Dissertação apresentada à Pró-Reitoria de Pós-Graduação e Pesquisa do Instituto Tecnológico de Aeronáutica, como parte dos requisitos para obtenção do título de Mestre em Engenharia no Programa de Pós-Graduação em Engenharia Eletrônica e Computação, Área Informática.

Ricardo Férre Lacerda Ferreira

USASEC: UM MÉTODO PARA INTEGRAÇÃO DE REQUISITOS DE USABILIDADE E SEGURANÇA PARA PROTEÇÃO CIBERNÉTICA EM APLICAÇÕES WEB

Dissertação aprovada em sua versão final pelos abaixo assinados:

Prof. Dr. Carlos Henrique Quartucci Forster
Orientador

Prof. Dr. Edgar Toshiro Yano
Coorientador

Prof. Dr. Luiz Carlos Sandoval Góes
Pró-Reitor de Pós-Graduação e Pesquisa

Campo Montenegro
São José dos Campos, SP – Brasil
2017

Dados Internacionais de Catalogação-na-Publicação (CIP)
Divisão de Informação e Documentação

Ferreira, Ricardo Férre Lacerda Ferreira
USASEC: Um método para integração de requisitos de usabilidade e segurança para proteção cibernética em aplicações Web.
São José dos Campos, 2017.
182f. Número de Folhas

Dissertação de mestrado – Curso de Engenharia Eletrônica e Computação, Área de Informática – Instituto Tecnológico de Aeronáutica, 2017. Orientador: Prof. Dr. Carlos Henrique Quartucci Forster e Co-orientador: Prof. Dr. Edgar Toshiro Yano.

1. Usabilidade.2 Segurança da Informação. 3.Desdobramento da Função de Qualidade de Software. I. Departamento de Ciência e Tecnologia Aeroespacial. Instituto Tecnologico de Aeronáuitca. II. USASEC: Um método para integração de requisitos de usabilidade em proteção cibernética para aplicações web.

REFERÊNCIA BIBLIOGRÁFICA

Ferreira, Ricardo Férre Lacerda Ferreira. **USASEC: Um método para integração de requisitos de usabilidade e segurança para proteção cibernética em aplicações Web.** 2017. 148f. Total de 182 folhas. Dissertação de (Mestrado em Informática) – Instituto Tecnológico de Aeronáutica, São José dos Campos.

CESSÃO DE DIREITOS

NOME DO AUTOR: Ricardo Férre Lacerda Ferreira
TÍTULO DO TRABALHO: USASEC: Um método para integração de requisitos de usabilidade e segurança para proteção cibernética em aplicações web.
TIPO DO TRABALHO/ANO: Dissertação / 2017

Ricardo Férre Lacerda Ferreira
Rua H9C, 102, Campus do CTA,
CEP: 12228-612, São José dos Campos - SP

USASEC: UM MÉTODO PARA INTEGRAÇÃO DE REQUISITOS DE USABILIDADE E SEGURANÇA PARA PROTEÇÃO CIBERNÉTICA EM APLICAÇÕES WEB.

Ricardo Férre Lacerda Ferreira

Composição da Banca Examinadora:

Prof. Dr.	José Maria Parente de Oliveira	Presidente	ITA
Prof. Dr.	Carlos Henrique Q. Forster	Orientador	ITA
Prof. Dr.	Edgar Toshiro Yano	Coorientador	ITA
Prof. Dr.	Adilson Marques da Cunha	Membro Interno	ITA
Prof. Dr.	Eduardo Martins Guerra	Membro Externo	INPE

ITA

Dedico este trabalho a minha família: Katya,
Ezequiel e André; sem o apoio dos
quais eu não poderia realizar este trabalho.

Agradecimentos

A Deus, primeiramente, por me manter firme na caminhada para a realização do Seu propósito em minha vida e da minha família.

A minha esposa Katya por ter dedicado todos os seus sonhos, profissão e vida a me seguir nas diversas cidades que a carreira militar impõe.

Aos meus filhos Ezequiel e André por entenderem a minha ausência durante os longos períodos de estudo e dedicação para a realização deste trabalho.

Ao meu orientador, Prof. Dr. Carlos Henrique Q. Forster, pela confiança, motivação, dedicação e paciência que foram desprendidos a mim durante a realização da pesquisa.

Ao meu co-orientador, Prof. Dr. Edgar T. Yano, pela inspiração e conhecimentos fundamentais passados.

Ao Exército Brasileiro, especificamente à equipe de Tecnologia da Informação do Centro de Aviação do Exército pelo profissionalismos, empenho, abnegação e contribuição fundamentais para a confecção deste trabalho.

"O que adquire entendimento ama sua alma; o que conserva a inteligência acha o bem".

(Salomão, Provérbios 19:8)

Resumo

A presteza das informações e as recentes tecnologias integradas de dados estabeleceram um ambiente mundial interconectado de alta concorrência onde requisitos como prazo, qualidade e segurança dos softwares precisam ser atendidos. Nesse intuito, organizações investem recursos para que suas soluções de tecnologias possam oferecer qualidade para seus usuários e segurança da informação. Ainda, por causa da migração para a plataforma web de vários serviços e atividades, tem crescido o número de incidentes de segurança como ataques cibernéticos a estes sistemas. Para mitigá-los, é necessário manter os sistemas em constante aperfeiçoamento e atualizados contra as novas ameaças e vulnerabilidades apresentadas diariamente no ambiente virtual. Esses avanços nas regras de segurança obrigam os usuários a realizar tarefas cada vez mais complexas, impactando a usabilidade dos usuários. Para garantir a usabilidade, sem empenhar padrões oportunos de segurança, mostra-se necessária um método capaz de acoplar os requisitos de usabilidade aos requisitos de segurança. Com o método proposto, denominado USASEC, é possível priorizar e integrar quais requisitos de usabilidade e segurança mais impactam as tarefas do usuário. Para isso, este método utiliza uma derivação de um método para qualidade de software; o Desdobramento da Função de Qualidade de Software (o moderno SQFD), para identificar, filtrar, classificar, organizar, priorizar e integrar estes requisitos. Em cada uma destas, foram definidos métodos específicos como: Avaliação em Percurso Pluralístico da aplicação web, Diagrama de Árvore, Diagrama de Afinidade, Diagrama de Hierarquia, Processo de Análise Hierárquica e o método da Casa da Qualidade. Para avaliar o USASEC foi realizado um estudo de caso: no Sistema de Gerenciamento de Investigação e Prevenção de Acidentes Aeronáuticos (SIGIPAAerEx), uma aplicação web do Comando de Aviação do Exército Brasileiro, Taubaté, Brasil. Com uma amostra de usuários, os resultados mostraram uma taxa de acerto de oitenta porcento na priorização dos requisitos de usabilidade, após a aplicação do método.

Abstract

Information readiness and recent integrated data technologies have established an interconnected global environment of high competition where requirements such as terms, quality, and security of software need to be met. To this end, organizations invest resources so that their technology solutions can offer quality to their users and information security. Yet, because of the migration to the web platform of various services and activities, the number of security incidents such as cyber attacks on these systems has grown. To mitigate them, it is necessary to keep systems constantly improving and up-to-date against the new threats and vulnerabilities that are presented daily in the virtual environment. These advances in security rules force users to perform increasingly complex tasks, impacting user usability. To ensure usability, without compromising timely security standards, a methodology is needed to match usability requirements with security requirements. With the proposed method, called USASEC, it is possible to prioritize and integrate which usability and security requirements most impact user's tasks. To this end, this method uses a derivation from the established methodology for software quality, the Software Quality Function Deployment (the modern SQFD), to identify, filter, classify, organize, prioritize, and integrate these requirements. In each of these, specific methods were defined as: Evaluation in Pluralistic Route of the web application, Tree Diagram, Affinity Diagram, Hierarchy Diagram, Hierarchical Analysis Process, and the Quality House method. To validate the USASEC, a case study was carried out: in the Aeronautical Investigation and Prevention Management System (SIGIPAAerEx), a web application of the Brazilian Army Aviation Command, Taubate, Brazil. With a sample of users from outside of the search, the results showed an accuracy rate of eighty percent in the prioritization of usability requirements after the proposed method application.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

A	Aprendizagem
ABNT	Associação Brasileira de Normas Técnicas
AHP	Processo de Análise Hierárquica
AI	Acesso à Internet
ASVS	*Application Security Verification Standard*
BAVEx	Batalhão de Aviação do Exército
BAVT	Base Administrativa de Aviação de Taubaté
CAVEx	Comando de Aviação do Exército
CAD	Consulta e Análise Estatística de Dados
CDCiber	Centro de Defesa Cibernética do Exército
CDS	Centro de Desenvolvimento de Sistemas
CITEx	Centro de Telemática do Exército
CIAVEx	Centro de Instrução de Aviação do Exército
COTER	Comando de Operações Terrestre
COLOG	Comando Logístico do Exército
COAPL	Confecção de Aplicativos para Celular
ComDCiber	Comando de Defesa Cibernético
CMA	Comando Militar da Amazônia
CMO	Comando Militar do Oeste
CMSE	Comando Militar do Sudeste
CRFS	*Cross-Site Request Forgery*
CSIS	Centro de Estratégia e Estudos Internacionais (*Center for Strategic and International Studies*)

CVT	*Customer Value Table*
DCU	Design Centrado no Usuário (*User-Centered Design* - UCD)
DECEx	Departamento de Educação e Cultura do Exército
DETMIL	Diretoria de Educação Técnica Militar
DFSS	*Design For Six Sigma*
DISMOV	Confecção de Dispositivos Móveis
DIV	Divulgação da Aplicação Web
DMAIC	*Define Measure Analyse Improve and Control*
DMADV	*Define Measure Analyse Design and Verify*
DMAVEx	Diretoria de Materiais de Aviação do Exército
DSIC	Departamento de Segurança da Informação e Comunicação
EFK	Eficácia
EFI	Eficiência
EM	Equipe Multidisciplinar
EnaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
E-GOV	Governo Eletrônico (*Electronic Government*)
FU	Facilidade de Uso
FMEA	*Failure Mode and Effect Analyses*
GSI/PR	Gabinete de Segurança Integrado da Presidência da República
IC	Índice de Consistência
IoT	Internet das Coisas (*Internet of Things*)
IR	Índice de Consistência Randômico
IMN	Inclusão de Manual para o usuário

HCISeg	Interação Homem-Computador e segurança (*Human-Computer Interaction Security*)
HCI	Interação Homem-Computador (*Human-Computer Interaction*)
HoQ	Casa da Qualidade (House of Quality)
HTTP	*HyperText Transfer Protocol*
IEC	Comissão Eletrotécnica Internacional (*International Electrotechnical Commission*)
ISO	*International Organization for Standardization*
KJ	*Kawakita Jiro*
M	Memorização
MD	Ministério da Defesa
MVT	Tabela de Máximo Valor (*Maximum Value Table*)
MAHP	*Multiple Analysis Hierarchy Process*
MP	*Management and Project*
NBR	Norma Brasileira
OSI	*Open System Interconnection*
OWASP	*Open Web Application Security Project*
PIB	Produto Interno Bruto
PPAA	Plano de Prevenção de Acidentes Aeronáuticos
PML	Peso Médio Local
PG	Vetor de Prioridade Global
QFD	Desdobramento da Função da Qualidade *(Quality Function Deployment)*
RC	Razão de Consistência
RF	Relatório Final

REL PREV	Relatório de Prevenção de Acidentes
RSDM	Modulo Robusto de Desenvolvimento de Software (*Robust Software Deployment Model*)
RSV	Recomendações de Segurança de Voo
S	Segurança
SQFD	Desdobramento da Função da Qualidade para Software *(Software Quality Function Deployment)*
SCADA	Sistema de Supervisão e Aquisição de dados (*Supervisory Control and Data Acquisition*)
SIGIPAAerEx	Sistema de Gerenciamento de Investigação e Prevenção de Acidentes Aeronáuticos do Exército
SIPAA	Seção de Investigação e Prevenção de Acidentes Aeronáuticos
SIPAAEx	Sistema de Investigação e Prevenção de Acidentes Aeronáuticos do Exército
SIPAAER	Sistema de Investigação e Prevenção de Acidentes Aeronáuticos
SISFRON	Sistema Integrado de Monitoramento de Fronteiras
SISMC²	Sistema Militar de Comando e Controle
SisAVEx	Sistema de Aviação do Exército
TAU	Telas diferenciadas de Acesso para administradores e Usuários
TQM	Gestão da Qualidade Total (*Total Quality Management*)
U	Utilidade
UVT	Tabela de Valor do Usuário (*User Value Table*)
USASEC	Método de integração de requisitos de usabilidade e segurança (*USAbility and SECurity*)
UoV	*User of Voice*

Sumário

Introdução

A abertura para o público em geral de uma rede de computadores, anteriormente exclusiva para pesquisa acadêmica, permitiu que organizações e empresas disponibilizassem seus serviços e produtos de maneira fácil e globalizada. Assim, no início da década de 90, a chamada Internet trouxe características como: necessidade de disponibilizar plataformas e sistemas para prover conteúdo multimídia para usuários e integrar novos contingentes de clientes e suas máquinas a este novo meio de comunicação. Estas características trouxeram uma maior proximidade e interação entre os usuários e seus fornecedores, através das plataformas de aplicações *web*. Tal aplicação foi criada por Tim Berners-Lee e denominada World Wide Web ou (www) [1].

Com a inclusão desse novo canal de comunicação, além dos já existentes como a TV e o rádio, foi possível disponibilizar conteúdos sob demanda para usuários e revolucionar formas de relacionamentos entre processos de oferta e procura de negócios para empresas e consumidores. Esse novo meio de comunicação, aliado a popularização dos computadores pessoais tornou que a Internet incorporada ao cotidiano das pessoas. Logo, a *web*, como ficou conhecida a aplicação de Lee, causaria uma mudança de comportamento nos relacionamentos dos indivíduos e da sociedade.

Contudo, enquanto a Internet proporcionou benefícios como: interação social, conteúdo de fácil acesso e diminuição de distâncias entre indivíduos, ela também facilitou a possibilidade de realização de crimes e de disseminação de informações falsas, esta última ainda não considerada como crime. Estas últimas realizações ocorrem devido ao grau de anonimato sobre os indivíduos que a praticam utilizando aplicações *web* e a característica de acesso de qualquer ponto remoto do planeta. Por isto, para garantir a segurança dos usuários, é necessário que estas aplicações tenham especificações como: facilidade de uso, confiabilidade e segurança. Estes requisitos acarretam maior credibilidade para seus usuários, durante a realização de suas atividades.

Na Internet, muitas informações são falsas e procuram enganar os usuários com o intuito de induzirem estes a realizarem atividades que possam prejudicá-los. O acesso às páginas *web* ou correio eletrônico com conteúdo maliciosos são exemplos destas atividades. Desta forma, usuários precisam se proteger e garantir que informações confidencias não sejam comprometidas por programas maliciosos que, uma vez instalados no computador de forma oculta, permitam ao invasor acesso a elas. Algumas destas informações podem levar o atacante

a obter senhas, dados bancários, *e-mails* institucionais e, até mesmo, acesso a informações estratégicas e de Segurança Nacional.

Desta forma, cresce de importância a segurança de sistemas *web* que utilizam informações críticas de Estado, que dão suporte a sistemas críticos [2] ou que podem representar alvos compensadores para nações oponentes e/ou estratégicos para apoio a tomada de decisão.

1.1 Contextualização

O equilíbrio entre atender à necessidade do usuário e manter a segurança dos dados que trafegam por esses sistemas, causa ao usuário uma percepção de confiabilidade na aplicação. Esta faz com que a aplicação seja aprovada pelos usuários, logo, usada com mais frequência. Além de manter uma proteção cibernética quanto a possíveis incidentes de segurança que possam surgir durante o uso da aplicação.

Logo, as interfaces das aplicações *web* devem ser projetadas com critérios específicos que não só facilitem a utilização por partes de usuários, como também, protejam informações e dados inseridos e manipulados pelos usuários destas aplicações. Desta forma, estes sistemas seguros, também chamados de softwares seguros, devem oferecer ao usuário uma alta percepção de segurança, bem como, satisfazer às necessidades dos seus clientes tornando-se mais fáceis de utilizar.

Segundo [3], o desenvolvimento de um software seguro é um processo complexo e demorado que visa acoplar fatores frequentemente concorrentes como funcionalidade, escalabilidade, simplicidade e adaptação ao mercado. Pesquisas de Engenharia de Software têm se concentrado em requisitos não-funcionais tais como estabilidade, desempenho, tolerância a falhas e segurança, conforme citado por [3].

Segundo [4], a segurança da informação e sua complexidade têm permitido novas ameaças; e não é só a natureza que pode causar catástrofes de proporções globais mas também a batalha dentro do campo cibernético.

Segundo [5], devido ao grande sucesso das aplicações *web,* áreas como negócios, comercio eletrônico e sites governamentais (*e-gov*) têm utilizado esses sistemas para aproximar o público alvo das organizações. Os serviços ofertados mostram a organização, facilidade e eficiência da ferramenta. Contudo, caso as atividades destas aplicações não sigam regras de usabilidade e segurança; vulnerabilidades podem ser exploradas dentro destas aplicações proporcionando falta de credibilidade nas instituições.

Sendo assim, destacam-se nesse cenário propor um método para equilibrar requisitos de usabilidade e segurança de software, contribuindo para a proteção contra ataques cibernéticos e para a melhoria da qualidade destes softwares. Este método proporciona segurança, gerando credibilidade para as instituições que a utilizam, além de priorizar a satisfação dos usuários durante a confecção da aplicação, utilizando *design* centrado no usuário. Para isto, o método do Desdobramento da Função de Qualidade de Software (SQFD) pode ser derivada para atendera esta necessidade. O Moderno QFD para Software (SQFD) com ênfase em usabilidade e segurança é utilizada neste trabalho de pesquisa denominado de método USASEC (do inglês *USAbility and SECurity*).

1.2 Motivação

A partir da década de 90, ataques realizados contra a rede mundial de computadores dependiam basicamente dos conhecimentos técnicos dos atacantes. Logo, o potencial agressor deveria ter um conhecimento avançado do sistema operacional e da aplicação que seriam os alvos para ganhar acesso e, então, realizar sua atividade maliciosa.

Tendo em vista que o foco principal, nesta época, era manter a efetividade das comunicações entre os *hosts* da rede, ainda havia uma grande relação de confiança entre as máquinas conectadas. Um exemplo de ataque a este tipo de operação pode ser encontrado em [6].

Mesmo nos tempos atuais, a segurança da informação de instituições públicas e privadas, referente as suas redes e softwares, ainda representam uma preocupação essencial. Apesar de existirem muitas ferramentas e dispositivos para se realizarem ações de segurança da informação [7], muitas organizações sofrem com incidentes de segurança, anualmente, conforme [8] . Ainda mais quando elas acreditam que a informação disponibilizada na sua aplicação *web* não tem valor para um provável invasor.

Soma-se a isso, a facilidade de automatização de artefatos cibernéticos para realizar ataques, chamados de *malware* que fez com que várias ferramentas de produção de ataques e exploração de vulnerabilidades estivessem disponíveis para qualquer indivíduo com acesso à Internet. Isto causou um aumento considerável de ataques não direcionados e, com o passar dos anos, aumento tambem a sofisticação dos ataques, apesar da diminuição de conhecimento dos invasores.

A falta de direcionamento desses ataques, em muitos dos casos, não surte efeito nenhum, tendo em vista que o artefato cibernético, *malware*, explorará qualquer máquina que esteja na

Internet, independentemente de ela possuir vulnerabilidade ou não. Sendo assim, o ataque só será efetivado quando o *malware* conseguir alcançar um computador que possui uma vulnerabilidade, obtendo, assim, seu objetivo de acessar informações privadas ou de infectar outros computadores.

Segundo [4], dois casos de ataques cibernéticos mostram os riscos de redes de computadores e telecomunicações: o caso do *malware Stuxnet*, detectado em 2010, afetando os sistemas de controle de supervisão e aquisição de dados de instalações nucleares (SCADA) no Irã e o roubo de dados sensíveis em instituições bancárias.

Segundo [9], cerca de 60% dos ataques cibernéticos na Internet têm como alvo aplicações *web*. Os resultados sugerem que a complexidade dos ataques não evoluiu significativamente e muitos destes ataques estão relacionados ao não conhecimento dos desenvolvedores ou a sua incapacidade de criar contramedidas para se opor a estes ataques. Ainda, segundo [9], houve um crescimento do número de ataques devido à evolução de ferramentas de desenvolvimento *web*. Contudo, o não preparo dos desenvolvedores trouxe, concomitantemente, um aumento dos índices de ataques.

No Brasil, de acordo com [10], as espionagens em organizações governamentais estão ocorrendo desde de 2013. Estas têm interesses políticos, econômicos e financeiros e colocam em risco a Segurança Nacional.

De acordo com o Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil [8], no ano de 2015, as interfaces web ficaram na terceira posição de incidentes de segurança da informação, conforme ilustra a Figura 1.1. A maior parte destes ataques foram provenientes do próprio País, conforme Figura 1.2.

Ainda, de acordo com a revista Forbes [11], uma nova onda de crimes cibernéticos (*cibercrime*) vem impulsionando o investimento no mercado de Internet das Coisas, *Internet of Things* (IoT), passando uma perspectiva de incremento de 170 bilhões de dólares de recursos até 2020 para este setor.

Conforme a Figura 1.1, as ações de escaneamento de porta (*scan*) são os incidentes que mais ocorrem no Brasil. Contudo, apenas encontrar a "porta aberta" de entrada não significa que esta vulnerabilidade será explorada. Mas, os incidentes de fraudes, que incluem fraudes as aplicações *web* e incidentes web são os incidentes que mais impactam no ciberespaço. Mostrando como os cibercriminosos têm se comportado durante a execução dos seus crimes.

Estes cibercriminosos são beneficiados, por essa nova modalidade de crime, pelo fácil acesso à rede e baixo risco de identificação, conforme [12]. Estes se utilizam de técnicas básicas, derivadas das ilegalidades já cometidas no mundo físico, tais como falsificação de

identificação, atos de vandalismo (*defacement*), estelionato e roubo de informações, para obtenção de algum tipo de benefício.

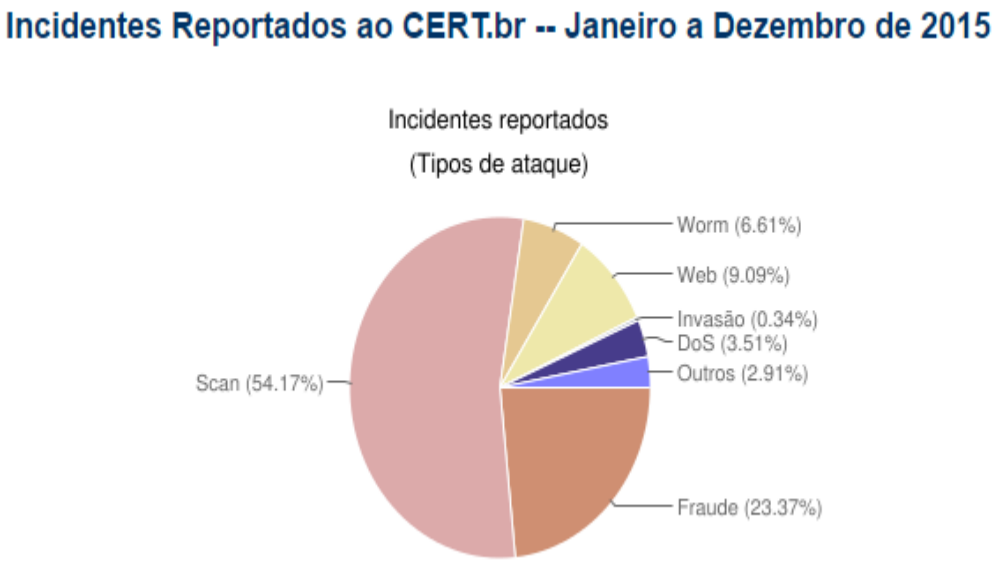


Figura 1. 1 - Reporte de Incidentes de Segurança da Informação 2015 [8].

