Apresentação de Mensagens

1.1.3.1 Mensagens de erro são apresentadas em falhas de Autenticação (p. ex.: mensagem “Usuário Inválido”)? (M/11) (O/9)

(____) SIM (____) NÃO

1.1.3.2 A aplicação responde com Mensagens não informativas (não esclarecedoras) de falhas de Autenticação? (O/7)

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

1.1.4 Mecanismo de Autenticação - Tempo-limite (Timeout)

1.1.4.1 Existe um Tempo-limite da sessão do usuário-cliente (O/21)? (geralmente aplica-se a produtos com dados sensíveis, os quais têm controle de tempo máximo de não utilização para, em seguida, terem o seu encerramento) (P/3.3.13.1)

(____) SIM (____) NÃO

Em caso afirmativo:

1.1.4.2 A contagem do Tempo-limite é feita no host-servidor? (C)

(____) SIM (____) NÃO

1.1.4.3 Este Tempo-limite de inatividade é apropriado à aplicação? (O/22)

(____) SIM (____) NÃO

1.1.4.4 O Tempo-limite de inatividade cancela a sessão atual autenticada? (O/23)

(____) SIM (____) NÃO

1.1.4.5 No caso de Autenticação compartilhada o Tempo-limite de inatividade cancela todas as outras sessões autenticadas simultâneas (de um mesmo usuário)? (O/24)

(____) SIM (____) NÃO

1.1.4.6 As credenciais de Autenticação expiram após um período de tempo sem acesso (W/11)?

(____) SIM (____) NÃO

1.1.5 Mecanismo de Autenticação - Criptografia

1.1.5.1 O mecanismo de Autenticação utiliza criptografia (por exemplo, ID de Usuário e Senha)? (P/3.3.11.6)

(____) SIM (____) NÃO

Descrever:

1.1.5.2 As credencias de Autenticação são armazenadas de forma cifrada/criptografada?

Obs.: É negativo a senha armazenada em texto claro (o mesmo conteúdo digitado na tela é armazenado em *plain text* no banco de dados) ou apenas codificada.

(____) SIM (____) NÃO

1.1.5.3 As credencias de Autenticação são criptografadas quando transmitidas pela rede, mesmo em canal não seguro? (O/12)

(____) SIM (____) NÃO

1.1.5.4 Caso a aplicação faça uso de aplicações/ferramentas externas, todas as credenciais de Autenticação para acesso a serviços externos a ela são criptografadas e armazenadas em um local protegido (e não em código-fonte)? (W/14)

(____) SIM (____) NÃO (____) NÃO SE APLICA

1.1.6 Mecanismo de Autenticação - Logout

1.1.6.1 O usuário-cliente consegue iniciar um procedimento de Logout pela aplicação? (O/25)

(____) SIM (____) NÃO

1.1.6.2 Em caso afirmativo e de Autenticação compartilhada, o Logout do usuário-cliente cancela todas as outras sessões ativas (de um mesmo usuário)? (O/26)

(____) SIM (____) NÃO

1.1.6.3 Algum tipo de refresh ou caching permite que usuários reutilizem a aplicação, sem fornecer novamente seus detalhes de Autenticação? (O/27)

(____) SIM (____) NÃO

1.1.7 Mecanismo de Autenticação - Bloqueio

1.1.7.1 *Existe algum tipo de procedimento para bloqueio de usuários-cliente, quando necessário? (O/15)*

(____) SIM (____) NÃO

Em caso afirmativo, descrever tipo de bloqueio:

1.1.7.2 *Há um número máximo de tentativas de Autenticação? (S) (ASVS/3)* ***Possui o controle de número de tentativas para a digitação de Senhas? (P/3.3.11.4)***

(____) SIM (____) NÃO

1.1.7.3 *Em caso afirmativo, se o número máximo de tentativas é ultrapassado, o que a aplicação faz? A conta do usuário-cliente é bloqueada por um período de tempo suficiente para deter os ataques de força bruta? (S) (W/3)*

(____) SIM (____) NÃO

Descrever:

1.1.7.4 *Existe algum tipo de procedimento para bloqueio de host-servidor ou cliente (por exemplo, bloqueio de IP) quando necessário? (O/16)*

(____) SIM (____) NÃO

1.1.7.5 Em caso afirmativo, a aplicação informa o usuário-cliente sobre o bloqueio de conta? (O/17)

(____) SIM (____) NÃO

Descrever como:

1.1.7.6 É possível desabilitar forçadamente o usuário-cliente autenticado pela anulação de credenciais no host-servidor? (O/28)

(____) SIM (____) NÃO

(OBS: para aplicações críticas, é recomendável que haja a possibilidade de monitoramento das ações e eventuais intervenções dentro do sistema, por exemplo, para uma eventual anulação de credenciais de autenticação)