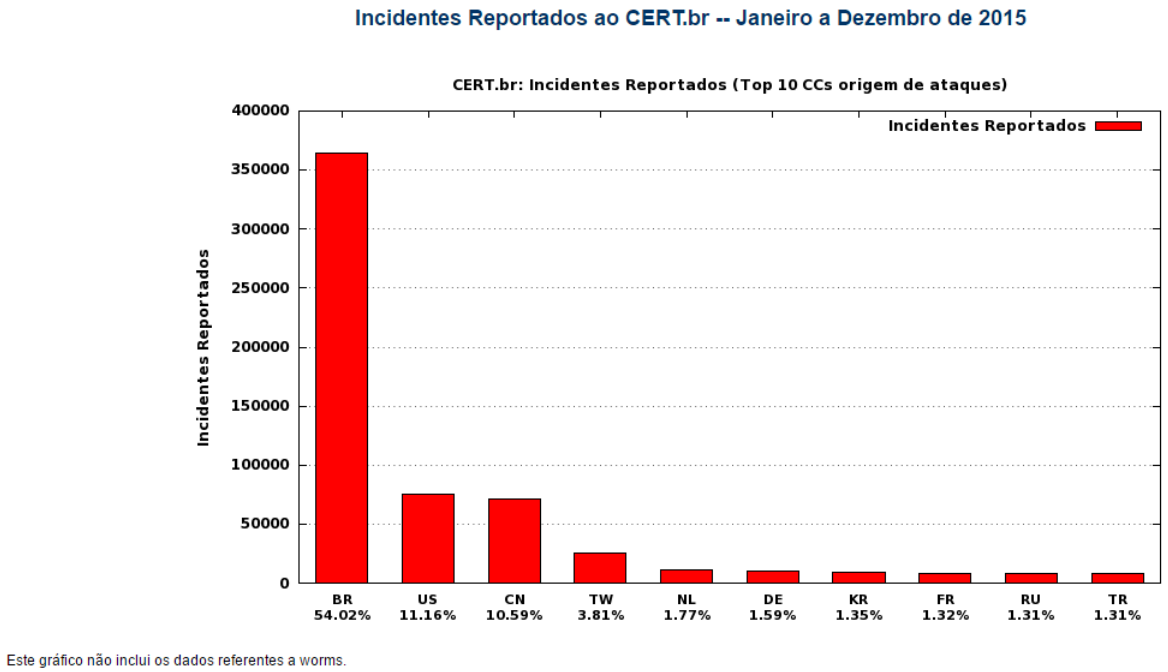


Figura 1. 2 - Reporte de países origens de incidentes de ataque [8].

O Centro de Estratégia e Estudos Internacionais, *Center for Strategic and International Studies* (CSIS), junto com a McAfee, empresa do ramo de antivírus, publicou, segundo [12], uma estimativa de quanto são os custos dos crimes cibernéticos dentro de um grupo de países, como mostrado na Figura 1.3. O estudo comprova a necessidade de se avaliar o custo/benefício

de investimentos na área de segurança cibernética em relação aos prejuízos por Produto Interno Bruto (PIB) do País.

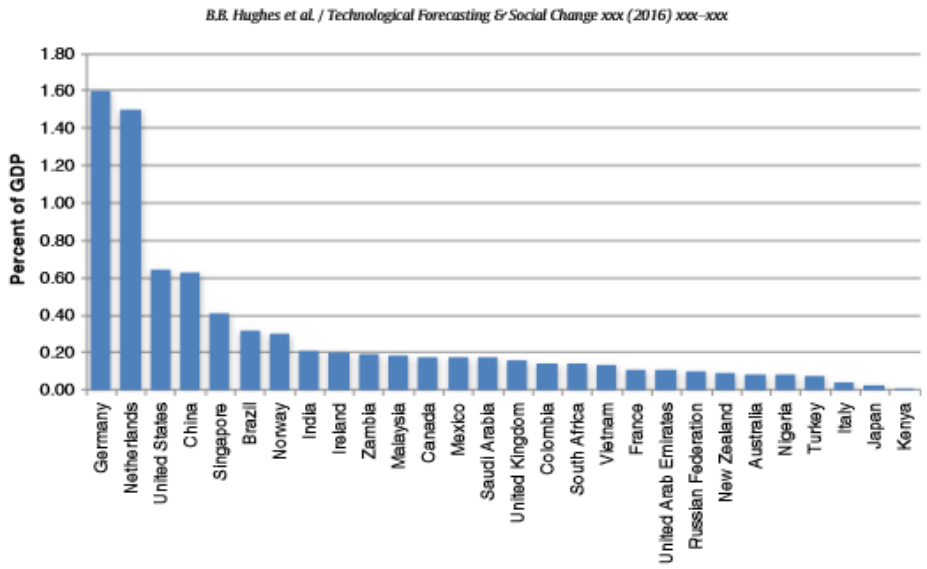


Figura 1. 3 - O custo de crimes cibernéticos e espionagem expresso em porcentagem do PIB [12].

No Brasil, o setor cibernético faz parte da Estratégia Nacional de Defesa (END) e engloba as capacitações que se destinarão ao mais amplo espectro de usos industriais, educativos e militares.

Para se contrapor a esta ameaça no espaço cibernético e de acordo com a END [13], cabe ao Exército Brasileiro (EB) as capacitações e os instrumentos cibernéticos necessários para assegurar as comunicações entre os monitores espaciais, aéreos e a força terrestre.

Ainda segundo a END, cabem as seguintes prioridades ao setor cibernético:

- " (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas; ";
- " (c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão

elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética; "; e

- " … o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra-ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento…"

Para cumprir esses objetivos, o EB possui o Centro de Defesa Cibernética e o recentemente criado Comando de Defesa Cibernética (ComDCiber), os quais possuem militares da três Forças Armadas (Exército, Marinha e Aeronáutica). Além disto, está sendo criada a Escola Nacional de Defesa Cibernética (ENaDCiber) para fomentar a pesquisa científica voltada para o setor, envolvendo a comunidade acadêmica nacional e internacional.

Por fim, o aumento desses incidentes de segurança da informação e sua expansão para aplicações *web* do Estado como: banco central, forças armadas e de utilidade pública podem desacreditar o Estado e suas organizações, além de trazer grande prejuízo ao erário público. Sendo assim, cresce de importância se definir as aplicações *web*, de acordo com a necessidade do seu usuário, com intuito de se expor a menor quantidade de informações sensíveis possíveis. Bem como, oferecer um serviço seguro, confiável e usável.

Neste sentido, a principal motivação deste trabalho foi a necessidade existente de se aplicar um método que aumente a segurança das aplicações web e que atenda às necessidades dos seus usuários, integrando requisitos de usabilidade e segurança priorizados para analisar o impacto do desequilíbrio entre os requisitos de usabilidades solicitados pelo usuário, e os requisitos de segurança realizados pela equipe técnica da aplicação.

1.3 Problema de Investigação

No ciberespaço, segundo [13], conceitos fundamentais de segurança da informação e comunicações como: confidencialidade, disponibilidade e autenticidade devem ser inseridos em tecnologias que permitam o planejamento e a execução de defesa cibernética no âmbito do Ministérios da Defesa (MD) e que contribuam com a segurança cibernética nacional, observando o aspecto de acesso sem fronteiras apresentado pela Internet. A falta destas características desenvolve as condições para ocorrência de crimes virtuais pois permitem aos cibercriminosos a realização de seus delitos de forma anônima e sem a certeza de sua localização prévia. Estas possibilidades oferecem a um possível país invasor o "*álibi*" de

realizar ataques de outros territórios através do comprometimento de máquinas infectadas em redes “estrangeiras”, onde as leis são menos restritivas quanto à identificação destas atividades.

Nesse intuito, em operações militares ou ainda em tempo de paz, a proteção cibernética deve ser uma preocupação constante para as ações de cibernéticas e uma necessidade constante para as Forças Armadas.

Como abordado na seção 1.2, a credibilidade de um sistema *web* está conectada a sua usabilidade e segurança. Ou seja, para garantir que o usuário final perceba que a aplicação tem credibilidade é necessário que ela atenda estes requisitos. Assim, a credibilidade não deve levar em consideração apenas os aspectos de usabilidade, satisfação do usuário, mas também o de segurança. Uma vez que a segurança garantirá que informação transmitida terá seus princípios de informação atendidos.

De acordo com [14], existem 35 fatores que têm efeito sobre a percepção de confiabilidade da informação na *web* que o usuário está utilizando. Entre eles os considerados mais importantes pelo autor são: a identidade da informação (segurança do órgão que enviou a informação); a relevância e oportunidade; e a experiência do usuário final (usabilidade). Ainda, a comunicação do risco, em relação à segurança cibernética, deve ser considerada a melhor forma de se prevenir estes riscos aos usuários, a fim de promover a melhor tomada de decisão. Contudo, segundo o autor, esta área é relativamente nova e depende de investigações mais profundas.

Segundo [14], o conceito de confiabilidade para uma aplicação *web* continua vago. Esta aplicação seria confiável por quem? Ou para fazer o quê? Assim, o conceito de confiabilidade está ligado a quanto o usuário pode confiar no software e se a aplicação se comportar de acordo com as expectativas e experiências dos usuários, segundo [15]. Mesmo assim, segundo o autor, existe um elemento que não pode ser desconsiderado para gerar confiabilidade no sistema, o modelo mental pensado pelo usuário. Este modelo determina o quanto agradável esta aplicação é para o indivíduo que a utiliza e como sua interação com o sistema é produtiva.

Ainda assim, para as aplicações *web*, no que diz respeito a percepção da segurança cibernética, existem muitos fatores que influenciam a decisão do usuário em tomar determinada decisão, durante as atividades *online*. Entre os diversos estudos, o de [14] afirma que existem seis fatores centrais: conhecimento; impacto; severidade; controlabilidade; possibilidade; e consciência. Já segundo [16], autor que apoia algumas destas dimensões de percepção dos riscos de um indivíduo relacionado as ameaças à segurança *online*, existem quatro dimensões comuns para julgar segurança, onde os autores concordam: capacidade de controlar ou evitar o risco (controlabilidade); medo das consequências (possibilidade); desconhecimento de risco

(conhecimento); e consequências ou impactos dos riscos (impactos). A diferença entre os autores se dá em relação a como se medir a percepção da segurança cibernética, ou seja, como colocar em métricas cada um destes fatores.

Segundo [17] e [18], um sistema de medição da percepção do risco de segurança foi criado para avaliar a percepção do usuário quanto ao nível de segurança cibernética em que se encontra o software. Ele foi baseado em dois fatores: o conhecimento do indivíduo sobre o risco e as consequências do risco.

Contudo, segundo [19], em termos de auxiliar na tomada de decisão para apoio a percepção da segurança cibernética, os fatores que determinam a decisão da concessão do risco de segurança entre usuário/indivíduo são: a percepção de risco, a habilidade de segurança e a cultura do indivíduo. Desta forma, o primeiro e terceiro fatores indicam uma responsabilidade sobre o indivíduo e suas atitudes frente às atividades que está realizando na aplicação. Já o segundo fator está relacionado a quanto de segurança cibernética a equipe do projeto do software implementou no sistema.

Ainda segundo [20], diversos fatores humanos foram identificados como influenciadores na tomada de decisão na comunicação da segurança cibernética. Entre eles estão: a tendência da satisfação das necessidades dos seres humanos (escolher alternativas rápidas e "suficientemente boas" não necessariamente as melhores), sucumbir a preconceitos cognitivos (como exemplo são as heurísticas de representatividade e viés de resposta), enfrentar pressões de tempo e a cegueira desatenciosa.

Contudo, considera-se que os usuários frequentemente não pensam nos riscos que estão correndo, a partir de tomadas de decisões erradas. Segundo [21], os usuários tendem a ser desmotivados a pensar na segurança da informação, durante a utilização da aplicação *web*. Desmotivando-os a considerar questões de segurança, transfere-se a responsabilidade de orientar e avaliar tarefas que devem ter uma maior atenção quanto a proteção cibernética para a equipe do projeto de software. Para estes usuários/indivíduos as perdas geralmente são percebidas desproporcionalmente aos ganhos em termos de segurança.

Estudos mais recentes [22], [23] e [24] indicam que a percepção do usuário quanto a comunicação da segurança cibernética envolve critérios chaves como: criação do projeto da interface, de acordo com os modelos mentais das tarefas que serão realizadas; estabelecimento de cores-padrões para chamar a atenção do usuário; usar ícones como indicadores visuais; explicitar com palavras os níveis riscos; e utilizar uma taxonomia coerente e significativa para o indivíduo.

Segundo a Associação Brasileira de Normas Técnicas (ABNT) na sua NBR ISO/IEC 12207, conforme [25], que versa sobre Engenharia de Requisitos e o seu processo no ciclo de vida para software, na fase de processos técnicos devem ser executadas tarefas e atividades para a definição dos requisitos dos *Stakeholders*. Estas atividades têm por objetivo descrever os requisitos do sistema, de acordo com a perspectiva do contratante, ou seja, o cliente.

Para isso, as especificações do sistema devem descrever: as funções e capacidades do sistema; os requisitos do usuário, da organização ou do negócio; os requisitos de segurança, proteção, engenharia de fatores-humanos (ergonômicos), de interface, operações e manutenção; restrições de *design*; e requisitos de qualificação, grifos do autor.

Acrescenta-se que a Norma ISO/IEC 25030:2008, conforme [26], que versa sobre os requisitos de qualidade de software, afirma que se os requisitos de qualidade de software não estiverem claramente explícitos eles podem ser interpretados, implementados e avaliados de formas diferentes, de acordo com a pessoa.

Ainda segundo a norma em questão, a não observância dos requisitos pode resultar; em software de qualidade inferior e que não atende às expectativas dos usuários; em usuários, clientes e desenvolvedores insatisfeitos; e em tempo e custo adicional para refazer o software.

Assim, verifica-se a importância desses requisitos e que, durante todo o desenvolvimento do projeto da aplicação, caso a "voz do usuário" não for ouvida, isto pode acarretar uma formulação errônea destes importantes requisitos para o software, comprometendo a qualidade do produto final

Sendo assim, será necessário investigar a percepção do usuário quanto aos requisitos de usabilidade, entendida como satisfação, e proteção cibernética para aplicações *web*. Esta deve levar em considerações quais tarefas os usuários/individuo devem realizar na aplicação e qual a melhor maneira de satisfazer suas necessidades (requisitos de usabilidade) sem comprometer a segurança da aplicação. Mas como conseguir um equilíbrio entre requisitos de usabilidade e segurança para aplicações *web*?

De acordo com [28], este conflito consiste no grande número de requisitos para o desenvolvimento de softwares, o tempo exíguo para entrega e recursos limitados. Todos estes fatores cooperam para que os softwares tenham uma baixa qualidade. Desta forma, é necessário um método que possa satisfazer os usuários, de forma eficiente, priorizando requisitos de alto valor. Estes requisitos devem ser priorizados para aproveitar-se dos melhores esforços, tempo e recursos; e são estes que irão impactar significativamente o produto final de software.

De acordo com a Figura 1.4, é necessário realizar uma priorização dos requisitos que são elencados para uma aplicação. Grande parte do esforço gasto em fazer um grande trabalho

com muitas exigências de baixo valor não tem grande impacto na satisfação do cliente. Contudo, segundo a método QFD para Software (SQFD), se concentrarmos nossos esforços disponíveis nos requisitos mais importantes, teremos a possibilidade de satisfazer o cliente de forma mais pontual.

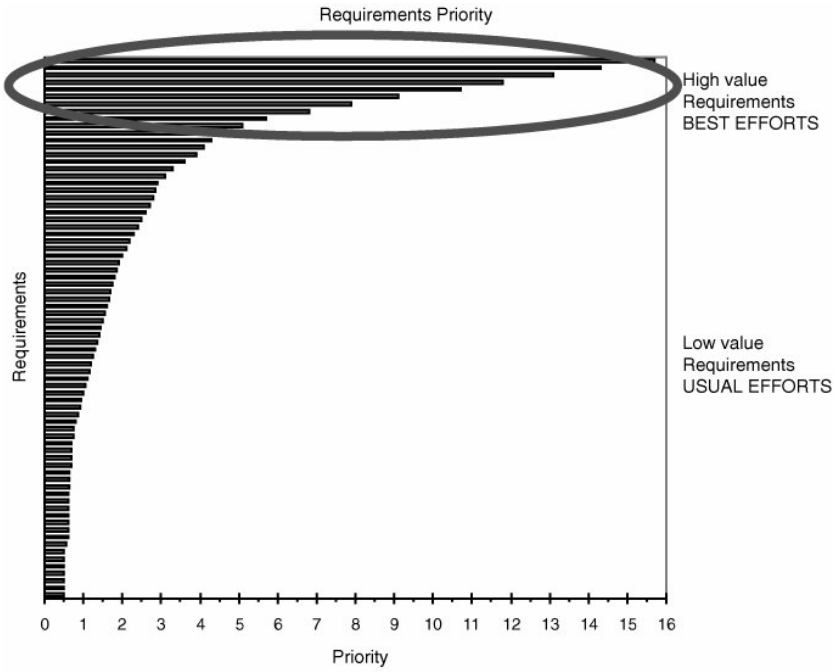


Figura 1. 4 - Medição precisa da prioridade dos requisitos revela uma distribuição de Pareto [28].

Isto não significa que todos os requisitos não devam ser atendidos. A priorização dos requisitos servirá para manter foco e recursos maiores na necessidade do usuário, ou seja, nas principais tarefas do usuário, durante todo o desenvolvimento do ciclo de vida do software. E, ainda, atender aos princípios de segurança de informação, a fim de proporcionar uma proteção cibernética aos indivíduos que utilizam o sistema. Mas para isto, é necessário propor um método que possa analisar a complexidade da relação entre a usabilidade e segurança para cada aplicação *web*.

Desta forma, através do método proposto neste trabalho, chamado método USASEC, é possível investigar uma proposta de integração de requisitos de usabilidade e segurança da informação. Este método utiliza para o desenvolvimento de software, o Moderno Desdobramento da Função de Qualidade de Software (QFD para Software), com ênfase em usabilidade e segurança.

1.4 Objetivo

Este trabalho de pesquisa tem por objetivo principal investigar, conceber, e aplicar um método para avaliação, priorização e integração de requisitos de usabilidade e segurança de aplicações *web* visando melhorara a qualidade do produto, alinhando a necessidade do usuário com os objetivos estratégicos da organização, e o proteção cibernética com a observância de vulnerabilidades que podem atingir a aplicação.

Com este objetivo principal, os seguintes objetivos específicos são definidos:

1) Identificar a estratégia da organização, em relação à utilização da aplicação *web*, como estratégia de negócio. Ou seja, entre as aplicações *web* da organização, qual é a alinhada com o objetivo estratégico da organização;

2) Identificar quais os principais segmentos de usuários que devem ser atendidos;

3) Criar um modelo de aplicação web para ser analisado pelo segmento de usuário que se pretende analisar. Caso, a aplicação *web*, já não esteja em fase de avaliação e entrega;

4) Coletar, através de uma pesquisa exploratória no ambiente onde a aplicação vai ser empregada, um processo de avaliação de usabilidade em percurso pluralístico, buscando quais as melhorias focadas na satisfação do usuário precisam ser adicionadas na aplicação alvo;

5) Confeccionar a tabela com a voz do usuário, em acordo com uma equipe multidisciplinar da aplicação, para filtrar as ideias de acordo com suas similaridades em niveis;

6) Organizar, com a confecção de uma diagrama de afinidade, o grande número de ideias da pesquisa exploratória em *cluster* de usabilidade, de acordo com os conceitos de [30] sobre usabilidade. Assim, é possível colocar metas de usabilidade, como critérios, para cada ideia transformando-as em requisitos, subcritérios;

7) Confeccionar um diagrama de hierarquia, com uma equipe multidisciplinar da aplicação, para facilitar a visualização dos critérios e subcritérios organizados;

8) Priorizar os requisitos de usabilidade, através de um formulário de priorização de requisitos de usabilidade, utilizando o Processo de Análise Hierárquica (AHP) e classificar os requisitos de usabilidade priorizados, no passo anterior, utilizando os conceitos de [31] e de [32]; e

9) Classificar os requisitos de segurança, de acordo com a análise da equipe multidisciplinar. Além disto, integrar quais requisitos mais impactam quanto a usabilidade e segurança, aplicando o conceito do SQFD com ênfase em usabilidade e segurança, de acordo com [28].

1.5 Alcances e Limites

O método concebido e aplicado neste trabalho limita-se a utilizar conceitos de qualidade de software, SQFD, com ênfase em características técnicas de usabilidade e segurança; abordando nestes conceitos os princípios de segurança da informação e vulnerabilidades para aplicações *web* e os conceitos de [30] para usabilidade.

Por existirem muitas vulnerabilidade que podem incidir sob uma aplicação *web*, as vulnerabilidades escolhidas nas questões técnicas são as representas em [7], além, das avaliadas como pertinentes pela equipe técnica que avalia a aplicação. Após realizado a proposta do método USASEC, teremos um comparativo de como o método analisa e prioriza os requisitos dos softwares, de acordo com os seus critérios de usabilidade e segurança elencados.

Existem vários métodos para desenvolver o ciclo de vida do software. Não cabe, durante esta pesquisa, a discussão dos melhores métodos e técnicas de desenvolvimento propostos para o ciclo de vida da aplicação como: método cascata, técnica de vias paralelas de projeto de interação e implementação, espiral ou o método Ágil. O foco principal está relacionado ao conceito de usabilidade no *Design* Centrado no Usuário, ou mais conhecido na literatura como *User Centered Design* (UCD), e da Interação Homem-Computador da [30]; e como os aspectos de segurança podem ser integrados aos de usabilidade para dar qualidade a aplicação. Contudo, fica evidente que, para o desenvolvimento ágil e suas equipes de usabilidade e segurança, este método pode ser de grande importância na avaliação de requisitos concorrentes para satisfação destas equipes.

Assim, este trabalho pretende oferecer uma contribuição técnica de quais requisitos de usabilidade e segurança devem ser priorizados através de uma hierarquização. Por conseguinte, quais podem criar um maior impacto sobre o sistema. Indicando, portanto, quais requisitos mais influenciam na satisfação do cliente (usuário) e quais podem ser atendidos sem comprometer a segurança do sistema.

1.6 Resultados Esperados

Ao seu término, esta pesquisa deverá ser capaz de propiciar:

1) Enumerar, através de uma pesquisa exploratória no ambiente onde o software vai ser empregado, quais as ideias para melhorias que o usuário precisa na aplicação e como classificá-las;

2) Produzir um diagrama de afinidade, em concordância de uma equipe multidisciplinar da aplicação, de acordo com os conceitos de [30] que aborda as metas de usabilidade ;

3) Construir um diagrama hierarquico dos critérios e subcritérios utilizando os conceitos de [31] e de [32];

5) Efetuar a priorização dos requisitos de usabilidade e segurança da informação; e

6) Identificar quais requisitos mais impactam quanto a usabilidade e segurança aplicando o conceito da casa da qualidade do Moderno SQFD com ênfase em usabilidade e segurança.