1.1.7.7 Em caso afirmativo, o usuário-cliente consegue continuar a operação após a anulação? (O/29)

(____) SIM (____) NÃO

1.1.7.8 O usuário-cliente autenticado é bloqueado, caso identifique uma operação ilícita dele? (C)

(____) SIM (____) NÃO

1.1.8 Mecanismo de Autenticação - Adicional

1.1.8.1 Os dados inseridos nos campos do formulário de autenticação são tratados de forma adequada, a fim de evitar ataques XSS e/ou SQL Injection? (M/15)

(____) SIM (____) NÃO

1.1.8.2 As Senhas de contas utilizam um mecanismo de salt único para aquela conta, e são codificadas por algoritmos de hash antes de serem armazenadas? (W/13)

(____) SIM (____) NÃO

1.1.8.3 As páginas de Login e de mudança de Senha utilizam SSL (Secure Sockets Layer) (HTTP ou HTTPS)? (M/1)

(____) SIM (____) NÃO

1.1.8.4 As páginas que contém dados sensíveis (CPF, RG, Cartão de Crédito) utilizam SSL? (M/2)

(____) SIM (____) NÃO

1.2 IDENTIDADE (ID) DE AUTENTICAÇÃO

A Identidade de Autenticação é originada de três categorias:

Autenticação baseada no conhecimento (o que se sabe): senhas, informações pessoais ou qualquer informação não necessariamente secreta, mas que seja considerada desconhecida por outros.

Autenticação baseada na propriedade (o que se tem): identidade inserida no Smartcard ou Token.

Autenticação baseada na característica (o que é): identidade por biometria, como impressão digital, íris, voz ou padrão de comportamento característico de uma pessoa.

1.2.1 Identidade de Autenticação - Geral

1.2.1.1 Existe uma política para a determinação da Identidade de Autenticação (há alguma regra para determinar o ID de Usuário, Senha, etc.)? (R)

(☐) SIM (☐) NÃO

Em caso afirmativo, descrever quais informações formam a identidade de um usuário-cliente:

1.2.1.2 A Identidade de Autenticação é armazenada nos hosts-cliente? (O/13) (M/8)

(☐) SIM (☐) NÃO

1.2.1.3 A Identidade de Autenticação é armazenada no host-servidor? (O/13) (M/8)

(☐) SIM (☐) NÃO

Descrever como a identidade é armazenada (cifrada ou texto claro, banco de dados ou arquivos texto, algoritmos utilizados, etc.):

1.2.1.4 No formulário de Logon, o host-servidor fornece uma Identidade única para este formulário de Autenticação? (C)

(____) SIM (____) NÃO

Em caso afirmativo, descrever quais informações formam a identidade do formulário:

1.2.1.5 A aplicação tem algum recurso para inibir força bruta nos procedimentos de Autenticação e nas contas de usuários-clientes? (testando-se todas as possibilidades para forçar a Autenticação nas contas dos usuários) (O/19)

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

1.2.1.6 É possível determinar detalhes das credenciais de Autenticação de outros usuários-clientes (p.ex., detalhes da Senha), a partir de um conjunto conhecido de credenciais (p.ex., dicionários)? (O/31)

(____) SIM (____) NÃO

1.2.2 Identidade de Autenticação - ID usuário/Senha

1.2.2.1 Existe uma política de complexidade das senhas utilizadas nos sistemas da organização e de terceiros? (O/34) (M/3) (P/3.3.11.2)

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

1.2.2.2 A Senha anterior é exigida para se confirmar qualquer mudança para uma nova composição dos detalhes de Autenticação (ID ou senha)? (O/36) (M/7)

(____) SIM (____) NÃO

1.2.2.3 Existe um processo para os usuários-clientes mudarem a própria Senha?

(____) SIM (____) NÃO

1.2.2.4 Quando a primeira senha, gerada aleatoriamente, é fornecida, a mudança de Senha é obrigatória no primeiro Login? (M/5) (O/32) (O/38) (P/3.3.11.5)

(____) SIM (____) NÃO

1.2.2.5 Existe um processo para recuperar a Senha (p.ex., página “Esqueci a Senha” ou “Lembre-me”)? (M/4, 8)

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

1.2.2.6 É possível reutilizarem-se Senhas anteriormente já utilizadas (de um mesmo usuário ou de outro usuário)? (O/33)

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

1.2.2.7 As páginas de Login e de mudança de Senha apresentam o recurso CAPTCHA ou outro semelhante para proteger a digitação de Senhas? (M/10)

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

1.2.2.8 Os detalhes sensíveis de Autenticação (p. ex., a Senha) são apresentados em texto claro enquanto o usuário-cliente está digitando-os? (O/10) (O/35) (P/3.3.11.3)

(____) SIM (____) NÃO

---

2. RASTREABILIDADE

1.3 2.1 LOG

2.1.1 Registro de Autenticação

2.1.1.1 O processo de Autenticação e todas as decisões de Autenticação, em caso de sucesso ou falha, são registrados? (O/4) (W/12) (O/39) (O/41 e 42)

(____) SIM (____) NÃO

Em caso afirmativo, descrever onde e como:

2.1.1.2 Como os eventos são registrados (p. ex., arquivos de texto ou banco de dados)?

Descrever:

2.1.1.3 Os eventos de Entrada e Saída de uma sessão são registrados no Log? (C)

(____) SIM (____) NÃO

Descrever:

2.1.1.4 As mudanças dos detalhes de Autenticação são registradas nos Logs? (O/37) (O/40)

Obs.: detalhes da Autenticação (identificação do host; horário, dia, mês e ano do evento).

(____) SIM (____) NÃO

2.1.1.5 Os arquivos de Log são registrados sequencialmente, permitindo identificar o tempo cronológico da autenticação realizada? (O/48)

(____) SIM (____) NÃO

2.1.1.6 Por quanto tempo são mantidos os arquivos de Log? (O/51)

Descrever:

2.1.1.7 As permissões são suficientemente restritivas para prevenir acessos inadequados aos registros nos arquivos de Log? (O/46)

(____) SIM (____) NÃO

2.1.2 Recuperação de Autenticação

2.1.2.1 É possível recuperar informações sensíveis de Autenticação (p.ex., Senhas, ID's de sessão), a partir dos registros nos arquivos de Log? (O/43)

(____) SIM (____) NÃO

Descrever:

2.1.2.2 É possível identificar, tanto o host-cliente como o ID do usuário, a partir dos registros nos arquivos de Log? (O/44)

(____) SIM (____) NÃO

2.1.2.3 É possível examinar os registros nos arquivos de Log, estando-se dentro da aplicação? (O/45)

(____) SIM (____) NÃO

Descrever:

2.1.2.4 *Há algum mecanismo ou recurso para backup e recuperação dos eventos nos arquivos de Log? (O/52)*

Obs.: definir registros e eventos nos arquivos de Log.

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

2.1.2.5 *Há algum mecanismo que conduza ou facilite o processo de análise dos registros nos arquivos de Log? (G)*

(____) SIM (____) NÃO

Em caso afirmativo, descrever:

10.4 APÊNDICE 4 – RELATÓRIO COMPRAS-ONLINE – AVALIAÇÃO
FORMAL

Relatório de Avaliação da Segurança de acesso de Aplicação Web

COMPRAS-ONLINE

*Responsável pelo Produto:
Empresa A – Equipe COMPRAS-ONLINE*

Campinas, 27 de Novembro de 2013

RELATÓRIO DE AVALIAÇÃO <COMPRAS-ONLINE>

1. ESCOPO

Este documento apresenta o resultado da avaliação da aplicação web *COMPRAS-ONLINE*

Abrange a avaliação e medição da propriedade de segurança Autenticidade, uma das propriedades da Segurança de acesso para aplicações web.

O *COMPRAS-ONLINE* é um portal na web que permite consultas e compras de Produtos EM GERAL.

Este trabalho faz parte da pesquisa de doutorado da aluna Regina M Thienne Colombo com o Prof orientador Marcelo S P Pessoa no departamento de Engenharia de Produção da POLI-USP

2. INTRODUÇÃO

A pesquisa de doutorado tem como objetivo geral apresentar uma metodologia de avaliação da segurança de acesso de aplicações web, este trabalho é uma prova de conceito para a propriedade Autenticidade.

3. O PROCESSO DE AVALIAÇÃO

O processo de Avaliação abordou as seguintes etapas:

a- Estabelecer os Requisitos de Segurança

Nesta etapa é considerada como propósito a verificação de conformidade da propriedade Autenticidade do *COMPRAS-ONLINE* em relação ao modelo de referência da Figura 1.

A Figura 2 mostra o mesmo modelo com mais níveis de desdobramento e configurado na ferramenta de software *SuperDecision®*, que auxilia a medição e priorização dos atributos de segurança com o método AHP – *Analytic Hierarchy Process*.

Figura 1 – Modelo de Referência para Autenticidade

Figura 2 – Modelo de autenticidade no SuperDecision®

b- Especificar a Avaliação

Nesta etapa é definido o *checklist* para medir a propriedade Autenticidade. O *checklist* é composto pelos atributos mensuráveis contidos na Tabela 1, ver a coluna “Nível 5”.