1.7 Organização da Dissertação

Neste Capítulo 1, apresentou-se uma introdução ao tema desta pesquisa sobre o método proposto, USASEC, sua contextualização, motivação, objetivo, alcance e limitações e resultados esperados.

No Capítulo 2 descrevem-se as definições de usabilidade para aplicações web, seus métodos de avaliação e requisitos de diálogos; a definição de segurança da informação e seus princípios, assim como, as melhores práticas e sua relação com a proteção cibernética. Ainda são abordadas as definições e técnicas para a confecção do diagrama de afinidade dos requisitos de usabilidade e o Método de Análise Hierárquica Clássico (AHP) e o Multiplicativo (MAHP). Por fim, ainda neste, são abordadas as definições do QFD e do moderno QFD para Software (SQFD), aplicado na fase final do método USASEC para a análise dos requisitos.

No Capítulo 3, encontra-se a descrição do método proposto neste trabalho de pesquisa, com seus principais fundamentos e considerações; objetivando a avaliação de requisitos de softwares seguros, método denominado USASEC.

O estudo de caso realizado com aplicação do método proposto é descrito no Capítulo 4.

No Capítulo 5, encontram-se as análises e as discussões sobre os resultados obtidos nos passos principais do método proposto, USASEC, e a efetividade do método proposto na aplicação do estudo de caso realizado nesta pesquisa.

Por fim, no último Capítulo serão apresentadas as conclusões especificas, principais contribuições, recomendações e sugestões de trabalhos futuros.

2 Referencial Teórico

Este Capítulo se encontra organizado em cinco seções que fornece um alicerce conceitual para o entendimento da pesquisa. A primeira seção apresenta conceitos de usabilidade com as principais definições investigadas na literatura. A segunda seção aborda os conceitos de segurança da informação, suas práticas e ações e a relação com a proteção cibernética. A terceira seção mostra uma síntese do método de Desdobramento da Função de Qualidade de Software. A quarta seção denota os conceitos do diagrama de afinidade e na última seção, seção 5, encontra-se uma sinopse do processo de análise hierárquica AHP e suas variações.

2.1 Definições de Usabilidade

O conceito de usabilidade se relaciona, principalmente, com a facilidade de uso de um produto e a satisfação do usuário em relação a este. A relação entre o usuário e um sistema começou na década de 30 onde estudos sobre ergonomia passaram a ser realizados. O termo ergonomia foi criado pelo inglês K.F.H. Murrel, citado pela primeira vez em 1949, e tem por definição uma disciplina que se preocupa em entender as interações entre os seres humanos e os outros elementos de um sistema, conforme [35].

Ainda, segundo [36], ao focarmos na usabilidade, economiza-se tempo e criam-se softwares que atendem a necessidade do usuário. Segundo o autor, existe uma confusão entre Design Centrado no Usuário (DCU) e usabilidade. Para ele, a usabilidade, referenciada como fatores humanos, corresponde ao estudo de como os seres humanos se relacionam com qualquer produto. Já a Interação Homem-Computador (IHC) está baseada na usabilidade mas foca no modo como os seres humanos se relacionam com os produtos ligados a computação. Já o DCU surgiu do IHC e consiste em uma metodologia de design de software para desenvolvedores e designers, conforme Figura 2.1.

Embora, é razoável dizer que a prática do DCU garante que sua aplicação mantenha uma boa usabilidade ao colocar o usuário como centro do processo de desenvolvimento. Sendo assim, com a prática do DCU, as ambiguidades dos requisitos são eliminadas e as necessidades centrais dos usuários são satisfeitas. Já o conceito atual de Experiência do Usuário (do inglês *User Experience* – (UX)) afirma que é necessário sintetizar toda a experiência do usuário com o software, ou seja, não engloba apenas as funcionalidades, mas também medidas subjetivas de como a aplicação e cativante e agradável. Para o UX, uma aplicação é maior do que a soma de

suas partes, ou seja, considera-se o nível de experiência que o usuário possui com certos tipos de aplicações e dispositivos.

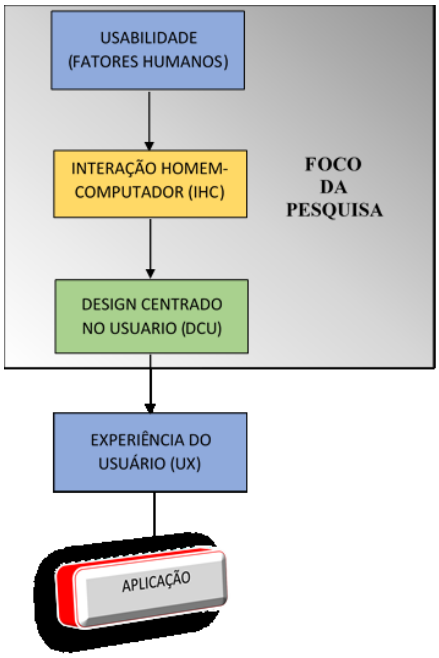


Figura 2.1 - Relação entre usabilidade, IHC, DCU e UX, adaptado de [36].

A interação é definida por [30] como um processo de comunicação entre pessoas e sistemas interativos. Para ela, entendendo a interação será mais fácil projetar interfaces. Já interfaces são a parte de um sistema computacional com a qual a pessoa entra em contato físico, perceptivo e conceitualmente. Em outras palavras, design de interação significa criar experiências que buscam aperfeiçoar e estender a maneira como as pessoas trabalham, se comunicam e interagem com o computador

Ainda, segundo [30], a definição de usabilidade vem como um fator que assegura que produtos se tornem mais fáceis de usar, eficientes e agradáveis e divide-se este conceito em metas de usabilidade como:

- Utilidade - refere-se a medida na qual o sistema propicia o tipo certo de funcionalidade, de maneira que os usuários possam realizar aquilo de que precisam ou que desejam.;
- Eficácia - se refere a quanto um sistema e bom em fazer o que se espera dele.;
- Eficiência - se refere a maneira como o sistema auxilia os usuários na realização de suas tarefas.;
- Segurança – implica em proteger o usuário de condições perigosas e situações indesejáveis;

- Capacidade de Aprendizagem (*learnability*) - refere-se a quão fácil e aprender a usar o sistema.; e
- Capacidade de memorização (*memorability*) - refere-se à facilidade de lembrar a utilização de um sistema, depois de já se ter aprendido como fazê-lo - algo especialmente importante para sistemas interativos que não são utilizados com muita frequência.

Contudo, segundo [37], a definição de usabilidade, não representa apenas uma propriedade singular ou unidimensional de uma interface, mas sim um conjunto de componentes associados a atributos.

Ainda, segundo [34], a qualidade dos softwares são divididas em seis características: **usabilidade**, funcionalidade, confiabilidade, eficiência, manutenibilidade e confiabilidade. Para cada uma destas características, existem sub características que podem ser medidas. Para a usabilidade, como uma característica de qualidade, entende-se como um conjunto de atributos que estão relacionados ao esforço para o uso do software por um conjunto determinado de indivíduos. As definições dos atributos de usabilidade são:

- Operacionalidade – atributo que mede o esforço do usuário para realizar uma operação ou controle no sistema;
- Conformidade – atributo que verifica a consistência as normas, regulamentações previstas, convenções e descrições similares relacionadas ao sistema. Este também considera harmonia e padrões e convenções para uso de portabilidade;
- Atratividade – atributo subjetivo que avalia a satisfação do usuário, durante o uso;
- Apreensibilidade – facilidade de aprendizado (*Learnability*) – atributo que evidência o esforço do usuário para aprender suas funcionalidades e compreender suas entradas, saídas e controles de operação; e
- Inteligibilidade – atributo relacionado com o esforço relacionado a reconhecer conceitos lógicos e aplicações.

Já para [38], a norma que trata especificamente de sistemas *web*, a definição de usabilidade é a medida na qual um produto pode ser usado por usuários específicos para alcançar objetivos específicos com eficiência, eficácia e satisfação em um contexto de uso especifico. Os objetivos de eficiência e eficácia são comuns aos de [30], a eficiência com foco em atingir objetivos com acurácia e abrangência, e a eficácia a realização de tarefas com

qualidade nos resultados. Logo, o objetivo de satisfação é diferente do [37] pois está ligado a ausência de desconforto e a presença de atitudes positivas para com o uso de um produto pois, ao se utilizar o software, o usuário deve se sentir satisfeito.

Observa-se que em todos os conceitos, as metas de satisfação do cliente, eficácia e eficiência estão presentes. Contudo, as demais vêm como complemento para expressar as necessidades dos requisitos expressos pelos usuários. Para o objetivo da pesquisa foi utilizado este conceito pois, conforme a citada, a usabilidade está diretamente ligada ao design de interações entre o usuário e o sistema.

Para isso, ainda de acordo com [30], como parte do processo de entender as necessidades dos usuários para projetar um sistema interativo, é necessário que estes requisitos verbais expressos pelos usuários (chamadas de verbatims) sejam consideradas como metas de usabilidade. As metas de usabilidade são destinadas as práticas de trabalho, ou seja, são altamente relevantes para empresas e organizações que estejam introduzindo ou atualizando aplicações para *desktop* e sistema em redes. Observando as características destas metas, espera-se o aumento da produtividade, melhorando e aperfeiçoando a maneira de realizar o trabalho, conforme [30].

Por conseguinte, adotando-se o conceito de [30], estas metas de usabilidade além de guiar empresas no que diz respeito a questões especificas, podem se tornar **critérios de usabilidade**. Estes critérios podem permitir que a usabilidade possa ser avaliada, mostrando como podemos aprimorar (ou não) o desempenho de usuário.

Entretanto, apesar de existirem critérios para enquadrar funções de usabilidade, é necessário utilizar métodos científicos para realizar a avaliação de usabilidade.

2.1.1 Métodos de Avaliação de Usabilidade

Existem diversos métodos de avaliação de usabilidade de softwares. Eles enquadram-se em: avaliações empregando métodos de inspeção e aquelas que envolvem a participação de usuários.

Segundo [39] os métodos de avaliação de usabilidade estão divididos em três:

- Métodos Analíticos ou de Inspeção;
- Métodos Empíricos ou de Teste com Usuários; e
- Outros métodos.

A Figura 2.2 mostra as divisões dos Métodos de Avaliação de Usabilidade Analíticos e Empíricos considerados como relevantes na elaboração do métodoa ser proposto nesta pesquisa.

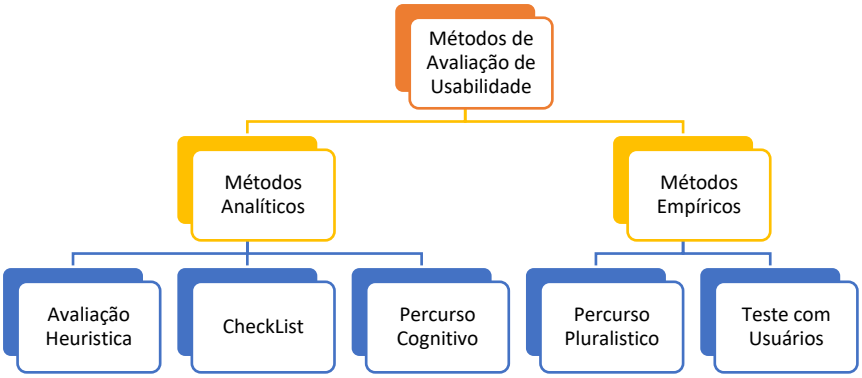


Figura 2.2 – Divisão dos métodos de avaliação de usabilidade [39].

Apesar de existirem equipamentos especializados (*eye tracking*) em realizar avaliações de usabilidade como, por exemplo, sensores que conseguem a mediação dos movimentos dos olhos de um determinado usuário ao olhar para as telas e interagir com um sistema, conforme [27], permitindo identificar como o usuário se comportar ao olhar para as telas e quais ele dispôs maior atenção; nesta pesquisa utilizaremos o método mais simples e econômicas prescritos por [40] que utilizam equipamentos comuns como computadores, papeis de anotações ou até câmeras convencionais (*webcam*), se for o caso, para observar e coletar dados de usabilidade expressos pelos usuários. Podendo ser aplicados em um dia ou menos, para se ensinar em até 4 horas, envolvendo de 5 a menos avaliadores.

2.1.1.1 Método Analitico de Avaliação de Usabilidade por Percurso Cognitivo

Também conhecido como *Cognitive Walkthrough*, o método por percurso cognitivo, método analítico, é aquele onde um analista assume o lugar do usuário real do sistema para realizar uma série de ações, ou seja, as possíveis tarefas que os usuários poderiam realizar. Assim, seria possível avaliar a capacidade do sistema de suportar cada uma destas tarefas, buscando-se identificar as dificuldades ou barreiras de interação com o sistema, conforme [41].

Um fator crucial para este tipo de avaliação é a definição e confecção de cenários; uma vez que o avaliador não consegue entender corretamente os detalhes dos cenários a efetividade da avaliação pode ser comprometida. O método repousa em quatro passos que funcionam como um guia da análise: definição da tarefa, verificação das opções de ação, definição da ação e avaliação do *feedback*.

2.1.1.2 Método Analítico de Avaliação de Usabilidade por *Checklists*

Ainda, como método de avaliação de usabilidade analítico, o método por *checklists*, segundo [42], forma uma lista de verificações para diagnosticar problemas gerais no uso das interfaces. Diferente das avaliações feita por percurso cognitivo, onde a definição e criação dos cenários e fundamental para o sucesso da avaliação, no método *checklists* a capacidade de criar as listas de verificação decretam a qualidade da avaliação.

Um fator positivo deste método é que ele, devido a facilidade de realizá-lo, oferece a possibilidade de qualquer indivíduo envolvido no projeto do software conseguir realizar a avaliação. Isso ocorre devido a não necessidade de que os avaliadores tenham conhecimento profundo de usabilidade. Apesar disso, uma lista com verificações insuficientes pode comprometer a efetividade da avaliação.

2.1.1.3 Método Analítico de Usabilidade por Avaliação Heurística

Esta avaliação foi proposta por [43] com a finalidade de encontrar problemas de usabilidade em projeto e representa um método de engenharia de usabilidade. Nela envolve-se um pequeno grupo de avaliadores na verificação da interface do sistema, de acordo com princípios de usabilidade proposto por [39] como: visibilidade do *status* do sistema, correspondência entre o sistema e o mundo real, controle e liberdade do usuário, consistência e padrões, prevenção de erros, reconhecimento em vez de lembrança, flexibilidade e eficiência de uso, estética e design minimalista, auxilio dos usuários em reconhecer, diagnosticar e recuperar-se de erros e, por fim, ajuda e documentação.

Por ser uma avaliação fora de ambiente de laboratório especifico e não necessitar de nenhum software ou equipamento diferenciado, este tipo de avaliação pode ser considerado econômico e rápido. Neste sentido, ele é fácil de aplicar, contudo montar uma equipe de 3 a 5 avaliadores, conforme [37], que tenham uma certa experiência em avaliação de usabilidade pode se tornar um problema.

Atualmente a [38], conseguiu reunir normas e padrões para encontrar problemas de usabilidade para sistemas *web* e garantir a qualidade de software. Esta norma, chamada de requisitos de diálogos, conseguiu comprimir os 10 princípios postos por [39] em sete famílias de problemas a saber: passos adicionais desnecessárias não exigidas como parte de uma tarefa, informação enganosa, informação insuficientes, interface pobres para informar ao usuário, resposta inesperada do sistema, limitações de navegação durante o uso e recuperação ineficiente em caso de erros.

2.1.1.4 Método Empírico de Avaliação de Usabilidade por Percurso Pluralístico

O método por percurso pluralístico, ou método empírico, é uma adaptação ao método por percurso cognitivo, conhecido como método analítico. Nele várias pessoas participam do processo de avaliação e não apenas o analista no papel do usuário. Dentre as pessoas estão: usuários representativos do sistema, desenvolvedores do produto, representantes do cliente do produto e especialista em usabilidade. Para realizar este método são necessários cinco passos, segundo [44]:

1. Formar um grupo pluralístico – tem como primícia ouvir a voz do cliente (usuário). Desta forma, deve-se ouvir as opiniões de todos os envolvidos na utilização, desenvolvimento e confecção do sistema *web*.
2. Utilizar cenários e protótipos – para que todos os envolvidos possam ter acesso ao conteúdo da aplicação é necessário a apresentação de telas na ordem em que os usuários executariam as tarefas;
3. Assumir o papel do usuário – é uma prerrogativa do método que tanto o usuário comum (representativo) como o proprietário ou desenvolver do sistema, durante está fase, considere-se no papel de um usuário, para que não haja viés na pesquisa e justificativas das dificuldades que foram encontradas pelos outros participantes;
4. Anotar as decisões – nesta pesquisa os participantes responderam um questionário com as anotações realizadas logo após o uso da aplicação. Portanto, de forma individual, cada um dos usuários do grupo pode expressar suas dificuldades em cada uma das telas e tarefas do sistema; e
5. Propiciar aos usuários comuns (representativos) a possibilidade de falar primeiro – após a realização de passo anterior, o grupo se reuni para discutir as necessidades de melhorias na aplicação. Neste momento, os usuários representativos são ouvidos primeiros para que eles possam expressar suas necessidades e considerações.

Uma das vantagens deste método e contribuir para uma aproximação entre os desenvolvedores, proprietários e principais clientes da aplicação, facilitando a chegada de soluções consensuais entre todas as partes envolvidas.

2.1.1.5 Método Empírico de Avaliação de Usabilidade por Teste com Usuários

O método de teste com usuário consiste na observação individual dos usuários durante a realização de tarefas no sistema. É considerado um dos métodos mais utilizados para avaliação de usabilidade na literatura, também é conhecido como método por ensaios de interação.

Para a coleta de dados durante as sessões de avaliação de usabilidade, são considerados recursos como observação de mais de um avaliador, câmeras, microfones e registros e eventos. O desempenho de cada avaliado é considerado utilizando dados quantitativos como: taxa de erros, tempo para execução da tarefa e quantidade de tarefas completadas.

Para a pesquisa realizada neste trabalho, foi utilizado este método de acordo com [45] que avalia a usabilidade através de questionários pós-testes para, de maneira subjetiva, avaliar a satisfação do usuário e a facilidade do uso do sistema. Além de discutir possíveis melhorias para a execução destas tarefas dentro do sistema. Ainda segundo [37], considera-se o método de teste com usuários um dos fundamentais para avaliação de usabilidade pois fornecem dados diretos de como as pessoas usam os computadores e quais os exatos problemas com seus sistemas.

Por fim, considera-se a definição de usabilidade adotada nesta pesquisa a qual considera a usabilidade como uma medida em que um produto pode ser usado por vários usuários específicos para atingir metas especificas com a eficácia, eficiência e satisfação em um contexto especifico de utilização. A definição implica em uma usabilidade contextual, ou seja, um sistema com boa usabilidade dentro de um contexto pode não ser em outro.

2.1.2 A Relação entre usabilidade e segurança

Segundo [46], para que um software proteja os interesse de seus usuários é necessário que seu comportamento seja consistente com suas expectativas, ou seja, para projetar segurança em um sistema é necessário a compreensão do modelo mental, uma ideia do usuário de como deseja que o sistema funcione.

Desta forma, não se deve esperar que o usuário fale a língua dos especialistas em segurança ou pense em mecanismo de segurança para fazer o seu trabalho. Assim, aplicações *web* seguras devem aplicar ações de segurança com base nas ações dos usuários.

A usabilidade e segurança entram em equilíbrio quando o sistema interpreta corretamente as necessidades “a voz” do usuário. No aparente conflito que existe entre

usabilidade e segurança existem várias definições. De acordo com [47], existe uma abordagem que afirma que é recorrente a perspectiva de que efetuar melhorias na usabilidade impactam negativamente a segurança, e vice-e-versa. Esta expectativa ocorre por dois motivos: os desenvolvedores acreditarem que estes dois requisitos são complementos de produtos acabados e o conflito entre proprietários do software e seus usuários. Apesar de que este conflito reside na ideia de que a segurança torna as operações mais difíceis e a usabilidade facilita as operações, por si só, está definição é imprecisa, segundo o próprio autor.

Ainda, segundo o mesmo, a segurança não é sobre fazer todas as operações difíceis; e sim, fazer difíceis as operações indesejáveis; para a usabilidade segue-se o mesmo conceito, ou seja, não significa fazer todas as operações fáceis mais melhorar o acesso aquelas com efeitos desejáveis.

De acordo com [45], é improvável que os usuários realizem tarefas de segurança extra e podem até mesmo contornar as medidas de segurança para tornar suas tarefas principais mais confortáveis. Segundo [47], as pessoas normalmente usam computadores para outros fins que não a segurança, como comunicar com amigos, usar serviços on-line, gerenciar tempo e dinheiro, compor e editar trabalhos criativos e assim por diante.

Para esta pesquisa foi considerada a satisfação do usuário como aspecto de um objetivo comum entre usabilidade e segurança: a satisfação do usuário ou “voz do usuário”. Foi considerado este objetivo tendo em vista que usuários comuns estão preocupados em realizar suas tarefas, mesmo que para isso tenham que burlar questões de segurança.

2.1.3 O Estado da Arte – Método de Avaliação de Usabilidade e Segurança (IHCSeg)

Segundo [48], existe uma grande diferença entre a avaliação de um software seguro e dos demais softwares. Para ele, a avaliação de usabilidade destas aplicações não deve se concentrar em usabilidade a ponto de excluir a segurança. Em alguns casos, devido as características do sistema, é necessário até incluir comportamentos de segurança e tarefas de nível complexo para os usuários para garantir a mesma.

O IHCSeg está de acordo com o modelo centrado no usuário (DCU), pois este precisa de um sistema que tenha seja, concomitantemente, seguro e usável. Para [30], avaliar o que foi construído está no centro do design de interação. Para avaliar um modelo que coloca o usuário no centro de aplicações construídas, deve-se utilizar o modelo híbrido de [29], pois este consegue abordar tanto questões de usabilidade quanto de segurança para softwares (IHCSeg).

Os seguintes fatores, considerados pelo autor, têm efeito sobre a usabilidade de um software ou contexto especifico:

- **Eficácia**: utiliza a definição de [38] que afirma que é medida pela capacidade do usuário em completar uma tarefa em particular ou não;
- **Satisfação**: considera a definição de [37], na qual afirma que o usuário deve "gostar" da aplicação. A satisfação do usuário pode ser avaliada através de entrevistas e questionários;
- **Precisão**: o fator de precisão foi identificado principalmente em tarefas de autenticação. Em muitos casos, sistemas de autenticação exigem que os usuários digitem a senha com 100% de precisão. Estas exigências podem ser impactadas por outras demandas ambientais, como a memorização de informação ou fatores pessoais;
- **Eficiência**: utiliza a definição de [37]. A eficiência é capturada através da medição de tempo para completar uma tarefa ou o número de cliques/ botões pressionados para atingir as metas exigidas;
- **Memorização**: muitos sistemas de autenticação exigem que os usuários memorizem segredos necessários para adentrar ao sistema. O número de segredos que um usuário é obrigado a guardar aumenta com o número de sistemas de autenticação diferentes que ele interage. Isso resulta em problemas de memorização, onde os usuários têm dificuldades para se autenticar em vários sistemas diferentes, muitas vezes requisitando opções de refazer as senhas; e
- **Habilidade**: Isto é baseado na suposição de que os usuários vão aprender ou realmente tentar aprender e entender o sistema. Este pressuposto é falho particularmente em sistemas seguros. Usuários só se preocupam com as partes que eles acham que são importantes para as operações específicas que necessitam fazer, e em muitos casos as tarefas de segurança não são vistas como importantes.