Tabela 1 - Cinco níveis da propriedade de Autenticidade

NÍVEL 1	NÍVEL 2	NÍVEL 3	NÍVEL 4	NÍVEL 5
AUTENTICIDADE	AUTENTICAÇÃO	MECANISMO	CARACTERÍSTICAS BÁSICAS	Revela Informações
				No Host Servidor
				Identifica Informações do Cache
				Múltiplos Usuários
				Perda de Credenciais
				Múltiplas Camadas
				URL's Privilegiadas
				Auto-Complete OFF
			REAUTENTICAÇÃO	Reautenticação Exigida
				Reautenticação Navegador
			MENSAGENS	Mensagens de Erro
				Mensagens Não-informativas
			TIMEOUT	Timeout por Inatividade
				Timeout Adequado
				Timeout Cancela Seção
				Cancela Sessões Simultâneas
			CRIPTOGRAFIA	Criptografia de Dados Sensíveis
				Acesso Seletivo
				Serviços (Dados) Externos
				Senha Não-criptografada
				Criptografia na Rede
			LOGOUT	Logout Usuário
				Cancela Todas as Sessões
				Refresh preserva Logout
			BLOQUEIO	Bloqueio de Usuário
				Máximo de Tentativas
				Detem Força-bruta
				Bloqueio de Host (IP)
				Desabilita Usuário
			CARACTERÍSTICAS ADICIONAIS	Login Resiste a SQL Injection
				Senhas Temperadas
				Páginas de Senhas em HTTPS
				Páginas (Dados) Sensíveis em SSL

		IDENTIDADE	CARACTERÍSTICAS BÁSICAS	Política para ID
				ID no Host-cliente
				ID no Host-servidor
				Força-bruta na Autenticação possível
				Adivinhação de Credenciais possível
			ID/SENHA	Política (Regras) para Senhas Fortes
				Senha Anterior em Mudanças
				Reutiliza Senhas Anteriores
				Muda Senha no 1º Login
				Recurso para Recuperar Senha
	RASTREABILIDADE	LOG	REGISTRO DE AUTENTICAÇÃO	Recurso CAPTCHA
				Usuário Muda Detalhes (Senha)
				Senha apresentada em Plain Text
				O processo de Autenticação, sucesso ou falha, são registrados
				Eventos são registrados
			RECUPERAÇÃO DE AUTENTICAÇÃO	Entrada e Saída de uma sessão são registrados
				Mudanças dos detalhes de Autenticação são registradas
				Arquivos de Log são registrados sequencialmente
				Quanto tempo são mantidos os arquivos de Log
				Permissões são suficientemente restritivas para prevenir acessos inadequados

c- Projetar a Avaliação

Nesta etapa é definido o plano de Avaliação, com a identificação dos instrumentos a serem utilizados – o ambiente de hardware e software, o

sistema alvo de Avaliação – COMPRAS-ONLINE, o *checklist*, a equipe responsável por responder ao checklist e possivelmente alguma documentação de acesso disponível. Os atributos da tabela 1 compõem o checklist.

d- Executar a Avaliação

Nesta etapa são efetuadas as verificações planejadas, a coleta dos dados e das informações obtidas durante a Avaliação e realizado o procedimento de análise dos resultados obtidos.

O *Checklist* AUTENTICIDADE foi respondido pela equipe responsável pelo COMPRAS-ONLINE e é validado por avaliador independente.

É realizado o julgamento dos critérios par a par, utilizando a escala de Saaty.

A Tabela 2 mostra os atributos de Mecanismo e Identidade da Autenticação e a Rastreabilidade, isto é, os critérios que devem ser pontuados com a escala de Saaty, por meio do julgamento dos critérios pelos responsáveis pelo COMPRAS-ONLINE. A Tabela 2 é utilizada pela equipe para fazer a comparação par a par entre os critérios. Esta fase é bastante debatida, mas é necessário que haja um consenso final pela equipe.

A escala de Saaty varia de 1 a 9, para definir a Importância entre os critérios, sendo:

- 1 – igual Importância;
- 3 – pouca Importância;
- 5 – média Importância;
- 7 – grande Importância;
- 9 – absoluta Importância;

Tabela 2 – Tabela de auxílio aos critérios

AUTENTICIDADE	ESCALA DE SAATY (Valores de 1 a 9)	CRITÉRIO
AUTENTICAÇÃO	7	RASTREABILIDADE
MECANISMO	5	IDENTIDADE
CARAC BÁSICAS- Cb (Mecanismo)	7	REAUTENTICAÇÃO
	7	MENSAGENS
	5	TIMEOUT
	1	CRIPTOGRAFIA
	7	LOGOUT
	7	BLOQUEIO
	5	CARAC. ADICIONAL - Ad
REAUTENTICAÇÃO- Re	7	MENSAGENS
	1/5	TIMEOUT
	1/7	CRIPTOGRAFIA
	1/5	LOGOUT
	1/5	BLOQUEIO
	1/7	CARAC.ADICIONAL
MENSAGENS-Me	1/7	TIMEOUT
	1/7	CRIPTOGRAFIA
	1/5	LOGOUT
	1/7	BLOQUEIO
	1/7	CARAC.ADICIONAL
TEMPO-LIMITE-Ti	1/7	CRIPTOGRAFIA
	7	LOGOUT
	1	BLOQUEIO
	1/5	CARAC.ADICIONAL
CRIPTOGRAFIA-Cri	7	LOGOUT
	7	BLOQUEIO
	7	CARAC.ADICIONAL
LOGOUT-Lo	1/5	BLOQUEIO
	1/7	CARAC.ADICIONAL
BLOQUEIO-BI	1/7	CARAC.ADICIONAL
CARAC. BÁSICAS (Identidade)	1/7	ID USUÁRIO/SENHA
REG AUTENT	5	REC AUTENT

Após a realização do julgamento, os dados são inseridos na ferramenta SuperDecision® para serem feitos os cálculos das Prioridades pelo método AHP. A Tabela 3 mostra um exemplo de uma matriz de decisão para os julgamentos realizados.

Tabela 3 - Matriz de Decisão para COMPRAS-ONLINE

	Cb	Re	Me	Ti	Cri	Lo	BI	Ad
Cb	1	7	5	1	1	5	1	1
Re	1/7	1	3	3	3	3	3	3
Me	1/5	1/3	1	3	3	3	3	3
Ti	1	1/3	1/3	1	1	5	1	3
Cri	1	1/3	1/3	1	1	5	5	3
Lo	1/5	1/3	1/3	1/5	1/5	1	5	1
BI	1	1/3	1/3	1	1/5	1/5	1	5
Ad	1	1/3	1/3	1/3	1/3	1	1	1

e- Concluir a Avaliação

Nesta etapa é preparado o resultado da Avaliação com o auxílio da ferramenta SuperDecision®, que realiza os cálculos e nos fornece os resultados quantitativos obtidos.

4. RESULTADOS DE AVALIAÇÃO

A seguir é apresentado o resultado da Avaliação, primeiramente de forma quantitativa e também de forma qualitativa, destacando os aspectos a serem revistos nos pontos que foram avaliados.

Quantitativamente o resultado é:

A Tabela 4 mostra a pontuação para cada componente e atributo de segurança.

Tabela 4 - Resultado da Autenticidade no AHP para o COMPRAS-ONLINE

Nível 1	Nível 2	Nível 3
Autenticação	Mecanismo	Características básicas
		Reautenticação
		Apresentação de mensagens
		Tempo-limite
		Criptografia
		Logout
		Bloqueio
Rastreabilidade	Identidade	Características básicas
		ID usuário/senha
	Log	Registro de Autenticação
		Recuperação de Autenticação

No primeiro nível vê-se que a pontuação para Autenticidade foi de 70%, para o COMPRAS-ONLINE.

No segundo nível vê-se que entre Mecanismo e Identidade, Mecanismo tem a prioridade de 60% perante a Identidade com 40 %. No nível 3 vê-se que o atributo Criptografia é 75 % mais importante que os demais atributos de Mecanismo.

Com este resultado, é possível ver o que o COMPRAS-ONLINE atende e não atende ao Modelo de referência e adicionalmente quais as prioridades entre os critérios, dessa forma, a equipe responsável tem um indicador de onde é prioritário ações para correção e melhoria da Autenticidade do COMPRAS-ONLINE.

Qualitativamente o resultado é apresentado, o desempenho do COMPRAS-ONLINE perante o Modelo de Referência de Autenticidade

4.1 AUTENTICAÇÃO

4.1.1 Mecanismo de autenticação

4.1.1.1 Características básicas

Aspectos de destaque positivo

- COMPRAS-ONLINE exige autenticação nas tarefas de acesso restrito;
- Os controles são realizados no host-servidor;
- Múltiplos usuários (~3000) autenticados podem acessar concomitante;
- Há mecanismo de recuperação de credenciais;
- Não permite uso de URL privilegiadas;
- Função auto-complete desativada.

Aspectos a serem revistos

- Possibilidade de identificar usuário anterior no host-cliente;
- Permite compartilhamento de um mesmo usuário;
- Implementação do código em múltiplas camadas.

Reautenticação

Aspectos de destaque positivo

- Não se exige reautenticação após acionamento da função “Atualizar” do navegador.

Aspectos a serem revistos

- Não exige reautenticação antes de operações críticas.

Mensagens

Aspectos de destaque positivo

- Apresenta mensagens sobre erro de autenticação e elas são neutras, isto é, não fornecem dados que possam ser utilizados para possíveis ataques.

Tempo-limite

Aspectos de destaque positivo

- Há um tempo-limite por sessão; ela é realizada no host-servidor; o tempo-limite é apropriado; ele cancela a sessão autenticada; as credenciais expiram após um tempo sem uso.