Já para os critérios de segurança são avaliados os seguintes fatores:

- **Motivação**: os usuários têm diferentes níveis de motivação para realizar as tarefas de segurança. Quando os usuários têm a noção de que os riscos são mais diretos a eles, se motivam para realizar tarefas com cautela;

- **Vigilância**: sistemas seguros tendem a esperar que os usuários estejam alertas e proativos de forma regular, o que é impossível. Tarefas que representam risco de segurança devem ser analisadas e integradas ao fluxo de trabalho dos usuários;
- **Atenção**: os usuários podem facilmente se distrair e diminuir a atenção dedicada a determinada tarefa. Tarefas de segurança exigem atenção total dos usuários, pois do contrário, podem existir falhas de segurança;
- **Memorização**: sistemas de autenticação muitas vezes exigem que os usuários memorizem senhas que são difíceis para alguém adivinhar ou até mesmo atacar com técnicas de força bruta (*cracking*);
- **Contexto Social**: os seres humanos são seres sociais. Eles ajudam uns aos outros e compartilham informações. Normalmente o compartilhamento é algo positivo. Porém pode vir a ser ruim para a segurança se os usuários compartilharem senhas ou procedimentos de segurança. Muitas vezes os usuários compartilham senhas quando alguém se oferece para ajudá-los com algum problema. A avaliação de um sistema deve analisar como o contexto social afeta a segurança;
- **Condicionamento**: tarefas repetitivas de segurança onde os usuários podem prever um resultado podem se tornar uma ameaça para a segurança de um sistema. Um exemplo comum são os *pop-up* que perguntam aos usuários se um determinado certificado é confiável ou não; e
- **Habilidade**: diferente do fator habilidade na usabilidade, o fator habilidade para segurança está voltado para o conhecimento dos usuários ou nível de habilidade que desempenha como um papel importante na segurança de um sistema.

Contudo, estes fatores devem ser avaliados de acordo com métricas mensuráveis especificas. Para a medição dos fatores de segurança já seriam necessários sistemas específicos de usabilidade como o *eye-tracking* para avaliar a falta de atenção do usuário em determinada tarefa ou local da aplicação. Pode-se avaliar a vigilância monitorando e gravando os passos do usuário para realizar a tarefa e a quantidade de erros durante a realização desta.

A motivação não pode ser medida diretamente, mas pesquisas mostram que para envolver-se em uma tarefa de segurança é dirigida pela percepção de suscetibilidade a ataques; os benefícios advindos das ações de segurança; facilidades de interação com os controles de segurança; e a gravidade de se cometer uma falha de segurança [49]. A mensuração de tais fatores permite observar a motivação dos usuários em executar tarefas de segurança de forma eficaz. Além disso, podemos capturar a memorização contando o número de ações corretas e

perguntando aos usuários se eles têm problemas de memorização ou não, enquanto a habilidade pode ser capturada em forma de sucesso no desempenho de tarefas.

Para a realização desta pesquisa, foram utilizadas as ferramentas mais econômicas e de fácil acesso para os usuários, como questionários e aplicações em fase de implementação. Desta forma, foram analisados requisitos de usabilidade, de acordo com a satisfação do usuário, e segurança de acordo com a equipe do projeto.

2.2 Segurança da Informação

A segurança da informação e Comunicações (SIC) são ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e a autenticidade de dados e informações, segundo [50]. A SIC busca garantir o Comando e Controle (C2) das informações e sua consciência situacional; objetivo este que também é da cibernética.

O termo cibernético tem sua origem no grego "KUBERNETES" e não possui uma única definição. Uma delas foi proposta pela *American Society for Cybernetics* em 1948, cujo o autor é o matemático Norbert Wiener, para abranger todo o campo da teoria do controle e comunicação, seja da máquina ou do animal, conforme [51]. Ainda, este autor considerou a cibernética como uma ciência multidisciplinar que surgiu para ocupar uma lacuna entre as disciplinas.

A partir do conceito de cibernética criado pela Teoria Geral dos Sistemas no final da década de 70, foi possível estabelecer uma relação entre a cibernética e o estudo das organizações [52].

No contexto militar a cibernética refere-se à comunicação e controle, relacionados ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. Para [50], dentro do contexto de Defesa Nacional, inclui recursos de tecnologia de informação e comunicações de ordem estratégicas como: Sistemas Militar de Comando e Controle (SISMC²), Sistemas Integrado de Monitoramento de Fronteiras (SISFRON) e os sistemas administrativos que possam afetar em atividades operacionais.

A partir destes conceitos, outras definições foram crescendo de importância como segurança cibernética, defesa cibernética e proteção cibernética. A segurança cibernética deve garantir a existência e continuidade do espaço cibernético de uma nação, protegendo e garantindo neste espaço os ativos de informação e suas infraestruturas críticas. Já a defesa cibernética deve agrupar um conjunto de ações ofensivas, defensivas e exploratórias para proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a

produção de conhecimento de inteligência e comprometer os sistemas de informações do oponente.

A proteção cibernética, segundo [50], envolve ações para neutralizar ataques e exploração cibernética contra os dispositivos computacionais, redes de computadores e de comunicações alvos. Incrementado as ações de segurança, defesa e guerra cibernética em face de uma situação de crise ou conflito.

Estas ações de segurança têm por objetivo assegurar o valor da informação de suas organizações, empresas e países pois em um mundo conectado a informação e os processos relacionados como: sistemas, redes e pessoas envolvidas nas suas operações (usuários) são considerados ativos de valor para o negócio da organização. Por isso, requerem proteção contra vários tipos de riscos.

Uma segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. O método USASEC contribui para a proteção cibernética, portanto para a segurança dos ativos de informação, incluindo procedimentos, processos e controles para a confecção de *softwares* (aplicações *web*) que são ativos estratégicos para as suas organizações.

2.2.1 Definições de Segurança da Informação

A segurança da informação, segundo [50], são ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e a autenticidade de dados e das informações. Ainda, a segurança da informação eficaz também garante à direção da organização, bem como os usuários de diversos níveis de função, que os ativos da organização estão razoavelmente seguros e protegidos contra danos, agindo como um facilitador dos negócios.

De acordo com a [53] a segurança da informação tem como propósito proteger as informações registradas, sem importar onde estejam situadas: impressa de papel, nos discos rígidos dos comutadores ou, até mesmo, na memória das pessoas que as conhecem.

Desta forma, a segurança da informação (SI) é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos e as oportunidades de negócio. Ou seja, a SI é um ponto crítico para a sobrevivência das organizações pois a sociedade depende das informações armazenadas nos sistemas computacionais para a tomada de decisão em empresas, órgãos governamentais e em outros contextos organizacionais.

Para analisar a segurança da informação é necessário definir alguns conceitos:

- **Incidente de segurança** – corresponde a qualquer evento adverso relacionado à segurança; por exemplo, ataques de roubo de informação, vazamento e obtenção de aceso não autorizado a informação e *Cross Site Scripiting,* que corresponde a aplicação que recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados;
- **Ativo** – qualquer objeto que possua valor para a organização e para seus negócios; como exemplo pode-se citar equipamentos, bancos de dados, softwares e aplicações, pessoas, processos e, até, serviços;
- **Ameaça** – são eventos que exploram a vulnerabilidade, sendo esta uma causa potencial de um incidente indesejado. Esta pode preceder um dano para uma aplicação ou organização;
- **Vulnerabilidade** – fraquezas que podem ser exploradas e, desta forma, comprometer a segurança do sistema ou informações. Geralmente, ocorre devido a uma fragilidade a um ativo ou grupo deles que pode ser explorada por uma ou mais ameaças;
- **Riscos** - uma combinação probabilística, chance de uma ameaça se concretizar, de um evento ocorrer e de suas consequências para a organização;
- **Ataque** – qualquer ação que comprometa a segurança da organização; e
- **Impacto** – consequência avaliada de uma ação em particular.

Dessa forma, esses conceitos devem ser considerados para identificação, análise e escolha dos controles adequados para garantir que os serviços e mecanismo de segurança devem ser aplicados de modo a atender os requisitos de segurança da organização.

De acordo com [53] e [54], o qual compreende a segurança e seus aspectos no modelo *Open System Interconnection* (OSI), os serviços de segurança são medidas preventivas escolhidas para combater ameaças identificadas.

2.2.2 Princípios de segurança da informação

Os serviços de segurança, portanto, aumentam a segurança da informação contra ataques fazendo uso de um ou mais mecanismos de segurança. Eles também são conhecidos como princípios básicos de segurança. Estes princípios básicos de segurança são, conforme [53]:

1. **Autenticidade** – princípio que garante que uma comunicação é autêntica, ou seja, pode-se verificar a identidade da origem e do destino envolvidos na comunicação, com a assertiva de determinar se a outra parte é essencialmente quem diz ser;

2. **Confidencialidade** – abrange a proteção dos dados transmitidos contra ataques passivos, que são aqueles que se baseiam em monitoramento e escutas de transmissões, como por exemplo o acesso não autorizado;
3. **Integridade** – preocupa-se na garantia contra ataques ativos, são aqueles que envolvem modificações de dados e criação de objetos falsificados ou negação de serviço, por meio alterações ou retiradas de dados não autorizadas. Para este princípio, é importante que haja um serviço de verificação da integridade dos dados armazenados e em transmissão;
4. **Disponibilidade** - decide que recursos estejam desimpedidos para acesso por entidades autorizadas, sempre que solicitado, representando a proteção contra perdas ou degradações. Quando a informação deixa de estar acessível por quem precisa dela, chama-se isso de perda de disponibilidade;
5. **Controle de acesso** – determina o limite e o permissão lógica e física aos ativos de uma organização por meio de processos de identificação, autorização e autenticação, com a finalidade de proteger os dados há acessos não autorizados;
6. **Conformidade** – garante em cumprir e fazer cumprir regulamentos internos e externos impostos às atividades da organização. Estar em conformidade é estar de acordo, seguindo e fazendo cumprir leis e regulamentos internos e externos a organização; e
7. **Não-repúdio** – compreende o serviço que previne uma origem ou destino de negar a transmissão da mensagem, ou seja, quando certa mensagem é enviada, o destino pode provar que esta foi realmente enviada pelo destinatário, e vice-e-versa.

Assim, cada característica destes princípios de segurança da informação deve ser considerada quando se busca desenvolver aplicações *web* que atendem a segurança que os usuários necessitam.

2.2.3 Práticas e ações de segurança da informação para aplicações *web*

A evolução das ameaças para a segurança das aplicações está relacionada: aos avanços feitos pelos atacantes, ao lançamento de novas tecnologias com novas vulnerabilidades ainda não identificadas e a implantação de sistema cada vez mais dinâmicos e complexos. Segundo [7], a dificuldade em obter segurança para aplicações aumenta exponencialmente à medida que as infraestruturas digital ficam cada vez mais interligadas. A possiblidade de se ter um software

inseguro debilita organizações financeiras, de saúde, defesa, de energia e outras que são infraestruturas críticas do Estado.

Assim, foi criada a *Open Web Application Security Project* (OWASP) como uma comunidade aberta, dedicada a capacitar organizações a desenvolver, adquirir e manter aplicações seguras.

O fato de ser uma comunidade livre e uma entidade sem fins lucrativos, retira a OWASP de pressões comerciais que possam vir a influenciar as normas e práticas determinadas por esta organização. Contudo, existe apoio de diversas empresas da área de tecnologia e segurança, a OWASP mantém o compromisso de ser imparcial com os dados e recomendações que são passadas em relatórios anuais.

A partir de 2003, a OWASP passou a lançar recomendações de riscos chamadas Top 10 para trazer à tona os dez principais problemas de segurança em aplicações web. Os Top 10 da OWASP servem para educar desenvolvedores, gestores, projetistas, arquitetos de softwares e organizações sobre as consequências das mais importantes vulnerabilidades de segurança para aplicações *web*. Além disso, traz recomendações e fornece técnicas básicas de como se proteger destas vulnerabilidades.

O OWASP Top 10 está na sua versão do ano de 2013, mas uma atualização está prevista para acontecer em relação ao ano de 2016. As mudanças da versão de 2010 para 2013 não foram muitos significativas, o que mostra que possivelmente a versão 2016 possuirá poucas modificações, conforme Figura 2.3.

OWASP Top 10 – 2010 (Anterior)	OWASP Top 10 – 2013 (Novo)
A1 – Injeção de código	A1 – Injeção de código
A3 – Quebra de autenticação e Gerenciamento de Sessão	A2 – Quebra de autenticação e Gerenciamento de Sessão
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos	A4 – Referência Insegura e Direta a Objetos
A6 – Configuração Incorreta de Segurança	A5 – Configuração Incorreta de Segurança
A7 – Armazenamento Criptográfico Inseguro – Agrupado com A9 →	A6 – Exposição de Dados Sensíveis
A8 – Falha na Restrição de Acesso a URL – Ampliado para →	A7 – Falta de Função para Controle do Nível de Acesso
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<Removido do A6: Configuração Incorreta de Segurança>	A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos	A10 – Redirecionamentos e Encaminhamentos Inválidos
A9 – Proteção Insuficiente no Nível de Transporte	Agrupado com 2010-A7 criando o 2013-A6

Figura 2.3 – Modificações da versão de 2010 para 2013 do Top 10 da OWASP, adaptado de [7].

Para cada um deste riscos para aplicações, existe uma característica que pode estar relacionada a um ou mais princípios de segurança da informação. A seguir serão dadas as

definições para cada um dos riscos previsto no Top 10 da OWASP 2013, conforme quadro comparativo abaixo:

Risco	Definição	Relação com o Princípio de Segurança da Informação
Injeção de Código	As falhas de Injeção, tais como injeção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.	Afeta a Confidencialidade Afeta a Autenticidade Afeta a Integridade Afeta Não-repudio Afeta Conformidade Afeta o Controle de acesso Afeta a Disponibilidade
Quebra de Autenticação e Gerenciamento de Sessão	As funções da aplicação relacionadas com autenticação e gerenciamento de sessão geralmente são implementadas de forma incorreta, permitindo que os atacantes comprometam senhas, chaves e *tokens* de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários	Afeta a Confidencialidade Afeta a Autenticidade Afeta a Integridade Afeta o Controle de acesso Afeta a Disponibilidade Afeta o Não- Repúdio Afeta Conformidade
Cross Site-Scripting (XSS)	Falhas XSS ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados. XSS permite aos atacantes executarem scripts no navegador da vítima que podem "sequestrar" sessões do usuário, desFigurar sites, ou redirecionar o usuário para sites maliciosos	Afeta a Autenticidade Afeta a Integridade Afeta o Não- Repúdio Afeta a Conformidade Afeta a Disponibilidade
Referência Insegura e Direta a objetos	Uma referência insegura e direta a um objeto ocorre quando um programador expõe uma referência à implementação interna de um objeto, como um arquivo, diretório, ou registro da base de dados. Sem a verificação do controle de acesso ou outra proteção, os atacantes podem manipular estas referências para acessar dados não-autorizados	Afeta a Integridade Afeta o Controle de acesso Afeta a Confidencialidade
Configuração Incorreta de Segurança	Uma boa segurança exige a definição de uma configuração segura e implementada na aplicação, frameworks, servidor de aplicação, servidor web, banco de dados e plataforma. Todas essas conFigurações devem ser definidas, implementadas e mantidas, já que geralmente a configuração	Afeta a Confidencialidade Afeta a Autenticidade Afeta a Integridade Afeta o Controle de acesso Afeta a Disponibilidade Afeta o Não- Repúdio

	padrão é insegura. Adicionalmente, o software deve ser mantido atualizado.	Afeta a Conformidade
Exposição de Dados Sensíveis	Muitas aplicações web não protegem devidamente os dados sensíveis, tais como cartões de crédito, IDs fiscais e credenciais de autenticação. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes. Os dados sensíveis merecem proteção extra como criptografia no armazenamento ou em trânsito, bem como precauções especiais quando trafegadas pelo navegador.	Afeta a Confidencialidade Afeta a Autenticidade Afeta a Integridade Afeta o Controle de acesso
Falta de função para controle do nível de acesso	A maioria das aplicações web verificam os direitos de acesso em nível de função antes de tornar-se essa funcionalidade visível na interface do usuário. No entanto, as aplicações precisam executar as mesmas verificações de controle de acesso no servidor quando cada função é invocada. Se estas requisições não forem verificadas, os atacantes serão capazes de forjar as requisições, com o propósito de acessar a funcionalidade sem autorização adequada	Afeta a Autenticidade Afeta a Integridade Afeta o Controle de acesso Afeta a Disponibilidade Afeta o Não- Repúdio
Cross Site Request Forgery (CRSF)	Um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma requisição HTTP forjada, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação web vulnerável. Esta falha permite ao atacante forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima	Afeta a Autenticidade Afeta a Integridade Afeta o Controle de acesso
Utilização de componentes vulneráveis conhecidos	Componentes, tais como bibliotecas, frameworks, e outros módulos de software quase sempre são executados com privilégios elevados. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor. As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos	Afeta a Confidencialidade Afeta a Autenticidade Afeta a Integridade Afeta o Controle de acesso Afeta a Disponibilidade Afeta o Não- Repúdio Afeta a Conformidade

Redirecionamentos e encaminhamentos inválidos	Aplicações web frequentemente redirecionam e encaminham usuários para outras páginas e sites, e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de *phishing* ou *malware*, ou usar encaminhamentos para acessar páginas não autorizadas.	Afeta a Confidencialidade Afeta a Autenticidade Afeta a Integridade

Tabela 2.1 – Tabela comparativa dos riscos da OWASP Top 10 e princípios de Segurança da Informação, adaptado de [7].

Assim, é possível comparar cada um dos riscos e suas consequências a um conceito dos princípios básicos de segurança que foi violado ou não atendido. Por exemplo, podemos exemplificar que a injeção de código, tem por definição o envio de dados não confiáveis para o interpretador do navegador, pode gerar a perda ou corrupção dos dados (afeta a integridade), acesso a dados não autorizados (afeta controle de acesso, confidencialidade, autenticidade) e, em alguns casos mais graves, comprometer o servidor (disponibilidade).

Desta forma, é possível aumentar o arcabouço de riscos que estão sendo analisados para compor a importância relativa do método proposto na pesquisa, método USASEC. A junção destes dois requisitos pode aumentar a proteção cibernética da aplicação.

2.2.4 Proteção Cibernética

A proteção cibernética, como definida na seção 2.2, deve se focar nas ações de neutralização a ataques e exploração cibernética. Um ataque cibernético são ações para interromper, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicação do oponente. Logo, a proteção cibernética deverá buscar neutralizar estas ações.

Já a exploração cibernética compreende em ações de busca e coleta, nos sistemas de tecnologia da informação de interesse, a fim de obter uma consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento das vulnerabilidades desses sistemas.

Ainda, de acordo com [50], existem vários níveis de decisão de acordo com a necessidade da ação que precisa ser tomada. De acordo com a Figura 2.4, as ações de guerra

cibernética (abrange as ações cibernética de proteção, ataque e exploração) são tomadas nos níveis tático e operacional pelos Forças Armadas presentes na situação. Logo, a proteção cibernética é de responsabilidade das Forças Armadas e de caráter permanente, ou seja, deve ser priorizada e feita ainda no tempo de paz.

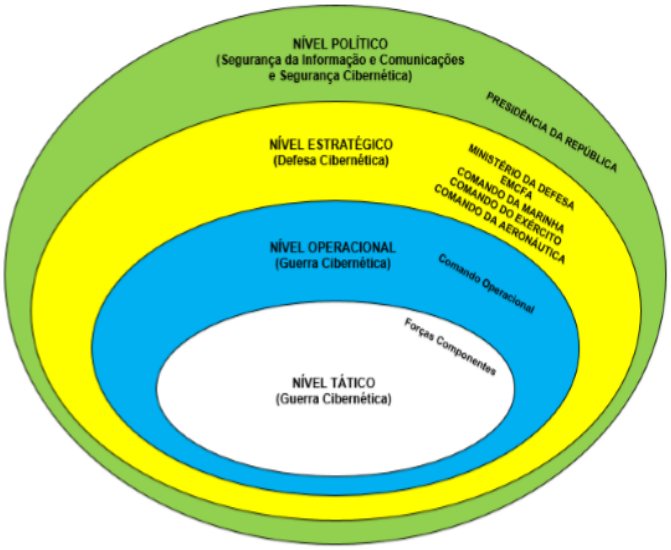


Figura 1: Níveis de decisão

Figura 2.4 – Níveis de decisão para ações no Espaço Cibernético [50].

Já a defesa cibernética fica a cargo de órgãos estratégicos como Ministério da Defesa e o Comando de Defesa Cibernético (ComDCiber), criado para conjugar as três forças. Por fim, a segurança cibernética e a SIC ficam a cargo do Departamento de Segurança da Informação e Comunicação (DSIC), órgão do governo federal ligado ao Gabinete de Segurança Institucional do Presidente da República (GSI/PR). Sendo assim, um nível político.

Logo, para alcançar esta ação, é necessário desenvolver padrões e processos que assegurem a qualidade das aplicações. Algumas destas são desenvolvidas por contratos à terceiros e utilizados por órgãos públicos como aplicações críticas de trabalho, como por exemplo aquelas que coordenam tráfego aéreo ou controlam grandes infraestruturas críticas. Sendo assim, cabe às organizações que compram ou produzem estes softwares, garantir pela sua qualidade e proteção.

2.3 Desdobramento da Função de Qualidade de Software (SQFD)

Segundo [33], a qualidade do software pode ser entendida como conformidade com os requisitos dos clientes. Portanto, todas as atividades no desenvolvimento no ciclo de vida do software devem ser voltadas e analisadas de acordo com as necessidades dos clientes [28].

Sendo assim, as atividades de desenvolvimento do software, tais como design de arquitetura, projeto da estrutura de dados, técnicas de modelagem de objeto, codificação e teste, devem ser conduzidas pela necessidade do cliente. Somam-se a esta necessidade, os conflitos entre as necessidades dos usuários (com ênfase em melhorar a usabilidade) e as questões de interesse dos proprietários da aplicação.

Para chegar a um "consenso" entre as partes interessadas foi desenvolvido um método denominado de Desdobramento de Função de Qualidade de Software, em inglês *Software Quality Function Deployment* (SQFD). Segundo [28], a aplicação da evolução do QFD para software (SQFD) começou no Japão em 1982, na América do Norte em 1988 e na Europa em 1990. Atualmente, muitas das principais organizações de software do mundo utilizam o SQFD como uma parte essencial da organização para avaliar a Gestão da Qualidade Total, *Total Quality Management* (TQM), e o Design para Seis Sigmas, *Design for Six Sigma* (DFSS), nessas empresas.

Apesar do QFD ser um sistema de qualidade, ainda segundo [28], ele possui implantações e subsistemas para lidar com questões de qualidade, tecnologia, custo, cronograma e confiabilidade.

2.3.1 Definições do SQFD

Segundo [55], o Desdobramento da Função de Qualidade, do inglês *Quality Function Deployment*, representa um esforço para que o ponto de vista do cliente referente a qualidade do produto seja incorporado nos passos inicias do desenvolvimento e continue sendo considerado ao longo de todo o ciclo de vida do produto. Sendo considerado por [56] como uma mudança do controle de qualidade focada na manufatura e processo para o controle da qualidade voltado para o desenvolvimento do produto.

Segundo [57], o SQFD é um método multifuncional que permite às organizações priorizarem as demandas dos consumidores e, em função disso, desenvolverem respostas inovadoras para as demandas dos clientes e que sejam efetivas em termos de custo e qualidade.

Segundo [58] e [59] *apud* [60], é um método de desenvolvimento de produtos que tem como principal finalidade definir a garantia da qualidade na fase de projetos, além de identificar e integrar as exigências dos clientes em características técnicas do produto para atender aos a esses requisitos.

Segundo [61], o QFD é um método que auxilia as empresas a venceram a lacuna que existe entra a satisfação do cliente e o desenvolvimento de qualidade em produtos e processos.

Segundo o autor, a ferramenta auxilia as empresas a serem competitivas uma vez que acelera o desenvolvimento do produto considerando explicitamente as demandas dos clientes.

Desenvolvido no Japão pelo Dr. Yoji Akao e Dr. Shigeru Mizuno, o QFD tem dois objetivos: assegurar que as verdadeiras necessidades dos clientes sejam adequadamente implantadas em todas as fases do processo de desenvolvimento e melhorar o próprio processo de desenvolvimento.

A aplicação do QFD para software (SQFD) começou no Japão em 1982, na América do Norte em 1988 e na Europa em 1990. Hoje, muitas das principais organizações de software em todo o mundo usam o SQFD como parte essencial de tais organizações. Este método proporciona a avaliação de requisitos da qualidade com fins de assegurar a satisfação do cliente.

O QFD deve ser executado em quatro fases popularizadas segundo [62], no seu trabalho aplicando o método para a fabricação de peças automotivas. Este modelo inicial, Figura 2.5, ainda não era apropriado para o desenvolvimento de software, mas já continha princípios e características que poderiam ser adaptados para este fim.

As quatros fases mostradas na Figura 2.5 são as seguintes:

A Fase 1 é conhecida como a “Casa da Qualidade” onde é realizada a matriz das necessidades dos clientes com as características técnicas de qualidade do produto. Esta tem por como objetivo responder o que significa um “bom produto” para o nosso cliente. Os requisitos de um “bom produto” são mapeados através da “voz do cliente” e representadas em atributos para o produto. Estes atributos são integrados às características de qualidade do produto para indicar o maior esforço nos atributos que podem satisfazer as necessidades do cliente.

A fase 2 (Matriz de Desenho) é um desdobramento da matriz da fase 1 e traz as características da qualidade que foram priorizadas para seu escopo. As características críticas da qualidade são mapeadas em partes e suas características mais críticas com as necessidades do cliente são relacionadas. A matriz de desenho tem por objetivo responder à pergunta: que parte dos produtos oferecem as características que nosso cliente quer.

Na fase 3 (Matriz Operacional) tem por objetivo relacionar parâmetros de processo com as características do processo de planejamento. A matriz operacional tem por objetivo de responde onde, durante nosso processo de fabricação, podemos afetar as características críticas das peças que forma apontadas na matriz 2. As características críticas das peças, então, são mapeadas em passos e parâmetros de processo. Nesta fase o QFD chega para melhorar o processo de fabricação do seu produto.

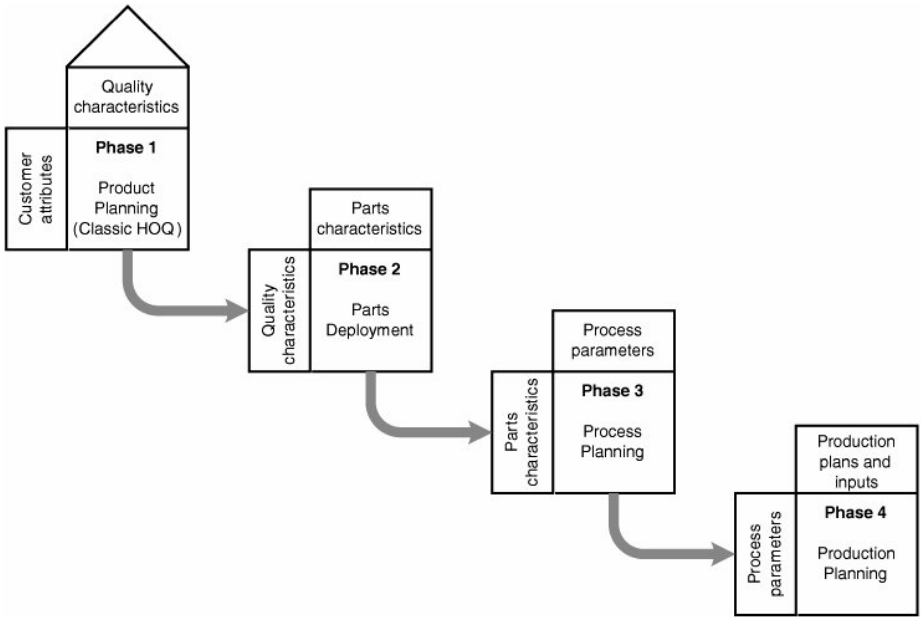


Figura 2.5 – Modelo do QFD [62].

Na última fase, fase 4 (Matriz de Controle), é possível fazer um relacionamento entre os parâmetros de planejamento de produção, vindos da matriz 3, e os requisitos para a produção. A matriz de controle responde à pergunta quanto a quais devem ser os planos de produção, procedimentos e insumos para que as operações principais do planejamento de produção possam produzir as características chaves para satisfazer o cliente. Desta forma, a "voz do cliente" atingiu os operadores de fabricação do produto determinando como será realizada a produção afim de satisfazer o cliente.

Desta forma, durante as fases do QFD só os itens mais importantes são desdobrados para a próxima fase, assim, o método está concentrado os melhores esforços no que é mais importante para o cliente. Assim, com a utilização do método, estamos priorizando o que é mais importante para o cliente e não apenas transformando requisitos de clientes em características técnicas de engenharia.

A matriz 1 "Casa da Qualidade" é a mais utilizada para adaptação de um produto. Ela é dividida em vários "quartos" e pode ser observada segundo a Figura 2.7. Segundo [33], a casa da qualidade deve conter as seguintes características:

No quarto 1 são colocados os requisitos dos clientes de acordo com múltiplas perspectivas. Estes requisitos descrevem o que os clientes querem e devem ser completos, consistentes, não ambíguos, não redundantes e identificados. Existem três tipos de requisitos: os revelados, esperados e excitantes conforme o modelo de Kano.

No quarto 2 são levantados os requisitos dos clientes de acordo com a comparação, *benchmarking*, com outros produtos ou serviços de seus concorrentes. Nesta fase, o cliente pode dizer quais as características que mais o atraem em outros produtos em relação ao produto que ele está utilizando ou querendo produzir. Caso não seja necessária uma comparação entre produtos, este quarto não é necessário.

No quarto 3, ficam as listas do que sua empresa pode fazer tecnicamente para satisfazer as necessidades do cliente. São as características de engenharia do produto e podem ser mensuráveis.

No quarto 4 podemos correlacionar os requisitos do cliente com as especificações técnicas dos engenheiros. Este relacionamento entre os requisitos pode ser feito atribuindo uma nota para como o requisito do cliente impacta o de características técnicas (forte colocando o valor de 9 na matriz, moderado coloca-se o valor 3 ou fraco de valor 1).

No quarto 5 são feitas avaliações de características técnicas do nosso em relação aos produtos concorrentes. Desta forma, a área técnica consegue colocar as características técnicas que o "atraem" em outros produtos que o seu produto não possui. Caso não haja comparação de clientes, quarto 2, para a matriz também não é obrigatório este quarto.

No quarto 6 fica o *trade-off* destas características que podem ser relacionar positivamente, negativamente ou irrelevante. Se duas características estão positivamente relacionadas se o aumento de uma acarreta o da outra e negativamente caso o sentido desta relação seja inverso.

Por fim, pode-se extrair quais os requisitos técnicos mais importantes para atender a demanda feita pela "voz do cliente" utilizando a multiplicação das importâncias relativas dos pesos calculados pela importância de cada requisito dado pelo usuário multiplicado pelo valor dado pela equipe técnica do projeto nos relacionamentos no quarto 4.

De acordo com a fórmula:

$$IA = \sum_{j=1}^{M} RC * RTec(IRai, IRaj) \qquad (2.1)$$

Onde IA é a Importância Absoluta dos requisitos consistente da soma do produto dos "M" requisitos que corresponde a voz dos clientes (RC) com as características técnicas do produto (*Requeriments Technical* - RTec).

Por ser um método multifuncional e muito flexível, segundo [63]; o QFD já foi adaptado em muitas outras aplicações do método. A tabela 2.2 demonstra, no decorrer do seu desenvolvimento, quais as adaptações e como o método QFD pode ser utilizado para cada tipo de produto, processo ou serviço.

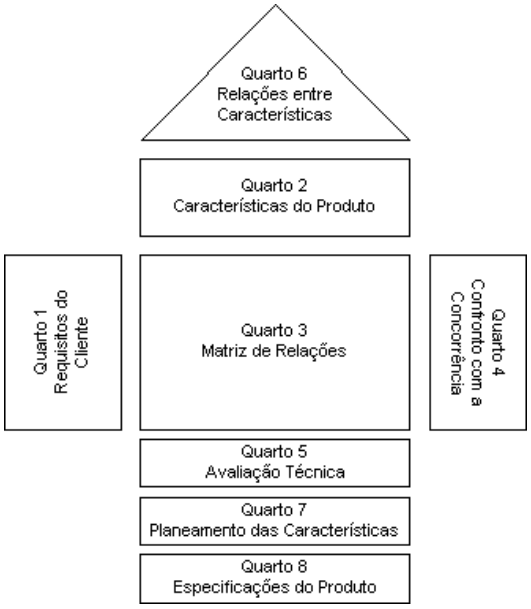


Figura 2.6 - Modelo da casa da qualidade, adaptado de [64].

De acordo com os benefícios que estão na tabela 2.2, pode-se levantar as principais características desta metodologia como: capacidade de identificar requisitos prioritários dos clientes ou usuários para o projeto e depois relacioná-los com requisitos técnicos do produto, desta forma, pode-se acoplá-los as especificações dos requisitos do projeto.

Tabela 2.2 – Exemplos na literatura do uso flexível do QFD, adaptado de [63].

AUTOR	**Aplicação para o desenvolvimento de produtos ecológicos**
[65]	Utilizam o QFD para otimizar produtos ecológicos considerando o impacto ecológico do produto e as restrições de orçamento do projeto. Junto com o QFD é utilizado um modelo matemático linear. Segundo o autor, com pequenas modificações o QFD pode ser usado para melhoria continua e ser útil para melhorar produtos considerando aspectos ambientais.
[66]	Desenvolvem uma metodologia (modelo conceitual) para aplicar o QFD a projeto de produtos considerando requisitos de consciência ambiental no início de projeto do produto. O QFD foi eficiente para considerar aspectos ambientais no desenvolvimento do produto e apresentar várias soluções para melhorar o produto, as quais foram avaliadas.
[67]	Uniram conceitos ambientais nas matrizes do QFD. Nessas matrizes as qualidades exigidas envolvem requisitos dos clientes, requisitos ecológicos e de custos.
AUTOR	**Aplicação para reprojetar produtos**

[68]	Desenvolveram uma metodologia baseada no QFD para minimizar falhas no projeto, podendo também ser usada para revisão de projetos atuais. Foram feitas aplicações acadêmicas e um estudo de caso. Segundo os autores o QFD ajuda a identificar erros de projeto, a avaliar subsistemas, ajuda na definição dos objetivos do projeto, a documentar os dados do projeto e a administrar os riscos de falha.
[69]	Desenvolveram um modelo de programação linear para ajudar na otimização de projetos de melhorias de produto, buscando reduzir custos e tempo. Apresentam uma aplicação na melhoria de mouse do computador, sendo que a aplicação foi acadêmica e não foi introduzida na indústria. Somente utilizaram princípios do QFD para definir as qualidades exigidas e as características da qualidade.
[70]	Apresenta um estudo de caso onde o QFD foi utilizado para re-projetar uma faca de desossar considerando aspectos ergonômicos. Esta é uma das pesquisas francesas que busca integrar aspectos ergonômicos nos produtos chamado de CEROM (*Conception Ergonomique d'Outils à Main*). Os benefícios do uso do QFD são identificar as melhores soluções entre as qualidades exigidas dos clientes e qualidades exigidas ergonômicas, e conseguir o consenso no atendimento dos dois tipos, além de alterar as características da qualidade atuais do produto para atender as qualidades ergonômicas exigidas.
AUTOR	**Aplicação diversas no desenvolvimento de produtos**
[60]	Utilização do QFD para indústria de alimentos. Trouxe benefícios como: contribuiu no estabelecimento das demandas do cliente, proporcionou uma visão ampla do processo, identificou todas as passos críticas, orientou as atividades de desenvolvimento do produto e organizou as informações necessárias para o planejamento da melhoria da qualidade.
[71]	Apresentam a aplicação e implementação do QFD numa empresa fabricante de filmes flexíveis. Segundo os autores, o uso do QFD trouxe os seguintes benefícios: sistematizou o processo de desenvolvimento; melhoria da comunicação; democratizou o conhecimento entre os membros da equipe, a capacidade de planejamento e registrou o conhecimento da empresa.

[72]	Sistema de suporte inteligente para projetar famílias de produtos. Esse sistema utiliza o QFD para identificar as qualidades exigidas e as características da qualidade e usa o ISM (*Interpretive Structural Model*) para verificar a hierarquia dos componentes e como eles se relacionam com o produto final. O benefício do uso do QFD foi identificar os principais requisitos dos clientes para cada tipo de mercado e as principais mudanças no reprojeto do produto para atender os clientes.
[73]	O autor participou da equipe de estudantes que utilizaram o QFD para ajudar a desenvolver um robô, para uma competição robótica. O QFD ajudou a identificar as características de qualidade críticas.
[74]	Desenvolvimento do pensamento enxuto para o desenvolvimento de produtos. Tem como benefício conciliar na agregação de valor para o produto, colocando cliente como coparticipe do projeto.
AUTOR	**Aplicação para softwares**
[75]	Utilização do QFD para software para realizar um estudo de caso para software de custo. Demostrou benefícios como: a definição antecipada das características principais do sistema é fundamental para o desenvolvimento de um software. O QFD vem se somar as demais ferramentas de análise de sistemas proporcionando, simultaneamente, um desenvolvimento mais rápido e mais qualificado.
[76]	Utilização do QFD para avaliar um sítio *web* de um canal de televisão popular e fornece os requisitos técnicos priorizados para atender aos consumidores.
[77]	Desenvolvimento de Processo de Melhoria para Software utilizando métodos como QFD para software e CMMI para avaliar a maturidade dos requisitos avaliados. Como benefício trouxe o mapeamento dos requisitos do processo, a priorização de requisitos e aumento na satisfação do cliente.
[78]	Uso da ferramenta QFD para software como ferramentas para otimizar a usabilidade de produtos de softwares. Como benefício avaliou, de forma teórica, a usabilidade como um dos requisitos dos produtos da área de tecnologia da informação pode utilizar ferramentas como o QFD para captar a voz dos seus clientes e ser otimizar em seus softwares.

[79]	Introdução de uma nova abordagem baseada em Análises Morfológicas e Teoria de Gráficos, para desenvolver uma nova forma sistemática de transição entre as fases do QFD.
[80]	Uma abordagem analítica do uso do QFD no domínio dos serviços web. Como benefício trouxe como melhor descrever as qualidades deste serviço e sua aplicação para recuperação deste serviço.

Com a crescente necessidade de ter produtos de softwares mais rápidos, com menor custo e priorizando os requisitos que satisfazem o cliente, foi utilizado os princípios e características da metodologia QFD para o desenvolvimento de softwares, denominado (SQFD).

Segundo [33], o SQFD tem por objetivo a melhoria da qualidade do processo e do produto no desenvolvimento de software. Esta melhoria proporciona menos mudanças na especificação de requisitos, design e código, uma redução no número de defeitos e menos retrabalho e, portanto, maior produtividade. Ainda, segundo o autor, o SQFD melhora a comunicação entre clientes e desenvolvedores de software e testadores.

Segundo [81], melhoraria o processo de desenvolvimento de software através da implementação de técnicas de melhoria de qualidade durante a fase de solicitação de requisitos no ciclo de vida do desenvolvimento do sistema. Com isso, aumenta-se a produtividade do analista e programador, conduziria menos mudanças no design, redução no número de erros passados de uma fase para a próxima do ciclo de vida de desenvolvimento do projeto e software de qualidade que satisfazem as necessidades do cliente.

Ainda, segundo [81], estes novos softwares de qualidade exigem menos manutenção, permitindo que os departamentos de TI disponibilizem recursos e tempo para novos projetos, uma vez que haverá redução do tempo dos projetos atuais.

Algumas das vantagens elencadas para o SQFD são: promover uma atenção melhor para as perspectivas dos clientes, criar um comunicação entre os departamentos, fornecer justificativas para a tomada de decisão, quantificar os requisitos qualitativos dos clientes, representa dados para facilitar o uso de métricas, facilitar a verificação cruzada, evitar a perda de informações, alcançar o consenso de recursos mais rápido, reduzir o tempo de definição do produto e pode ser adaptado para várias metodologias dentro do Ciclo de vida do Software.

Desta forma, segundo o autor, o SQFD é um método de solicitação de requisitos iniciais, adaptável a qualquer metodologia de engenharia de software que quantifica e definir requisitos

de clientes. Mas para fazer isso, o SQFD utiliza a matriz 1 “Casa da Qualidade”, conforme Figura 2.8, dos princípios tradicionais do QFD, com as seguintes modificações nos passos:

Passo 1 – Os requisitos dos clientes “a voz do cliente” será solicitada e registrada no eixo y a esquerda da matriz (1). Os clientes considerados são usuários finais, gerentes, pessoal de desenvolvimento de sistemas e qualquer pessoa que se beneficie com o uso do software proposto. Os requisitos são frases curtas como “fácil de aprender”, com a terminologia dos clientes e podem ser acompanhadas de uma definição detalhada;

Passo 2 – Com a cooperação dos clientes, os requisitos são convertidos em declarações técnicas e mensuráveis no produto de software e colocados no eixo x superior (2). Sendo assim, os requisitos dos clientes são transformados em especificações técnicas que podem ser mensuráveis de alguma forma: numérica ou booleana;

Passo 3 – Os clientes são convidados a preencher e chegar a um “consenso” na matriz de correlação (3), identificando a força das relações entre os vários requisitos do cliente e as especificações técnicas do produto;

Passo 4 – Baseados em dados das entrevistas dos clientes, outros dados são priorizados para serem utilizados para a correlação no eixo y do lado direito (4). Estes dados são informações adicionais que podem ser coletadas e levadas em consideração ou não, como avaliação da concorrência, índices de vendas e melhorias. Segundo [28], se não houver preocupações com a concorrência do cliente, como para um projeto interno, esse componente é desnecessário; e

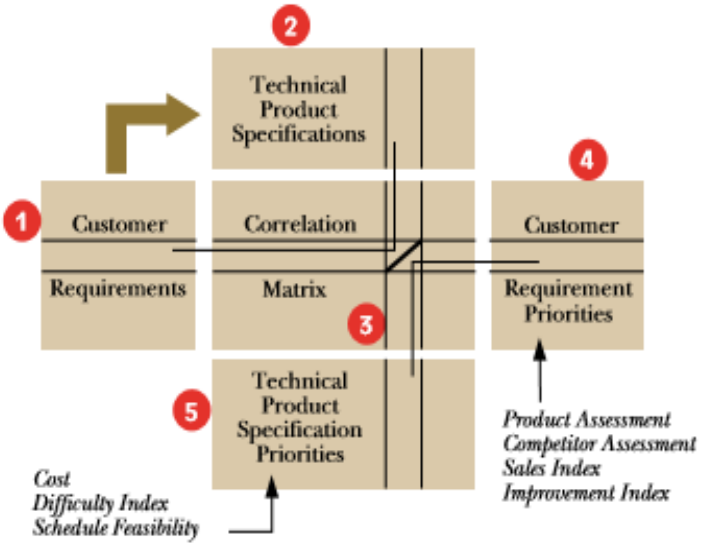


Figura 2.7 – Matriz do método SQFD, conforme [81].

Passo 5 - Este processo envolve o desenvolvimento das prioridades técnicas de especificação do produto (5) somando os resultados da multiplicação das prioridades de necessidades do cliente pelos valores de correlação entre os requisitos do cliente e as especificações técnicas do produto.

Esses pesos de prioridade brutos para as especificações técnicas do produto são normalmente convertidos em uma porcentagem do total de pesos de prioridade brutos. O produto final do método SQFD deverá conter especificações técnicas do produto, sua porcentagem de importância ou medidas direcionadas para obter a satisfação do cliente. Estas informações devem ser transportadas para dentro do desenvolvimento do software.

2.3.2 O Moderno QFD para Software

Durante a evolução do SQFD percebeu-se que apenas utilizar a ferramenta da casa da qualidade tornar-se-ia insuficiente para garantir que se estava realizando uma avaliação segura. Para corrigir erros no modelo, foi desenvolvido o modelo do moderno QFD para Software, conforme [28], com o objetivo de apoiar o Modelo Robusto de Desenvolvimento de Software, do inglês *Robust Software Development Model* (RSDM), criado pelo autor.

Durante um processo de desenvolvimento do software as necessidades do cliente nem sempre deduzidas de maneira correta (caixas à esquerda), por isso, dentro das demais fases do projeto, o julgamento onde os melhores esforços e recursos aplicáveis no local. Por causa disto, ao longa da vida do projeto, alguns não permanecerão alinhados, apenas por acaso. Assim, sem um método adequado às necessidades dos clientes (voz do usuário) e os pontos fortes do projeto, aqueles que devem receber foco em recursos, indeferindo estes requisitos no produto final, conforme Figura 2.9.

Contudo, se as necessidades mais verdadeiras do cliente, inclusive sua importância, são inicialmente bem definidas e analisadas, utilizando o Moderno SQFD, checa-se todos os melhores esforços e recursos encontrando-se alinhados e focados com as necessidades do cliente.

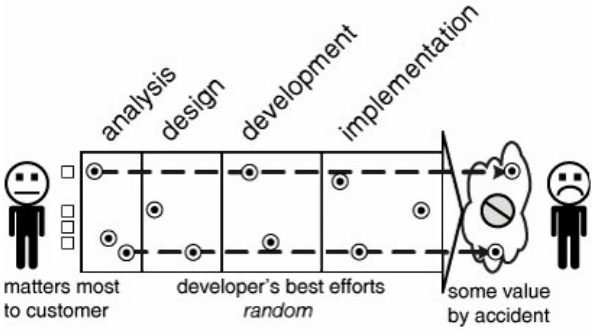


Figura 2.8 – Processo de desenvolvimento não-coerente, adaptado de [28].

Com isto, o resultado mostra um produto de valor para o cliente, uma vez que ele participou de alguma forma do processo de melhoria do software [82], e há um melhor direcionamento de tempo e recursos para criar um produto com itens de maior importância de maneira eficiente, conforme Figura 2.10.