Aspectos a serem revistos

- Aceita compartilhamento de um mesmo usuário e não cancela todas as sessões autenticadas simultaneamente.

Criptografia

Aspectos de destaque positivo

- Há criptografia no mecanismo de autenticação, a senha; as credenciais são armazenadas de forma criptografada.

Aspectos a serem revistos

- As credenciais transmitidas na rede não são criptografadas.

Logout

Aspectos de destaque positivo

- O usuário-cliente pode iniciar um logout; ele só reutiliza a aplicação com uma nova autenticação.

Aspectos a serem revistos

- Com autenticação compartilhada, um logout do usuário-cliente não cancela todas as sessões ativas.

4.1.1.2 Bloqueio

Aspectos de destaque positivo

-

Aspectos a serem revistos

- Não Existe um procedimento de bloqueio, se necessário; não há um controle de tentativas de autenticação e não bloqueia o usuário, caso precise; avisa o usuário em caso de seu bloqueio.
- Não tem procedimento de bloqueio de IP; não é possível desabilitar um usuário-cliente; não há bloqueio de usuário cliente caso ele faça operação ilícita.

4.1.1.3 Adicional

Aspectos de destaque positivo

- As senhas utilizam mecanismo de salt antes de serem armazenadas no host-servidor de dados.

Aspectos a serem revistos

- Dados de entrada em formulários são tratados para evitar ataques de SQL Injection, mas não está eficiente, é possível fazer SQL Injection; as páginas de Login e as que contém dados sensíveis só utilizam HTTPS se for definido pelo usuário-cliente, ele não é feito automaticamente.

4.1.2 Identidade de autenticação

4.1.2.1 Características básicas

Aspectos de destaque positivo

- Há uma política para determinação do Id usuário e senha; a identidade de autenticação é armazenada somente no host-servidor, mas ela fica em texto claro; o formulário de Login tem uma identidade única.

Aspectos a serem revistos

- É possível usar força bruta nos procedimento de autenticação; é possível explorar credenciais de usuários-cliente; é possível explorar detalhes de credenciais.

4.1.2.2 Identidade ID usuário/senha

Aspectos de destaque positivo

- Há um processo para mudança de senha pelo usuário-cliente e para redefinir senha, caso de esquecimento; na digitação de senha, a senha não é mostrada na tela.

Aspectos a serem revistos

- É necessário uma política de definir senha forte; na definição de uma nova senha, não é pedido a senha anterior; é possível a reutilização de senhas anteriores; não há o recurso de Captcha para proteção de digitação de senhas.

4.2 RASTREABILIDADE

4.2.1 Log

4.2.1.2 Registro de autenticação

Aspectos de destaque positivo

- Os eventos de autenticação, os de Entrada e Saída e as mudanças de detalhes são registrados no Log; o Log tem registros sequenciais, por exemplo, pelo tempo cronológico; o acesso ao Log tem acesso restrito.

4.2.1.2 Recuperação de autenticação

Aspectos de destaque positivo

- Não é possível recuperar dados sensíveis do Log; é possível identificar ID de usuário no Log; não é possível acessar o Log pela aplicação.

Aspectos a serem revistos

- Não é possível recuperar eventos registrados no Log; não há um procedimento para análise dos registros do Log.

5. CONCLUSÕES

Os próximos passos sugeridos são:

- Uma reflexão pela equipe responsável pelo COMPRAS-ONLINE, nas seguintes questões
  - Vulnerabilidade é nova ou já conhecida?
  - Gravidade é Pequena, Média, Alta?
  - A Fonte/Causa do problema está relacionada a Rede, Servidor, Aplicação, Arquitetura, ou outra?
  - Tem outros desdobramentos de correções no sistema?
  - Quem é Responsável/Função por corrigir?
  - Qual o Prazo para corrigir?
  - Que ações podem gerar à equipe de desenvolvimento?
  - Que ações podem gerar aos responsáveis pelo sistema?
  - Que problemas podem gerar ao usuário do sistema?

- Uma reunião com os responsáveis pelo COMPRAS-ONLINE para maiores esclarecimentos sobre o sistema e os resultados obtidos relatados neste relatório e uma reflexão para possíveis ações a serem tomadas.

10.5 APÊNDICE 5 - GLOSSÁRIO

TERMINOLOGIA E CONCEITOS

Na área de segurança da informação, de software ou de TI não existe uniformidade de nomenclatura sendo que a mesma palavra tem significados diferentes. Também não existe uniformidade na tradução do Inglês para português, onde muitos vocábulos são utilizados sem tradução. A seguir apresento definições, conceitos e mesmo reflexões de interesse para esta pesquisa.