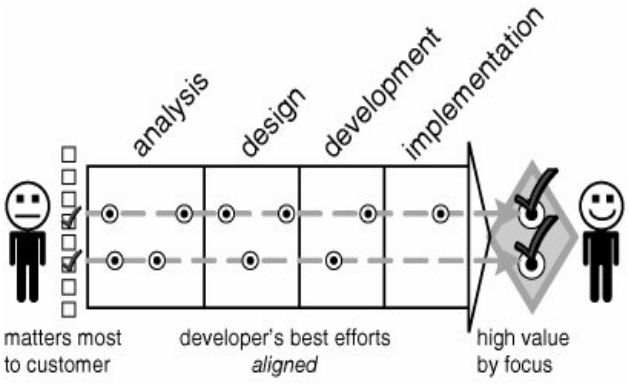


Figura 2.9 – Processo de desenvolvimento coerente, adaptado de [28].

O processo do moderno QFD tem nove passos e só utiliza matriz do QFD no final. Do primeiro passo até a oitava, Tabela de Máximo Valor (MVT), vários métodos e conceitos são utilizados para chegar até o último passo. Entre eles temos o método KJ, para montar o diagrama de afinidade, e o processo de análise hierárquica (AHP), com a finalidade de montar a hierarquização da importância dos requisitos feitos pelos usuários.

No passo final, quatro tipos de ferramentas são mostrados como ramificações: FMEA (para análise detalhada de itens de alto risco), *Kansei Enginneering* (para análise de design de interface e questões ligadas a (imagem e sentimento), tarefas essenciais em diagramas de Precedência (para desenvolvimento de projeto críticos) e para resolver problemas no projeto utiliza-se os métodos seis Sigma DMADV ou DMAIC), conforme a Figura 2.11.

De acordo com a Figura 2.11, cada passo deste processo deve ser assim definido:

1. Passo 1 – Objetivo do software – serve para definir em que parte da estratégia da organização este software será aplicado. Ou seja, porque se esta fazendo este software e qual a sua finalidade estratégica para a organização;
2. Passo 2 – Segmento dos clientes – qual o grupo de principais clientes pode nos ajudar a atingir o objetivo do software. Identificar quais são os principais clientes do software e sua importância relativa para ele, tendo em vista seu grande número. Este subconjunto de usuários deve ser bem escolhido para garantir que ouviremos cada segmento que utiliza o software;

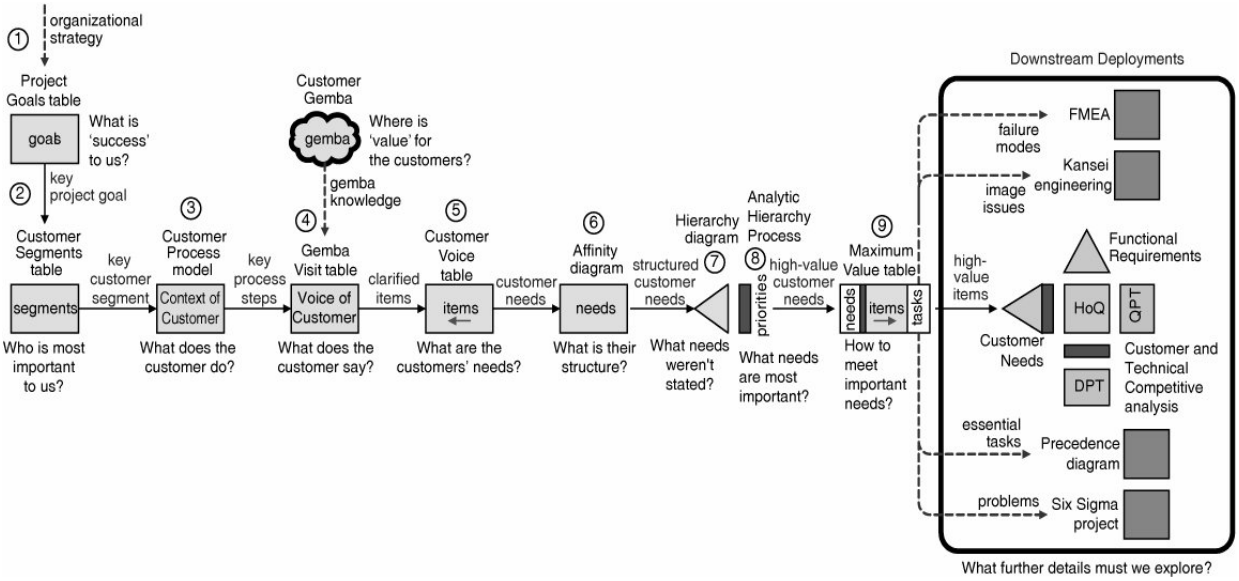


Figura 2.10 – O processo do Moderno QFD para Software, conforme [83] *apud* [28].

3. Passo 3 – Criar o modelo do software – de posse do segmento chave, aquele que precisa ser ouvido para garantir o sucesso da aplicação, e do entendimento estratégico da finalidade da criação do software; é necessário ir até o local onde ele deve agregar valor ao cliente. Mas para isso é necessário levar um modelo mental de como será o software: um diagrama de fluxo de caso, uma prototipação ou, no caso de já implementado, o software em si;
4. Passo 4 – Ir no ambiente de trabalho – deve-se ir até o local onde os usuários estão e ouvir a "voz do cliente". Observar e relatar seus problemas, sua situação e suas oportunidades de melhorias, para os softwares recém instalados. Para isso, pode se usar entrevistas, observações, questionários e gravações para análise da situação afim de reunir a voz do cliente. Os questionários para coleta de dados devem ter a capacidade de apresentar a ideia de forma simples, textual e livre. Desta forma,

podem ser utilizados os questionários abertos de acordo com [75], [84], [85] e [86]. De posse destas informações pode-se compartilhar com a equipe multidisciplinar do projeto, o questionário foi aplicado conforme apêndice A;

5. Passo 5 – Quais são as reais necessidades dos clientes – o que o cliente fala não são requisitos, são afirmações que devem ser entendidas, classificadas, organizadas e priorizadas. As afirmações são seus problemas, ou seja, oportunidades de melhoria e direções estratégicas para o sistema. As repostas para estas é que são as verdadeiras exigências dos usuários. Assim, os verbatims podem vir de várias fontes, entre elas fontes diretas como questionários, entrevistas e observações e indiretas por pesquisa por correio e telefone. Algumas destas fontes são históricas como elogios e reclamações sobre a aplicação, contudo o produto final deste passo deve ser uma tabela com as principais declarações relacionadas a usabilidade pelo cliente, também chamada de *Customer Voice Table* (CVT);
6. Passo 6 – Estruturar as necessidades dos clientes – após levantar os dados, será necessário envolver mais uma vez o cliente para clarificar como eles pensam suas necessidades. O resultado é um Diagrama de Afinidade, método KJ de [87], que revela a estrutura das necessidades e preenche as necessidades em falta e não declarada;
7. Passo 7 – Análise da estrutura das necessidades – é um procedimento onde transforma-se um diagrama de afinidade em um diagrama hierárquico. Você usa o diagrama de hierarquia para analisar a estrutura das necessidades do usuário e para descobrir necessidades em falta ou não declaradas. Este diagrama é importante para entender quais são critérios e alternativas que devem ser quantificados durante o passo seguinte (AHP) e tornar a estrutura de requisitos de alto valor visíveis;
8. Passo 8 – Priorizando as necessidades dos clientes – a partir do diagrama hierárquico, é necessário priorizar e quantificar cada um destes requisitos em proporção de escala, necessidades dos usuários, de acordo com o método AHP. Este método é um dos mais simples que fornece resultados precisos em uma escala de razão, conforme [88], e realizado atualmente conforme [89]. Embora os requisitos do cliente fossem priorizados em uma escala simples de 1 a 5, com o método AHP é possível ter uma maior acurácia da importância relativa de cada um destes requisitos, bem como consistência e sensibilidade; e os cálculos podem ser feitos de maneira simples através de planilhas ou software específicos para AHP; e

9. Passo 9 – Identificação das necessidades priorizadas do cliente com as necessidades técnicas do produto – a partir da realização do método AHP é possível quantificar as necessidades dos usuários e identificar qual as que mais impactam o projeto de software. Estes requisitos são chamados de Tabela de Máximo Valor (MVT) e entram na Casa da Qualidade como itens de alto valor para as necessidades dos clientes. Mas, ainda é necessário avaliar os requisitos técnicos funcionais para a inclusão desta MVT. Assim, é realizado um relacionamento entre os itens de alto valor e itens relacionados ao longo do projeto, para alinhar e descobrir itens essenciais para o desenvolvimento do mesmo.

No passo 9, outros métodos ramificados podem utilizar a MVT para explorar outros aspectos relacionados aos requisitos que foram quantificados, como já abordado. O FMEA, do inglês *Failure Mode and Effect Analysis*, conhecido como Análise de Modelo de Falhas e Efeitos é uma ferramenta para prevenir falhas e analisar riscos de um processo ou produto [90].

O *Kansei Engineering*, criada segundo [91] pelo próprio autor em 1989, visa a tradução do Kansei (sentimento e imagem) do consumidor para o produto.

O Diagrama de precedentes seria um complemento para o QFD moderno, uma vez que ele é responsável por identificar o caminho critico que deve ser usado para atender os prazos do projeto utilizando diagramas de redes de atividades.

E por fim, a ferramenta Seis Sigma foi criada em 1987 por Bill Smith da Motorola e ganhou força com sua aplicação na empresa GE. Consiste em um conjunto de práticas desenvolvidas para maximizar o desempenho dos processos dentro da empresa, eliminando os seus defeitos e as não-conformidades de acordo com as especificações técnicas de fábrica.

Assim, a casa da qualidade pode trazer benefícios importantes para todo o Moderno QFD pois evita o início do desenvolvimento do projeto do software sem ouvir os vários segmentos de usuário.

2.4 O Diagrama de Afinidades

O diagrama de afinidade, também conhecido como método KJ devido à nome do seu criador *Kawakita Jiro*, é um conjunto de ideias sobre determinado tema que são agrupadas com base em suas similaridades. É um método criado para estruturação de problemas caóticos, difíceis e complexos e serve para organizar e entender melhor um problema a partir de diversos dados estruturados, verbais e não estruturados.

O diagrama de afinidade pode ser feito, basicamente, em três fases conforme [92]:

1. Gerar os dados verbais, incentivando as pessoas a expressar suas ideias, desejos, frustações, percepções e opiniões. Esta primeira fase pode ser realizada através de dados redigidos válidos, falados ou escritos nas próprias palavras da pessoa. Para isso podem ser usadas ferramentas de coleta como: reuniões formais ou informais, correspondência, entrevistas, reposta e questionários e reclamações de clientes;
2. Agrupar os dados em cluster de ideias semelhantes; e
3. Analisar, esclarecer e concordar com o problema a ser tratado.

Outros dados podem ser obtidos na fase 2 onde um grupo focal de cada segmento com experiência em trabalho em conjunto realizará, através do processo de *brainstorming*, uma análise para verificar se faltou alguma ideia a ser colocada. O ideal é que os membros deste grupo devem possuir conhecimento para lidar com as questões a serem discutidas, conforme [93].

Na fase três, todas as ideias são agrupadas com base em suas similaridades e é dado um título para cada família de ideias, sendo o produto final conforme a Figura 2.12. No modelo do Moderno SQFD essas ideias devem ser organizadas no formato de um diagrama de afinidade e devem ser priorizadas de acordo com a sua importância para cada um dos segmentos de usuários envolvidos no grupo multidisciplinar.

Para realizar esta priorização se utiliza o Processo de Análise Hierárquica (AHP), conforme [94]. Método este que visa resolver problemas de múltiplos objetivos, critérios concorrentes, muitas alternativas e outros fatores.

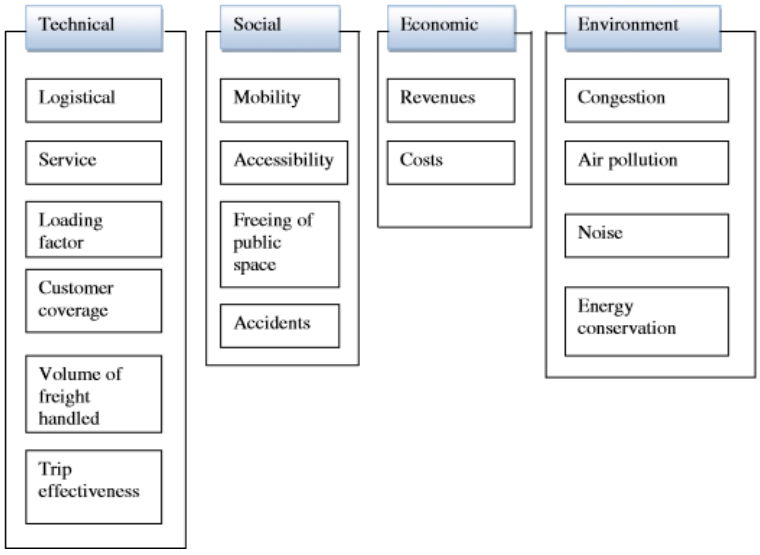


Figura 2.11 – Modelo do diagrama de afinidade, conforme [94].

2.5 O Processo de Análise Hierárquica (AHP)

O processo de Análise Hierárquica foi proposto por [31] tem como objetivo a seleção e escolha de alternativas em um processo decisório que considere múltiplos critérios. Foi um dos primeiros processos desenvolvidos para no ambiente de decisões multicritérios e, para este método, o problema é dividido em níveis hierárquicos, facilitando sua compreensão e avaliação.

Segundo o autor [95], o AHP está estruturado segundo três características:

a) Construção de hierarquias: através do particionamento de elementos é possível compreender melhor sistemas complexos. Estes elementos devem ser estruturados hierarquicamente e, a partir disso, realizar os julgamentos da importância relativa de cada nível de hierarquia em um conjunto de prioridades. Segundo este princípio é preciso definir: o objetivo principal que está sendo hierarquizado (objetivo problema), os critérios (em tantos níveis quanto necessários) e as alternativas, conforme Figura 2.13;

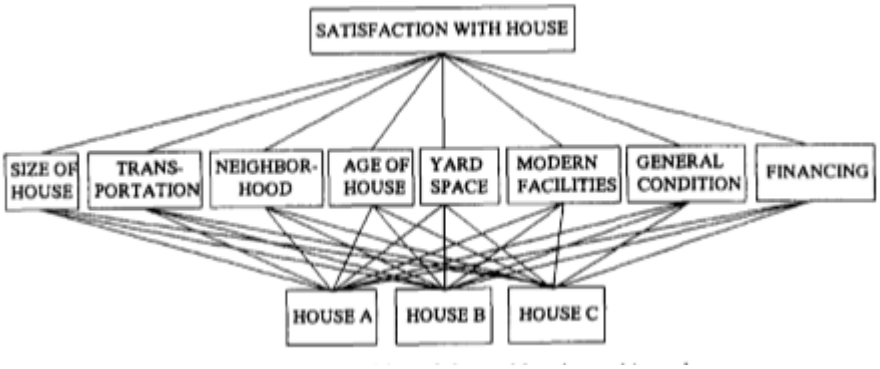


Figura 2.12 – Decomposição de um problema em hierarquia, conforme [96].

b) Definição de prioridades: “o ser humano tem a habilidade de perceber as relações entre as coisas que observa, comparar pares de objetos similares à luz de certos critérios, e discriminar entre os membros de um par a par através do julgamento da intensidade de sua preferência de um elemento sobre o outro” [95]. Para cumprir estes julgamentos foi necessário cumprir alguns passos:

Intensity of importance on an absolute scale	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective
3	Moderate importance of one over another	Experience and judgment strongly favor one activity over another
5	Essential or strong importance	Experience and judgement strongly favor one activity over another
7	Very strong importance	An activity is strongly favored and its dominance demonstrated in practice
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation
2, 4, 6, 8	Intermediate values between the two adjacent judgments	When compromise is needed
Reciprocals	If activity i has one of the above numbers assigned to it when compared with activity j, then j has the reciprocal value when compared with i	
Rationals	Ratios arising from the scale	If consistency were to be forced by obtaining n numerical values to span the matrix

Figura 2.13 – Escala fundamental de Saaty, conforme [31].

- Realização de julgamentos paritários: afim de montar a matriz de comparação é necessário o julgamento de um nível da hierarquia de acordo com o foco de cada elemento pai do nível superior, compondo as matrizes os valores previsto na escala fundamental de Saaty [31], conforme a Figura 2.14. Saaty observa que a percepção deste segue uma escala linear e, levando em consideração o limite psicológico segundo o qual o ser humano pode, no máximo julgar corretamente 7 ± 2 pontos, o limite da escala vai até 9 pontos;

- A quantidade de julgamentos necessários para a construção de uma matriz de comparações genérica A é n (n-1) /2, onde “n” é o número de elementos pertencentes a esta matriz. Os elementos de A são definidos pelas condições previstas na Figura 2.15;

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{21} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 1/a_{n1} & 1/a_{n2} & \cdots & 1 \end{bmatrix}, \text{ onde:}$$

$$a_{ij} > 0 \Rightarrow positiva$$
$$a_{ij} = 1 \therefore a_{ji} = 1$$
$$a_{ij} = 1/a_{ji} \Rightarrow recíproca$$
$$a_{ik} = a_{ij} \cdot a_{jk} \Rightarrow consistência$$

Figura 2.14 – Estrutura da matriz de comparação, adaptado de [95]

- A Normalização das matrizes de comparação: a obtenção da matriz normalizada através da soma dos elementos de cada coluna das matrizes de julgamento e posterior divisão de cada elemento destas matrizes pelo somatório dos valores da respectiva coluna;

- Cálculo dos pesos médios locais (PML's): as PML's são as médias das linhas dos quadros normalizado

- Cálculo das prioridades globais: neste passo deseja-se identificar um vetor de prioridades global (PG), que armazene a prioridade associada a cada alternativa em relação ao foco principal

c) Consistência lógica: com a afirmação de [97] admite-se que a inconsistência pode ser inerente ao comportamento humano. A matriz de decisão que irá gerar as prioridades globais deve ser consistente, sendo que sua inconsistência deve alertar o decisor de como ele está fazendo suas comparações mais do que ser um fato necessariamente não desejável. Assim, [31] propõe o cálculo da Razão de Consistência dos julgamentos (RC), obtida pela fórmula RC = IC/IR, onde IR é o Índice de Consistência Randômico obtido para uma matriz recíproca de ordem n, com elementos não-negativos e gerada randomicamente. O Índice de Consistência (IC) é dado por IC = ($\lambda_{máx}$ –n) / (n-1), onde $\lambda_{máx}$ é o maior autovetor da matriz de julgamentos. Segundo [31], a condição de consistência dos julgamentos é RC ≤ 0,10.

2.5.1 – Conceitos básicos do Processo de Análise Hierarquica (AHP) clássico

Segundo [98], o método AHP clássico proposto por Saaty deve obedecer sete pilares fundamentais: a escalas de razão, proporcionalidade e escalas de razão normalizadas, comparações recíprocas par a par, sensibilidade do principal autovetor direito, homogeneidade e clusterização, síntese que pode ser estendida para dependência e feedback, preservação e reversibilidade de ordem e decisões em grupo.

Na prática o decisor deverá fazer $n\,(n-1)/2$ comparações, sendo n o número de elementos do nível considerado. Na matriz quadrada, tem-se que a_{ij} para i = 1,2, …, n e j =

1,2…, n. estas matrizes são sempre matrizes recíprocas positivas. As comparações par a par são realizadas em todos os níveis hierárquicos.

Assim, considera-se um determinado nível hierárquico e deseja-se determinar os pesos dos elementos em relação a um elemento do nível imediatamente superior da matriz de comparação par a par, por meio do cálculo do autovetor. Desta forma, considerando a_{ij} a matriz formada pelos elementos da comparação par a par, onde denomina-se $A = a_{ij}$. Esta matriz A é recíproca tal que $a_{ij} = {}^{1}/_{a_{ij}}$, na qual em todas as comparações seria possível verificar que $a_{ij} = a_{jk}\ x\ a_{ik}$ para qualquer *i,j,k*. Portanto, segundo esse procedimento, a matriz A seria consistente.

Logo, seja *n* o número de elementos a serem comparados, λ_{max} o autovetor de A e *w* o vetor próprio de correspondente ou vetor de prioridades. Caso os juízos emitidos pelo decisor sejam perfeitamente consistentes, têm-se $\lambda_{max} = n$ e $a_{ij} = {}^{w_i}/_{w_j}$. A inconsistência, fato que é admitido pelo AHP, pode ser medido da seguinte maneira: quanto mais próximo estiver o λ_{max} de *n*, maior será a consistência dos juízos. Portanto, $\lambda_{max} - n$ é um indicador de consistência.

Desta forma, conforme [31], sendo A a matriz de valores, deverá ser encontrado o vetor que satisfaça a equação:

$$Aw = \lambda_{max} * w \tag{2.2}$$

Para obter o autovetor a partir da equação (2.2), tem-se:

$$\lambda_{max} = \frac{1}{n} + \sum_{i=1}^{n}(\text{vi})\,[Aw]i/wi \tag{2.3}$$

Ainda, segundo o autor, observou-se que pequenas variações em a_{ij} implicam pequenas variações em λ_{max} em que o desvio do autovetor em relação a *n* (número de ordem da matriz) é considerado uma medida de consistência. Portanto, é possível afirmar que λ_{max} permite avaliar a proximidade da escala de razões ou quocientes que seria usada se a matriz A fosse totalmente consistente. Isso pode ser feito por meio de um Índice de Consistência (IC).

Logo, se A é consistente, então, quando for calculada a magnitude da perturbação da matriz A, utilizando a relação:

$$IC = (\lambda_{max} - \text{n})/(\text{n} - 1) \tag{2.4}$$

Para ser considerado consistente o RC terá um valor menor ou igual a 0,1. A equação para a Razão de Consistência (RC) é obtida pela fórmula:

$$\mathrm{RC} = \frac{\mathrm{IC}}{\mathrm{IR}} \qquad (2.5)$$

Onde IC corresponde ao Índice de Consistência calculado a partir da fórmula (2.4), que usa um autovetor λ_{max} obtido por meio da multiplicação do autovetor direto pela matriz original. Esse cálculo fornece como resultado um novo vetor, em que cada elemento é dividido pelo elemento correspondente no autovetor, e os resultados são somados, calculando-se, em seguida, a média.

Por sua vez, o IR é um índice aleatório, calculado para matrizes quadradas de ordem *n* pelo Laboratório de *Oak Ridge*, nos estados Unidos. Alguns dos valores de IR são apresentados na tabela 2.16. Quanto maior for RC, maior será a inconsistência. Quando n = 2, RC é nulo; quando n = 3, RC deve ser menor que 0,05; quando *n* = 4, RC deve ser menor que 0,09. Para que a consistência possa ser considerada aceitável, para *n* > 4, o RC ≤ 0,10.

Ordem da Matriz (n)	1	2	3	4	5	6	7	8	9	10	11
Valores de IR	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51

Figura 2.15 – Tabela com o Índice de Consistência Randômico, conforme [99].

Para a montagem da matriz de comparação par a par deve-se observar a definição dos recíprocos, ou seja, quando uma atividade *i* em relação a uma atividade *j* recebe um dos valores da tabela da Figura 2.16, a atividade *j* em relação à atividade *i* receberá o valor recíproco. Cada comparação par a par representa uma estimativa do coeficiente das prioridades ou dos pesos de cada elemento.