Aplicação Web

Aplicações web baseadas em sistemas distribuídos representam aplicativos de software complexos que fornecem informações e serviços usando linguagem HTML e interfaces XHTML. Este tipo de aplicações integra vários componentes como: elementos multimídia, como som, vídeo e clipes de mídia interativa; rotinas de processamento desenvolvidos em várias linguagens de programação como ASP, ASP, NET, PHP, JSP ou scripts CGI; rotinas de processamento que utilizam sintaxe JavaScript; estruturas lógicas que definem o quadro em que os dados de entrada são processadas, a fim de dar os resultados necessários; estruturas de rede que definem papéis diferentes para os componentes do aplicativo, tudo isso para que o sistema funcione adequadamente.

A *World Wide Web*, que em português significa, "Rede de alcance mundial"; também conhecida como Web e WWW, é um sistema de documentos em hipermídia que são interligados e executados em um conglomerado de redes em escala mundial de milhões de computadores interligados pelo protocolo TCP/IP que permite o acesso a informações e todo tipo de transferência de dados.

Arquitetura Cliente-Servidor

Na arquitetura cliente-servidor o usuário tem acesso a recursos remotos por meio de componentes do cliente implementado pela aplicação. Os recursos residem e são distribuídos em outras máquinas e este modo de processamento remoto é transparente para os usuários. Uma aplicação web distribuído é

dividido em vários componentes, de acordo com três níveis de arquitetura, como descrito na Figura 1: a camada de apresentação é o cliente, que é representado por um aplicativo de navegador; neste nível, o cliente exibe os dados recebidos do sever usando formulários XHTML e também aceita entradas do usuário e envia de volta para o servidor, usando JavaScript ou scripts Java applets.

Figura 1 - Arquitetura de três camadas de aplicativos baseados na Web

A camada de aplicação manipula o processo entre o cliente e o servidor, o servidor Web, servidor de Conteúdo, FTP ou servidor de e-mail proporcionando acesso a diferentes serviços e recursos; o núcleo do componente de uma distribuição baseada na aplicação Web. O serviço que serve de conteúdo web, normalmente é escutado na porta 80 para *Hyper Text Transfer Protocol* (HTTP), RFC 2616, ou na porta 443 para *Hyper Text Transfer Protocol Secure* (HTTPS), RFC 2818 (54).

Pelo critério número de usuários, baseadas nas aplicações Web distribuídas as seguintes opções podem estar presentes:

- Aplicações locais com um usuário; o produto de software permite que apenas uma seção de trabalho tenha acesso a apenas um usuário;
- Rede de aplicações com mais usuários simultaneamente, a aplicação de software gerencia série de sessões de trabalho ligadas a um grupo de usuários, estes utilizam os mesmos recursos e têm acesso simultâneo a

um conjunto comum de funções do aplicativo; um exemplo deste software é cliente-servidor de aplicativos.

Os dados de entrada baseados em aplicações Web distribuídas são compostos por:

- Entrada do usuário; aplicativos que permitem que o usuário digite dados, como captura de texto, voz e vídeo que serão processados, e avaliados, pois o aplicativo é baseado em uma aplicação Web com usuários que podem interagir com vários controles selecionando suas opções;
- Entrada automática; aplicações permitem aos usuários carregar os dados pré-formatados resultado de sessões de trabalho anteriores ou de outros aplicativos compatíveis.

Ameaça

Ameaça é a probabilidade ou frequência de um acontecimento nocivo (CVSS).

Auditoria

Auditoria é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada empresa, setor ou produto, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

Autenticidade

Propriedade que uma entidade é o que afirma ser (ISO/IEC FDIS 27000, 2009).

Autenticar (*Authenticate*) - Verificação da identidade de um usuário, de dispositivo, ou de outra entidade em um sistema computadorizado, frequentemente como um pré-requisito a permitir o acesso aos recursos em um sistema.

Autenticação (*Authentication*) - Verificação reivindicada de uma identidade. O processo de determinar a identidade de um usuário que esteja tentando alcançar um sistema.

Avaliação de software

É uma operação técnica que consiste na produção de uma avaliação de uma ou mais características de um software de acordo com um procedimento especificado.

Back-Up

Cópia rotineira dos dados para assegurar a recuperação dos que forem perdidos ou corrompidos.

Categorias de software

A classificação adotada pela IEEE STD 1062 (1998), para os produtos de software, é definida conforme o grau de liberdade que tem o usuário para definir e especificar suas funcionalidades. Segundo essa norma, há três tipos de produtos: COTS (*Commercial Off-The-Shelf-Software*), MOTS (*Modified Off-The-Shelf-Software*). , CUSTOMIZADO ou FD (Fully Developed Software).

Certificação de software

Certificação de software é emissão de um certificado de conformidade de um software a certo conjunto de normas ou especificações. Para obter uma certificação é necessária a realização de uma avaliação, atendendo a conformidade de requisitos, e é emitido um laudo ou certificado.

Confidencialidade

Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. O conceito de garantir a informação sensível confidencial, limitada para um grupo apropriado de pessoas ou organizações(ISO/IEC 13335-1:2004)

Confiabilidade

Capacidade do componente de manter um nível de desempenho especificado, quando usado em condições especificadas.

Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada. A informação deve ser entregue para a pessoa certa, quando ela precisar.

Falha, Defeito, e Erro

Uma falha de software ocorre por meio de um processo complexo que pode ocorrer na execução do software. Três conceitos são importantes para compreensão do processo de falha: **falha, defeito, e erro**.

Uma **falha** (failure em inglês) é a ocorrência de uma discrepância entre o resultado observado da execução do software e o resultado prescrito pelos requisitos.

Um **defeito** (fault ou defect) é uma anomalia no software que pode causar uma falha (exemplos: um comando imperfeito, incompleto, ausente ou extra no software).

Um **erro** (error) é um estado incorreto, intermediário ou final, de execução do software que pode produzir um resultado incorreto, ou seja, pode levar a uma falha do software.

Integridade

Propriedade que salvaguarda a exatidão e completeza de ativos. (ISO/IEC 13335-1: 2004). A qualidade de um sistema ou um componente que reflita sua exatidão e confiabilidade lógica, integridade, e consistência. Em termos da segurança, a integridade gera a exigência para o sistema ou o componente a ser protegido de encontro às tentativas intencionais ou acidentais a (1) alterar, modifica, ou destrói de maneira imprópria ou desautorizada, ou (2) impedem que execute suas funções pretendidas de uma maneira não enfraquecida, livre da manipulação imprópria ou desautorizada.

Medidas

Medição (obtem medidas) - é o processo no qual números ou símbolos são atribuídos para atributos de entidades do mundo real. É uma contagem, uma visão em um determinado tempo. Pode ser direta ou indireta.

Métricas

Métrica é derivada de duas ou mais medidas, vem de sua análise e Ajuda na tomada de decisão.

A chave para que as métricas de segurança tenham sucesso é a obtenção de dados que tenham as seguintes características ideais:

- Devem medir elementos organizacionais que tenham significância;
- Devem ser reprodutíveis;
- Devem ser objetivas e imparciais;
- Com o passar do tempo, devem ser capazes de medir algum tipo de progressão em direção a um objetivo da empresa.

Modelo de referência

Os modelos de referência, os quais podem ser desenvolvidos em situações reais ou por meio de estudos teóricos, documentam os vários aspectos de um processo de negócio ou produto. Pode-se distinguir entre modelos procedimentais ou de implementação de softwares-padrão, e modelos de negócios, tais como modelos para gestão da produção e desenvolvimento de produtos. Além disso, os modelos de referência podem ser especializados para mercados, segmentos ou tipologias específicas, categorias de produtos como, por exemplo, para a indústria automobilística, indústria de alimentos, varejo, indústria aeroespacial, software entre outros.

Não Repudio

Capacidade de provar a ocorrência de um evento ou ação requerida e de suas entidades originárias, a fim de resolver disputas sobre a ocorrência ou não ocorrência de evento ou ação e envolvimento de entidades no evento (ISO/IEC FDIS 27000, 2009).

Requisitos de Segurança

Os requisitos de segurança são utilizados para desenvolver o software com as devidas contramedidas aos possíveis ataques.

De acordo com SAVOLA (2007) Requisitos de segurança são declarações de contramedidas de alto nível que fazem mitigação de risco identificando adequadamente, formam a base de referência para a segurança do desenvolvimento de métricas. Esses riscos podem derivar de ameaças, das políticas gerais da organização e de propriedades do ambiente.

Requisitos de segurança derivados de ameaças representam as contramedidas, ou impõem mecanismos de segurança. Uma política de

segurança está preocupada com a análise, projeto, implementação, implantação e uso de tecnologia eficiente e segura que manipula o *Sul-System under Investigation*, em conformidade com o conjunto relevante de regras e procedimentos de segurança, e é baseado em requisitos de segurança .

Segurança de acesso

O grau pelo qual um produto ou sistema protege informação e dados de modo que pessoas ou outros produtos ou sistemas tenham o grau de acesso apropriado aos seus tipos e níveis de autorização aos dados (ISO/IEC 25010:2011)

Segurança de software

Segurança de Software não é o mesmo que software seguro. Se o software executa informações relacionadas à funções de segurança não significa que o software em si é seguro. Software que realiza a segurança de funções tem a mesma probabilidade de conter falhas e *bugs* como outros softwares. No entanto, porque as funções de segurança podem ter consequências danosas no caso de falha, o compromisso de que o software funcione adequadamente tem um impacto significativamente maior do que o compromisso ou o fracasso de outros softwares.