Utilizando a matriz de decisão A, o método AHP calcula resultados parciais do conjunto A dentro de cada critério v*i* (A_j), *j* = 1, …, *n*, denominado de **valor de impacto** da alternativa *j* em relação à alternativa *i*, em que esses resultados representam valores numéricos das atribuições verbais dadas pelo decisor a cada comparação de alternativas. Tais resultados são normalizados pela expressão:

$$\sum_{i=1}^{n}(\mathrm{v}i)\,[Aj] = 1 \qquad \mathrm{J} = 1, \ldots, \mathrm{n} \qquad (2.6)$$

Onde *n* corresponde ao número de alternativas ou elementos comparados. Cada parte desse somatório consiste em:

$$v(aij) = \frac{aij}{\sum_{i=1}^{n} \mathbf{aij}} \qquad (2.7)$$

Isso faz com que o vetor de prioridades da alternativa *i* em relação ao critério seja:

$$vk\ (Ai) = \sum_{i=1}^{n} (\mathrm{v}i)\ [Aj]/n \qquad \mathrm{i} = 1,\ \ldots., n \qquad (2.8)$$

Por exemplo, suponha que o decisor, utilizando um grupo de alternativas sob um critério C_k, tenha chegado à seguinte matriz de decisão:

	A1	A2	A3	A4
A1	1	1/5	1/5	1
A2	5	1	1	3
A3	5	1	1	3
A4	1	1/3	1/3	1

Normalizando essa matriz de comparação, utilizando a equação (2.8), tem-se:

	A1	A2	A3	A4
A1	1/12	3/38	3/38	1/8
A2	5/12	15/38	15/38	3/8
A3	5/12	15/38	15/38	3/8
A4	1/12	5/38	5/38	1/8

Assim, usando a equação (2.8), obtém-se o vetor de prioridade, conforme se apresenta a seguir:

v*k* (A1) = (1/12 + 3/8 + 3/38 + 1/8)/4 = 0,36623/4 = 0,09156

v*k* (A2) = (5/12 + 15/38 + 15/38 + 3/8)/4 = 1,58114/4 = 0,39529

v*k* (A3) = (5/12 + 15/38 + 15/38 + 3/8)/4 = 1,58114/4 = 0,39529

v*k* (A4) = (1/12 + 5/38 + 5/38 + 1/8)/4 = 0,47149/4 = 0,11787

Portanto a ordem das alternativas segundo o critério C_k é 0,39529 para as alternativas A2 e A3; 0,11787 para a alternativa A4 e 0,09156 para a alternativa A1, ou seja, A3, A2, A4 e A1 respectivamente. Depois de obtido o vetor de prioridades ou de impacto das alternativas sob cada critério C_k , continua-se com o nível dos critérios. Nesse caso, adota-se novamente a escala verbal para a classificação par a par dos critérios, que são normalizados a partir da equação:

$$wi(Cj) = \frac{Cij}{\sum_{i=1}^{m} Cij} \qquad j = 1, \ldots, m \qquad (2.9)$$

Onde *m* corresponde ao número de critérios de um mesmo nível. O vetor prioridade é:

$$w\,(Ci) = \sum_{j=1}^{m} (wi)\,[Cj]/m \qquad i = 1, \ldots, m \qquad (2.10)$$

Por fim, um processo de agregação permite gerar os valores finais das alternativas, ordenando-se por meio da seguinte função aditiva:

$$f(Aj) = \sum_{i=1}^{m} w\,(Ci) * vi\,(Aj) \qquad j = 1, \ldots, n \qquad (2.11)$$

Relembrando que *n* corresponde ao número de alternativas. Dessa maneira, obtém-se uma ordenação global por intermédio de uma função global de valor.

2.5.2 – Limitações do método AHP

No método AHP, o decisor expressa sua preferência entre duas alternativas comparando-as de acordo com a escala fundamental. Isso gera uma escala de razão de preferências, conflitando com o princípio da função aditiva, que se adapta melhor a uma escala de intervalos.

Contudo, a maior limitação ao AHP refere-se ao problema de inversão de ordem das alternativas. A formulação do Método AHP Clássico é contrária à inversão de ordem, ou seja, a posição relativa das alternativas obtida segundo a função aditiva na equação (2.8) pode ser alterada caso uma alternativa seja adicionada ou removida da análise. A existência de uma alternativa que, ao ser introduzida no problema, ocasiona inversão de ordem mostra que, na fase de modelagem do problema, podem ter ocorrido falhas.

Nesse sentido, três variações do AHP Clássico com o objetivo de resolver o problema de inversão de ordem existem. Os métodos: O AHP Multiplicativo, AHP Referenciado e AHP

B-G os quais apresentam a mesma base teórica do AHP Clássico. Para fins desta pesquisa falaremos apenas sobre o AHP Multiplicativo (MAHP).

2.5.3 – O Processo de Análise Hierárquica Multiplicativo (MAHP)

O método multiplicativo, proposto por [32], é uma variação do método AHP clássico por superar os seguintes pontos críticos: A escala fundamental de proposta por [31] para quantificar os juízos humanos, o uso do autovetor para o cálculo do impacto dos "valores de impacto" das alternativas e os valores finais calculados por uma regra de média aritmética de agregação.

A comparação par a par das alternativas sob um determinado critério é feita baseada na escala verbal de preferências, onde Si é a preferência da alternativa A_i. Essa escala é denominada Escala Natural de Lootsma.

-8	S_i é amplamente menos desejável que S_j
-6	S_i é muito menos desejável que S_j
-4	S_i é menos desejável que S_j
-2	S_i é pouco menos desejável que S_j
0	S_i é indiferente a S_j
2	S_i é pouco menos desejável que S_j
4	S_i é menos desejável que S_j
6	S_i é muito menos desejável que S_j
8	S_i é amplamente menos desejável que S_j

Figura 2.16 – Tabela com a escala Natural de Lootsman, conforme [32].

De acordo com o MAHP, a comparação par a par das alternativas deveria ser baseada numa regra geométrica, e não aritmética, como ocorre no método clássico. Logo, a Escala Natural de Lootsma possui um espectro mais amplo que a Escala Fundamental de Saaty, já que a última não é uma escala geométrica, e, portanto, os valores recíprocos propostos por Saaty podem introduzir uma inconsistência que não está presente na mente do decisor.

Além disso, no limite, a Escala Fundamental representa uma superioridade absoluta, o que não corresponde à realidade. A Escala Natural é mais consistente que a Escala Fundamental, porque não permite a ocorrência dos desvios mencionados. Por fim, a Escala Natural possui uma natureza multiplicativa, apresentando uma tendência natural para evitar a inversão de ordem.

Por conseguinte, durante a aplicação do método USASEC foi utilizada a escala natural de Loostman e não a escala fundamental de Saaty para evitar o erro na interpretação numérica da escala verbal utilizada na comparação.

Contudo é necessário fazer uma comparação entre as escalas tendo em vista que o método USASEC, assim como o moderno QFD, utilizam o método clássico do AHP. Para isso foi utilizada a comparação entre tabelas de [100], conforme Figura 2.17.

Semantic relationship	Value (δ_{ij})	
	MAHP	AHP
Very strong preference for S_i versus S_j	-8	1/9
Strong preference for S_i versus S_j	-6	1/7
Definite preference for S_i versus S_j	-4	1/5
Weak preference for S_i versus S_j	-2	1/3
Indifference between S_i and S_j	1	1
Weak preference for S_j versus S_i	+2	3
Definite preference for S_j versus S_i	+4	5
Strong preference for S_j versus S_i	+6	7
Very strong preference for S_j versus S_i	+8	9

Figura 2.17 – Julgamento comparativo do valor numérico do MAHP para AHP, conforme [100].

Mas apenas a utilização da escala natural ainda não é suficiente para garantir que as matrizes do método AHP tenha razão de consistência menor do que 0,10. Outro problema apresentado pelo AHP, de ordem de aplicabilidade, se encontra no uso do método em situações em que o número de critérios e alternativas é muito grande [101]. Em situações como essas a quantidade de comparações par a par feita pelo decisor cresce muito e gera um grande esforço do decisor em realizar as comparações.

2.5.4 – A linearização da matriz de comparação

Durante o projeto de uma aplicação web vários requisitos podem ser elicitados para compor este software. A grande quantidade de requisitos em comparação e o tempo em que analistas de decisão passam com os decisores é cada vez mais escasso e convencer um alto executivo a dispender horas, quem sabe dias, fazendo comparações par a par, de alternativas e critérios, pode ser inviável.

Ainda, vários autores demonstraram propostas para reduzir o número de comparações e facilitar o acerto no momento de graduar entre duas opções. Os autores [103], propõem reduzir o número necessário de perguntas feitas a cada decisor através da utilização de blocos incompletos administrados a diferentes decisores. Harker, 1987, desenvolveu uma técnica de comparação par a par incompleta (IPC), método que busca reduzir esse esforço por ordenar as perguntas em ordem decrescente de valor informativo e parando o processo quando o valor adicionado de perguntas diminui abaixo de certo nível.

Tabela 2.3 – Tabela com o número de comparações par a par em função do número de critérios e alternativas, conforme [102].

	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	3	7	13	21	31	43	57	73	91
3	6	12	21	33	48	66	87	111	138
4	10	18	30	46	66	90	118	150	186
5	15	25	40	60	85	115	150	190	235
6	21	33	51	75	105	141	183	231	285
7	28	42	63	91	126	168	217	273	336
8	36	52	76	108	148	196	252	316	388
9	45	63	90	126	171	225	288	360	441
10	55	75	105	145	195	255	325	405	495

O AHP usa a capacidade humana de utilizar seu conhecimento e sua experiência para comparar alternativas e critérios par a par e montar as matrizes de [104]. A inconsistência surge quando algumas opiniões da matriz de comparação se contradizem com outras. É importante verificar a consistência das opiniões efetuando uma série de cálculos para chegar ao valor da Razão de Consistência (RC), que indica a consistência ou não da matriz de comparação. Do ponto de vista do AHP, é desejável que a RC de qualquer matriz de comparação seja menor ou igual a 0,10.

Levando em consideração que a matriz de comparação é uma matriz positiva e reciproca, [105] demonstrou a linearização da matriz de comparação pois uma matriz quadrada diz-se reciproca e positiva quando $a_{ij} = {}^{i}/_{a_{ji}}$, para todo $a_{ij} > 0$. Seja uma matriz A reciproca e positiva onde $a_{21} = {}^{1}/_{a_{12}}$, $a_{31} = {}^{1}/_{a_{13}}$, $a_{32} = {}^{1}/_{a_{23}}$ e $a_{ij} = 1$.

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

Uma matriz será consistente quando $a_{ij} = a_{ik} * a_{kj}$. Assim, seja uma matriz A consistente onde $a_{ij} = a_{ik} * a_{kj} = {}^{a_{kj}}/_{a_{ki}}$.

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

Deve-se levar em consideração para o decisor o quanto a permissão de um RC menor ou igual ao de 0,10 pode influenciar a sua recomendação final na escolha da graduação para par dos critérios e alternativas. Ou seja, o quanto se pode ultrapassar o limite de influenciar a decisão do julgamento do decisor para manter-se a matriz o mais consistente possível? Para o método desta pesquisa esta influência é válida pois a aplicação *web*, que está sendo analisada, é uma aplicação crítica, ou seja, aquela que deve dar suporte a um sistema crítico que envolve o resguardo de vidas humanas.

Assim, a linearização da matriz de comparação exige tempo e esforço muito menor do decisor pois exige que ele realize apenas uma linha da matriz de comparação, os demais valores são preenchidos obedecendo os pressupostos matemáticos de uma matriz reciproca, conforme a tabela 2.4.

Tabela 2.4 – Matriz de comparação preenchida pelo processo de linearização de matrizes, conforme [102].

	C1	C2	C3	C4	…..	Cn
C1	1	$C_{c1}/_{c2}$	$C_{c1}/_{c3}$	$C_{c1}/_{c4}$	….	$C_{c1}/_{cn}$
C2	$1/C_{c1}/_{c2}$	1	$C_{c1}/_{c3} / C_{c1}/_{c2}$	$C_{c1}/_{c4} / C_{c1}/_{c2}$	….	$C_{c1}/_{cn} / C_{c1}/_{c2}$
C3	$1/C_{c1}/_{c3}$	$C_{c1}/_{c2} / C_{c1}/_{c3}$	1	$C_{c1}/_{c4} / C_{c1}/_{c3}$	….	$C_{c1}/_{cn} / C_{c1}/_{c3}$
C4	$1/C_{c1}/_{c4}$	$C_{c1}/_{c2} / C_{c1}/_{c4}$	$C_{c1}/_{c3} / C_{c1}/_{c4}$	1	….	$C_{c1}/_{cn} / C_{c1}/_{c4}$
….	….	….	….	….	….	….
Cn	$1/C_{c1}/_{cn}$	$C_{c1}/_{c2} / C_{c1}/_{cn}$	$C_{c1}/_{c3} / C_{c1}/_{cn}$	$C_{c1}/_{c4} / C_{c1}/_{cn}$	….	1

Apenas para exemplificar que a matriz de comparação satisfaz o critério de consistência e reciprocidade, ou seja, $a_{ij} = a_{ik}$ x $a_{kj} = {a_{kj}}/{a_{ki}}$, realiza-se o seguinte teste:

$a_{21} = {C_{c1}/_{c1}} / {C_{c1}/_{c2}}$ e $a_{13} = C_{c1}/_{c3}$. Logo $a_{23} = a_{21}$ x $a_{13} = {C_{c1}/_{c1}} / {C_{c1}/_{c2}}$ x $C_{c1}/_{c3}$

Como $C_{c1/c1}$ = 1, então, $a_{23} = {}^{C\ c1/c3}\big/_{C_{c1/c2}}$.

Este método reduzirá o esforço dos decisores e aumentará a possibilidade de matrizes de comparação sem inconsistência. Utilizando apenas o método AHP tradicional, um problema com sete critérios e oito alternativas teria 217 comparações a serem realizadas, segundo a tabela 2.3. Contudo, utilizando a linearização de matrizes este número de comparações reduziria para 55, conforme tabela 2.5.

Reduzir o esforço mental do julgamento dos decisores, facilitará a produção de matriz com índices consistentes e evitará o retrabalho para preencher outro formulário de priorização de requisitos.

Tabela 2.5 - Tabela com o número de comparações par a par em função do número de critérios e alternativas, conforme [105].

	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	3	5	7	9	11	13	15	17	19
3	5	8	11	14	17	20	23	26	29
4	7	11	15	19	26	27	31	35	39
5	9	14	19	24	29	34	39	44	49
6	11	17	23	29	35	41	47	53	59
7	13	20	27	34	41	48	55	62	69
8	15	23	31	39	47	55	63	71	79
9	17	26	35	44	53	62	71	80	89
10	19	29	39	49	59	69	79	89	99

Apesar de todas as técnicas utilizadas para manter o esforço em matriz consistentes, ainda assim, não é garantido que a opinião dos decisores consiga alcançá-las. Por isso, o formulário de priorização de requisitos, anexo B, deve ser executado mais de uma vez até que as matrizes de comparação tenham seus valores consistentes. Só assim, é possível garantir que o julgamento dos decisores será consistente e que se julgamento, apesar de inicialmente gerar matriz inconsistente, será respeitado. Cabe ressaltar que apenas o decisor deve alterar seu julgamento, não cabendo ao pesquisador a mudança dos julgamentos feitos pelo mesmo.

Ainda, é necessário considerar que o envolvimento de múltiplos decisores aumenta a dificuldade de realizar os julgamentos para cada um dos critérios e subcritérios que estão sendo avaliados.

2.5.5 – O AHP com múltiplos decisores

Segundo [106], dentro de um grupo de decisores existe grande diferença em termos de formação profissional, competência e experiência no âmbito de um problema decisório. Soma-se a isso, nem sempre todos os decisores têm o mesmo interesse na análise do problema e os critérios a serem avaliados podem ser essencialmente técnicos (muitos avaliadores podem não estar habilitados a julgar à luz destes critérios).

A partir disso, fica evidente a importância da escolha do grupo multidisciplinar focal pois, caso estes avaliadores ou decisores não sejam qualificados para contribuir no processo decisório, os resultados podem ser controversos.

Quando os avaliadores têm interesses e objetivos idênticos quanto ao julgamento dos critérios, segundo [107] relata-se que o AHP pode ser utilizado em quatro contextos:

1. Sistema de Votação – caso o consenso entre os julgamentos não for atingido em determinada situação, devido às experiências de cada decisor e seu nível de comprometimento com a solução, o grupo de avaliadores pode realizar uma votação para escolher um julgamento intermediário;

2. Modelo distinto e avaliadores – se os avaliadores têm perspectivas do objetivo muito divergentes ou não podem se encontrar para discutir a decisão, cada decisor pode emitir suas decisões separadamente. Para realizar os modelos distintos cada avaliador atribui seus julgamentos em um modelo onde as prioridades resultantes podem ser obtidas pelo cálculo da média dos julgamentos;

3. Consenso – se os avaliadores têm os mesmos objetivos, é aconselhável que estes se reúnam e se esforcem para obter o consenso na estruturação do problema e nos julgamentos da importância relativa de cada critério e alternativas; e

4. Uso da média geométrica – se não for possível realizar uma votação e os membros da equipe não chegarem a um consenso, a média geométrica dos julgamentos dos membros deve ser calculada. De acordo com [108], foi demonstrado que quando o mesmo valor de importância for atribuída a cada membro do grupo, a média

geométrica é a forma mais apropriada para sintetizar os julgamentos obtidos por cada membro do grupo.

Ainda, é possível propor a determinação da importância relativa de cada avaliador, utilizando o próprio AHP, através de comparações paritárias interpessoais da importância ou influência dos membros avaliadores no processo decisório. Entretanto, segundo [109], este procedimento pode causar um desvio no processo decisório visto que há uma tendência de um indivíduo superestimar sua própria importância.

3 O método proposto de Integração de Requisitos de Usabilidade e Segurança para Proteção Cibernética em Aplicações Web

O método de integração de requisitos de usabilidade e segurança para proteção cibernética em aplicações Web, denominado de USASEC, nomeado a partir do termo em inglês ***USA****bility* e ***SEC****urity*, desenvolvido para coletar, filtrar, priorizar, classificar e integrar requisitos de usabilidade e segurança e seus impactos para aplicações *web* através de nove passos. Ele utiliza o Moderno SQFD, conforme seção 2.3.2, com ênfase em usabilidade e segurança; onde os métodos KJ, bem como, o AHP, seções 2.4 e 2.5, respectivamente, com ênfase em requisitos de usabilidade e o método da casa da qualidade, conforme seção 2.3, integra os requisitos usabilidade quantificados com requisitos de segurança, também quantificados.

Para a realização do método USASEC, delineia-se segmentos de usuários e, através de suas necessidades expostas no questionário aberto sobre usabilidade, apêndice A, identificam-se as principais necessidades e tarefas de cada um deles no software. Ao longo dos passos, após preencher o questionário aberto, estes usuários têm suas funções exercidas por uma equipe multidisciplinar (EM) composta por: administradores do sistema, analistas de segurança e desenvolvedores, que participam da elaboração e utilizam do software.

O método USASEC é aproveitado por equipes de desenvolvimento de software que procuram aumentar a satisfação dos seus clientes, incluindo-os no seu processo de melhoria, coma intenção de ganhar segurança e qualidade com os requisitos os quais devem ser priorizados.

O método proposto tem grande valia ao quantificar os requisitos e priorizar os mais importantes, além de, considerar a segurança da informação que a aplicação necessitar para atender as necessidades dos usuários.

3.1 Processo conceitual do método

Este trabalho de pesquisa se concentra nas atividades de análise de requisitos de usabilidade e segurança aplicavéis tanto na fase de exploração e elicitação dos requisitos de novo produto de software, como, na sua fase final de melhoria, conforme mostrado na Figura 3.1.

Inicialmente, executado na fase de exploração e requisitos, o método proposto vai entender melhor as necessidades dos usuários, quanto a *Usability*, facilitando o entendimento do problema que ele se propicia em resolver para o usuário. O objetivo deste passo do método pretende incluir o usuário no processo de desenvolvimento de forma mais efetiva. Para isto, faz-se necessário ir até o local de trabalho do usuário; ouvir suas tarefas, expectativas, experiências e motivações para o uso da aplicação.

Conforme mostrado na Figura 3.1, a fase 1 de exploração corresponde ao planejamento da aplicação. Para o USASEC, toda nova aplicação ou funcionalidade precisa ser planejada, desde o início, por todos os profissionais da equipe multidisciplinar do método. Os profissionais que fazem parte da equipe multidisciplinar devem entender qual o objetivo estratégico da organização que a aplicação vai atender, quais os segmentos de usuários chaves que conseguirão ser atendidos por ela e qual a expectativas destes clientes quanto as tarefas que pertencerão a aplicação.

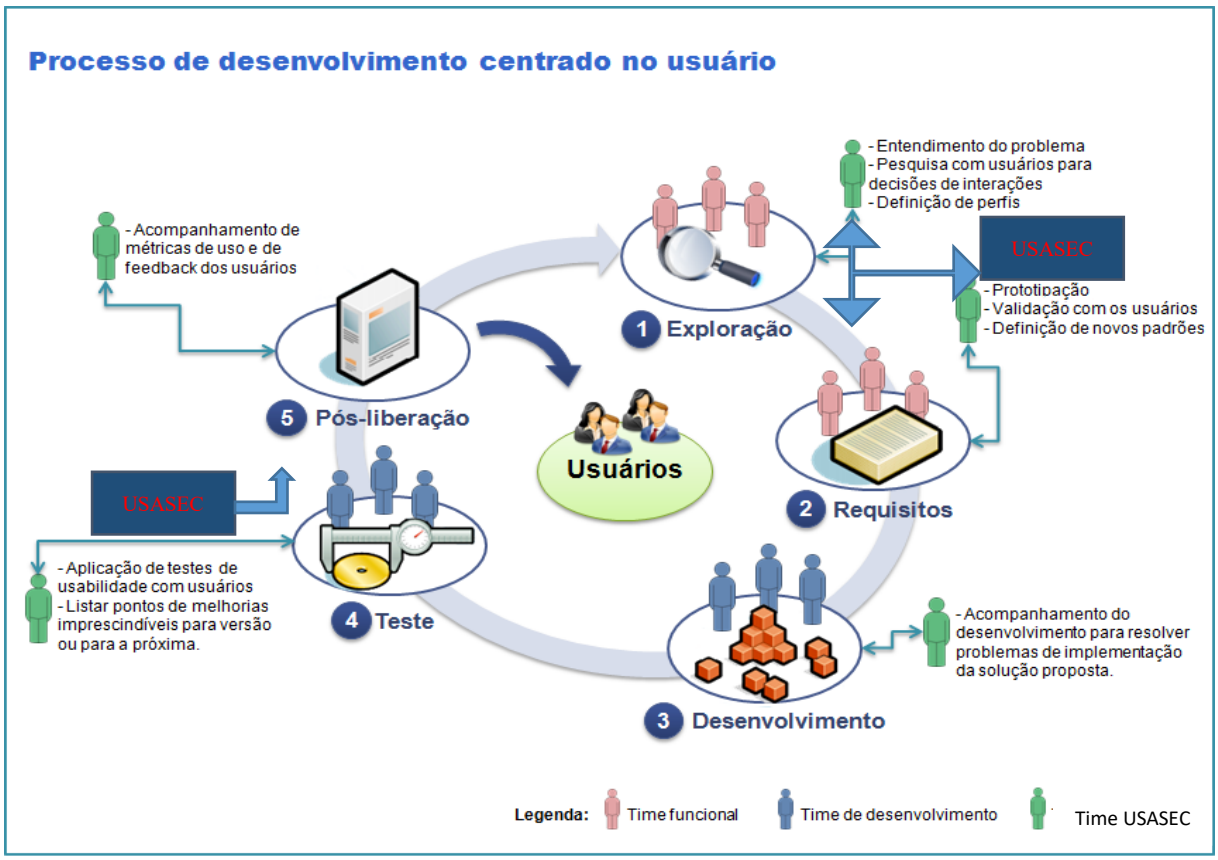


Figura 3.1 – Processo conceitual para aplicação do método USASEC, adaptado de [110].

Contudo, para o método USASEC, não é traçado perfis para os usuários. Estes perfis ficarão ligados aos níveis de interação que o usuário deve possuir com a aplicação, como: usuários comuns, administradores da aplicação, desenvolvedores e proprietário.

Para a fase de requisitos, fase 2, é necessário entender como os diversos segmentos de usuário pensam a aplicação. Para isso, será necessário ouvir a voz do usuário (UoV), e não apenas com a explicação de analistas de negócio, funcionais ou líderes de produto.

Assim, é necessário entender o modelo mental dos segmentos de usuários que estão sendo ouvidos. E, consequência, é necessário a prototipação da aplicação, diagramas de tarefas ou linguagem de modelo unificada (UML) da aplicação, para trazer análise e validação para o UoV. Além disso, com a ida até o local de trabalho dos usuários é possível a definição de novos padrões de tarefas para a aplicação, ainda não identificados.

Para a fase de desenvolvimento, fase 3, o método USASEC deve apenas acompanhar o desenvolvimento para garantir a padronização dos requisitos que foram priorizados e propostos durante a sua execução. Os requisitos de usabilidade e segurança devem ser levados em consideração durante toda a fase.

Caso a equipe de desenvolvedores encontre algum problema técnico durante esta fase, todo a equipe multidisciplinar deve ser reunida para analisar a necessidade ou não de realizar um novo ciclo do método. Um problema muito frequente é a inclusão de novos requisitos durante a fase de desenvolvimento; caso isso ocorra a equipe multidisciplinar deve analisar se este novo requisito pode entrar em níveis secundários ou terciários do diagrama de árvore do método, desta forma não será necessário realizar todo o ciclo do método. Caso contrário, será necessário realizar todo o ciclo.

O método USASEC pode ser executado na fase de pós-liberação, fase 5, sendo esta uma forma mais rápida e simples de aplicar o método, utilizando todos os passos previsto. Ele tem as características de ser mais rápido e simples nesta fase do desenvolvimento da aplicação por ter a prototipação e a linguagem de modelo unificada já prontas. Nesta fase, o método deve acompanhar as principais ideias de melhorias dos segmentos chaves de usuários da aplicação e corrigir eventuais erros que possam comprometer a satisfação e segurança destes.

A grande diferença do método USASEC, em relação ao método UX (*User Experience*), está relacionado que este não visa apenas entender o usuário e satisfazê-lo, mas também, atender as questões técnicas de segurança que são uma preocupação da equipe técnica, com o balanceamento do impacto que cada um dos requisitos de usabilidade afeta os requisitos de segurança, a qual pode colocar o usuário e a aplicação em uma situação crítica de segurança.

3.2 Fundamentos do método proposto

O Desdobramento da Função de Qualidade de Software (SQFD), descrito na seção 2.3, se baseia em conceitos e características adaptadas para requisitos de usabilidade e segurança da aplicação *web*.

Para a concepção do método USASEC, algumas características do método SQFD foram utilizadas como base para fundamentação do método proposto, especificamente em seu passo de número nove, conforme seção 3.3.9. Com isto, foi possível incorporar as vantagens que o método SQFD já possuía para o modelo USASEC.

A tabela 3.1 apresenta as principais características e princípios que fundamentaram o método USASEC e seu relacionamento com o método SQFD, discutido na seção 2.3.2; bem como, as vantagens adquiridas com a utilização deste método, em comparação com as vantagens de utilização do modelo SQFD.

Tabela 3.1 – Comparação das características do método Moderno SQFD em relação ao método USASEC

N°	Valores, princípios ou características	Referência
01	Valoriza a voz do usuário e sua satisfação com a aplicação como ponto de partida para o método.	Segundo SQFD, deve-se ouvir o usuário.
02	Pessoas da organização, de diferentes segmentos de usuários da aplicação, vão trabalhar juntas para chegar a uma solução de comprometimento para a melhora da aplicação. (Equipe multidisciplinar)	Conceito previsto no moderno SQFD que visa ter todos os segmentos de usuários participando da análise.
03	Mudança de requisitos podem ocorrer, mesmo que tardias, pois serão incluídas na UVT como ideias relacionadas.	Requisitos filtrados dentro de cluster por similaridade.
04	Ir no local onde os usuários da aplicação vão utilizá-la para ouvir deles suas necessidades quanto as melhorias de usabilidade.	Conceito do moderno SQFD que visa ter a real necessidade do usuário atendida.
05	Organizar as ideias em metas de usabilidade de forma hierárquica para melhor organizá-las.	Conceito do SQFD que utiliza o diagrama de afinidade para organizar as

		ideias e transforma em requisitos.
06	Utilizar o método AHP Clássico com as ferramentas de linearização da matriz de comparação e tabela de Lootsma.	Quantificar os requisitos de usabilidade, conceito do SQFD.
07	Aplicar a casa da qualidade para integrar o quanto cada requisito de usabilidade impacta os requisitos de segurança, e vice-e-versa.	Característica do moderno SQFD que identificar quais requisitos da aplicação mais impactam a qualidade final do produto.

Ainda para o método proposto, devemos considerar a segurança da informação como um fator relacionado a proteção cibernética da aplicação *web*. A proteção cibernética, definida na seção 2.2.4, está em constante modificação e evolui para melhor atender as demandas das organizações e satisfazer a segurança dos seus clientes. Sendo a proteção cibernética, conforme definição na seção de referência, uma atividade de caráter permanente.

A integração desses dois requisitos não funcionais de software, usabilidade e segurança, têm a possibilidade de indicar forças competitivas e orientar a alocação de recursos para os requisitos mais importantes durante o desenvolvimento ou melhoria da qualidade do software.

3.3 O Método USASEC

Para elaboração do método USASEC, foram considerados os conceitos de usabilidade, descritos no Método Empírico de Avaliação de Usabilidade por Percurso Pluralístico, da seção 2.1.1.4, bem como os conceitos e metas de usabilidade [30], descritos na seção 2.1. Ainda, para os requisitos de segurança da informação foram considerados os conceitos da seção 2.2.2, bem como os 10 tipos de ataques mais comum executados contra aplicações web, descritos na seção 2.2.3.

Este método visa a beneficiar a comunidade científica com uma possível forma de se solucionar conflitos existentes entre os requisitos de segurança e usabilidade para o desenvolvimento de softwares e identificar requisitos chaves para satisfazer os usuários sem comprometer a segurança. Ainda, o método propõe um esforço direcionado nestes requisitos, durante o desenvolvimento do software, proporcionando melhores possibilidades de satisfação

do usuário e acrescentando requisitos técnicos de segurança da informação para proteção cibernética da aplicação.

Durante a realização do método USASEC, proposto neste trabalho, ficou evidente a utilização dos nove passos do moderno SQFD com ênfase em usabilidade e segurança, conforme se encontra descrito na seção 2.3.2. Logo, os nove passos necessárias para a utilização do método USASEC são assim descritas, conforme Figura 3.2.

3.3.1 Passo 1 – Definir o objetivo principal da aplicação

No primeiro passo para o método USASEC faz-se necessário identificar qual a estratégia da organização, qual a relação da aplicação *web* com a estratégia de negócio da organização e como o método USASEC pode ser aplicado para este tipo de software. Existem aplicações *web* críticas para a instituição como *e-comerce,* serviços de banco e diretamente ligadas a atividade principal da organização.

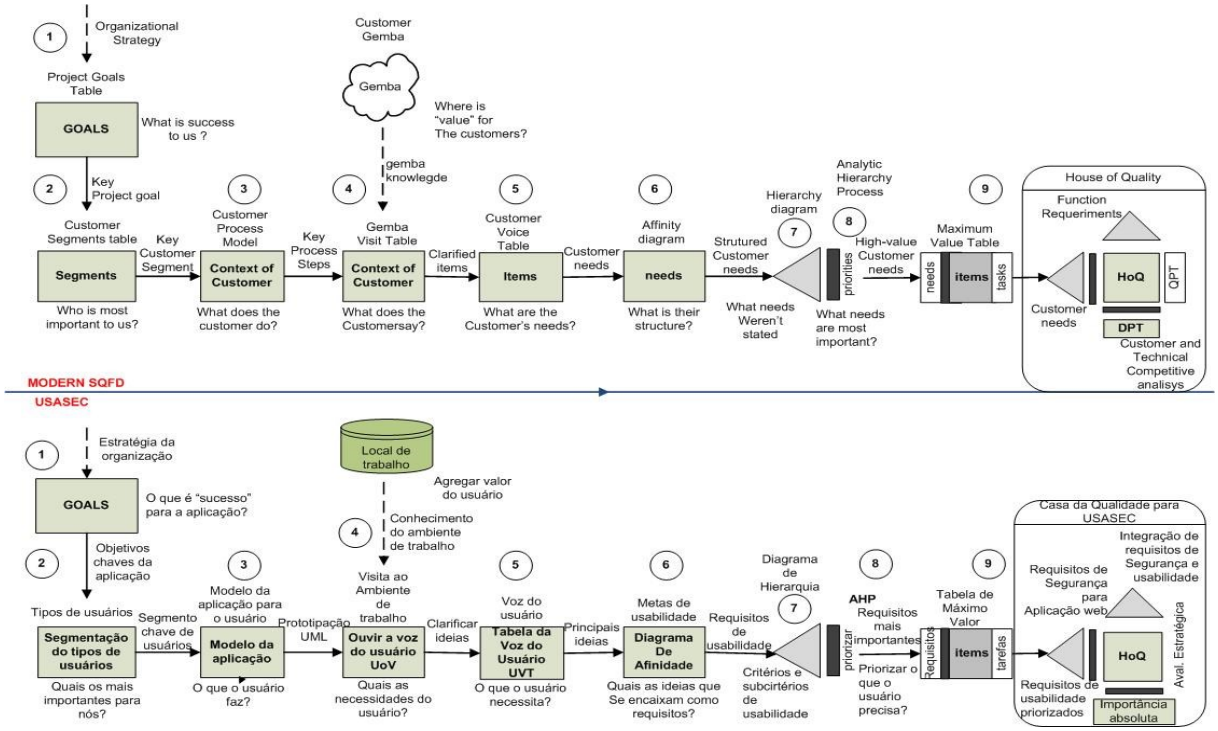


Figura 3.2 – Comparação entre o método SQFD e o método USASEC

3.3.2 Passo 2 - Identificar o segmento de usuários

No passo dois do método USASEC, através da segmentação dos usuários, pode-se identificar quais deles são chaves para a identificação das ideias necessárias para a sua

satisfação. Ou seja, quais usuários devem ser satisfeitos para a obtenção do sucesso da aplicação. Portanto, deve-se identificar os tipos de usuários que se deseja agradar e qual sua importância relativa para o projeto do software. Como reunir todos os usuários é muito trabalhoso, deve ser feita uma entrevista, questionário ou visita para um subconjunto deles. Por isso, é fundamental identificar os segmentos deles, para que pelo menos 1 de cada segmento, possa ser ouvido.

3.3.3 Passo 3 - Criar um modelo da aplicação

No passo três do método, agora que foi identificado o segmento que deve ser ouvido para garantir o sucesso, deve-se criar um modelo do sistema caso esteja sendo aplicado o método USASEC na fase 1 e 2 do ciclo de vida do software, conforme Figura 3.1. Este modelo pode consistir de diagramas de fluxos, diagrama de UML ou prototipação, o que for melhor para que os futuros usuários possam entender como será feita a execução das tarefas que ele necessita no software. Através destes modelos pode-se entender o que os usuários fazem e o porquê; assim como, quais seus problemas e qual a dificuldades deles. Uma das dificuldades encontradas, nesta fase, é tentar descobrir o que o usuário pensa que quer ou acha que precisa, por isso, acredita-se que a fase 5 é a mais interessante para aplicação do método.

Caso o método esteja sendo aplicado na fase 5 da Figura 3.1, deve-se apenas ir até o local onde o sistema está sendo utilizado e aplicar o questionário aberto, conforme anexo A, de usabilidade a amostra do grupo segmentado do local.

3.3.4 Passo 4 – Visitar o local da utilização da aplicação

Durante o passo 4 do método, deve-se a ir ao local de trabalho, ou seja, onde a aplicação *web* será utilizada e aplicar o questionário aberto para coletar as ideias de usabilidade que os usuários acreditam que podem trazer melhorias a aplicação. O objetivo é entender o que os usuários fazem e porque fazem. Neste passo, de acordo com o método de avaliação pluralístico, seção 2.1.1.4, tanto desenvolvedores quanto usuários comuns e até outros tipos de usuários devem ser ouvidos (diversidade de *stakeholders*). Esta pluralidade de usuários tem por objetivo levantar diversos pontos de vista sobre as diferentes tarefas que a aplicação deve realizar.

O questionário deverá ser realizado no ambiente onde o software está sendo utilizado, ou seja, no seu local de trabalho. O usuário deve utilizar termos não técnicos para expor sua "voz", estes termos não técnicos são chamados de verbatims; que significa ideias palavra por

palavra. Desta forma, caso o pesquisador tenha alguma dúvida do que o usuário escreveu, o aplicador do método poderá pedir mais detalhes sobre a dificuldade que o usuário está tentando expressar na tarefa que ele precisa realizar na aplicação.

Para coletar as ideias dos usuários é utilizado um questionário aberto, definido na seção 2.3.2, que colhe as principais ideias de melhoria para satisfação quanto a usabilidade, conforme seção 2.3.2, dos vários segmentos de usuário, chamado de questionário aberto, este foi confeccionado de acordo com as normas de metodologia científica, conforme apêndice A.

3.3.5 Passo 5 - Filtrar as necessidades dos usuários

Para este passo do método, deve-se compreender claramente as afirmações colocadas no questionário antes de compreender o que vai satisfazê-lo. Algumas declarações como portabilidade, custo, tecnologias e usabilidades são bem diferentes dos verbatims para o que o usuário precisa. Por isso, cabe ao aplicador do método e ao grupo multidisciplinar, montado com indivíduos de cada segmento, classificar as ideias e separá-las por similaridade. Para isso, a equipe deve, caso necessário, voltar ao local onde o usuário colocou a sua ideia e sanar dúvidas quanto a real necessidade do usuário.

De posse de todas as ideias é montada a *User Voice Table* (UVT), tabela com a voz do usuário, para separar as ideias semelhantes de um problema para atingir um objetivo em comum.

Só assim, pode-se separar as principais ideias que satisfazem os usuários. Aquelas ideias que não serão classificadas como verbatims de usabilidade devem ser catalogadas e colocadas em outros grupos que poderão ser formados futuramente para classificação. Caso a equipe multidisciplinar fique em dúvida sobre o que o usuário tentou expressar, ela pode ir outra vez até o local de trabalho para entender o que o usuário tentou escrever.

3.3.6 Passo 6 - Elaborar o diagrama de afinidade dos requisitos

Neste passo do USASEC, de posse das ideias passadas pelos usuários filtradas pela UVT, deve-se organizá-las de acordo com a análise de suas características e as necessidades do usuário. Para isso, utiliza-se o método KJ para gerar o diagrama de afinidade, conforme seção 2.4. Este método revela a estrutura natural das necessidades do usuário, ou seja, como os diversos usuários pensam sobre suas tarefas realizadas na aplicação.

A estrutura do diagrama de afinidade é feita e, de posse das ideias primárias já filtradas no passo anterior, o método USASEC utiliza os conceitos de usabilidade e metas de usabilidade de [30], conforme seção 2.1, para organizar as ideias que se tornarão requisitos de usabilidades quando são ligadas a uma meta de usabilidade. Estas ideias a partir deste instante passam a ser um requisito pois é uma condição ou uma capacidade com a qual o sistema deve estar de acordo e estão ligadas a uma meta "pai", tendo vista que a definição de meta corresponde a um resultado final a ser alcançado, um fim exato e quantitativo almejado pelo usuário.

Contudo, estes requisitos ainda devem ser hierarquizados, quantificados e priorizados de acordo com o próximo passo, o diagrama hierárquico.

3.3.7 Passo 7 - Montar o diagrama hierárquico

Para este passo, durante um procedimento de organização simples, transforma-se o diagrama de afinidade em diagrama hierárquico. Estrutura-se as metas de usabilidade e seus requisitos classificados no diagrama de afinidade em uma estrutura hierárquica, conforme Figura 3.3.

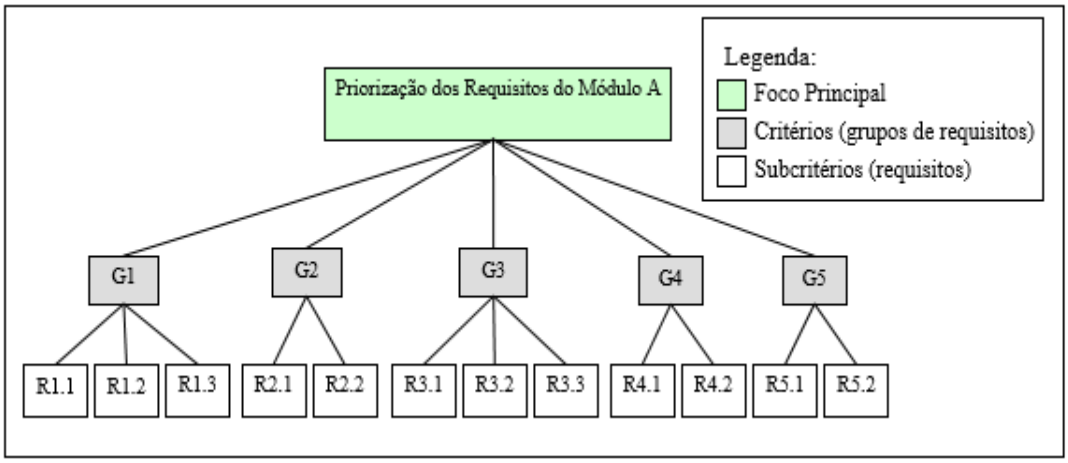


Figura 3.3 – Exemplo da montagem do diagrama hierárquico, adaptado de [111].

Com o formato da Figura 3.3, fica mais fácil a identificação para validação dos membros da equipe multidisciplinar (EM) de quais critérios (metas de usabilidade) e subcritérios (requisitos de usabilidade) serão julgadas par a par na próxima passo, o processo de análise hierárquica.

3.3.8 Passo 8 – Realizar Análise do Processo Hierárquico (AHP)

Neste passo, após colocar os requisitos escolhidos pelos usuários em uma estrutura hierárquica, pode-se identificar aqueles que estão conectados a mais de uma meta de usabilidade

e busca-se quantificá-los em uma ordem de importância de acordo com os julgamentos de cada membro do grupo multidisciplinar.

O Processo de Análise Hierarquica (AHP), do inglês *Analytic Hierarchy Process*, é um processo de auxílio multicritério de tomada de decisão, conforme seção 2.5. Ele é utilizado para priorizar requisitos do usuário em um diagrama de hierarquia. Tradicionalmente, seria realizada esta priorização utilizando uma escala de Likert (1 a 5). Contudo, a utilização do AHP mostra um resultado mais preciso quanto a classificação destes dados e requer um pouco mais de esforço.

A importância deste processo aumenta quando se observa uma aplicação crítica que necessita de precisão pois, o método USASEC, está voltada para as aplicações que respondem pelo negócio estratégico da organização. Desta forma, a priorizações corretas destas necessidades aumenta a possibilidade de satisfazer as necessidades dos usuários e, assim, comprometendo o mesmo de utilizar o sistema com mais atenção e cuidado para o resguardo de vidas.

Para o método USASEC são utilizadas complementações ao método clássico exposto por Saaty, todas as variações que foram implementadas visam evitar a inversão de ordem e a inconsistência das matrizes. São elas: A utilização da tabela natural de Loostman, conforme Figura 2.17 e seção 2.5.3, aplicado ao grupo multidisciplinar de acordo com o formulário de priorização dos requisitos utilizando o método AHP, conforme anexo B, para evitar uma errada interpretação para os pesos dos critérios, representando a importância relativa. Realizar uma linearização da matriz de comparação, conforme seção 2.5.4, afim de reduzir o esforço mental dos indivíduos do grupo focal tendo em vista o grande número de requisitos previstos em um projeto de software.

Assim, será dado aos membros do grupo focal o formulário de priorização de requisitos, conforme anexo B, para que todos respondam individualmente. Este formulário será utilizado para a montagem da matriz de comparação e normalização, de acordo com a linearização das matrizes e o cálculo do AHP, seção 2.5.4 e 2.5.1 respectivamente. O formulário faz uma comparação par-a-par de cada requisito (subcritério) em relação ao seu critério (meta de usabilidade) “pai”, e uma comparação entre os critérios (metas de usabilidade) em relação ao objetivo global (usabilidade). Os valores dos julgamentos seguem a escala de Loostma, contudo, durante a realização do AHP, estes valores são convertidos segundo a escala de Olson, conforme Figura 2.18 da seção 2.5.3.

O formulário de priorização dos requisitos pode ser preenchido quantas vezes for necessário pelo membro do grupo, até que todos os julgamentos possam gerar matrizes

consistentes. Sendo assim, existe um esforço do aplicador do método para que o julgamento do membro da equipe seja atendido, mas este não pode ultrapassar o limite para ter resultados consistentes.

Após isso, tendo o peso (importância relativa) da matriz de normalização consistente de cada um dos requisitos e seus critérios, deve-se ter uma importância relativa global para cada um dos requisitos tendo em vista os múltiplos decisores que estão julgando-os. Para isso, conforme seção 2.5.5, será calculada a média geométrica de cada grupo de julgamento com base no seu critério "pai" para cada um dos membros da equipe multidisciplinar. Ou seja, será feita uma média geométrica dos pesos, por exemplo, dos requisitos com foco na aprendizagem de todos os atores da equipe multidisciplinar e assim por diante.

Uma vez obtida a importância relativa de cada critério (meta de usabilidade) à luz do foco principal e importância relativa de cada subcritério (requisito) à luz de cada critério para cada usuário; a importância relativa global de cada subcritério pode ser obtida, fazendo-se o somatório dos produtos da importância deste subcritério à luz de cada critério pela importância relativa do critério correspondente, à luz do foco principal, e dividindo-se pelo total de usuários participantes da avaliação.

Para o método proposto, método USASEC, tendo em vista há não influência de superiores hierárquicos e decisores no julgamento dos critérios é utilizado o processo de média geométrica para obtenção da importância relativa dos diversos julgamentos emitidos pelos decisores do grupo, conforme definido na seção 2.5.5. Caso a matriz de consistência não alcance o valor abaixo de 0,10, apesar de todas as tentativas de refazer o julgamento do requisito junto com o membro da equipe focal, o valor daquele requisito é desconsiderado para o MVT.

Após a classificação dos requisitos mais importantes através do processo de análise hierárquica (AHP), é importante validar os resultados através do questionário fechado, apêndice E, com usuários que não participaram da coleta de dados do método. Assim, é possível comprovar a taxa de acerto dos julgamentos da Equipe Multidisciplinar (EM) em relação aos requisitos que mais satisfazem os usuários.

3.3.9 Elaborar a casa da qualidade do método USASEC

Conforme a seção 2.3, a casa da qualidade é a primeira fase do método SQFD e serve para criar a matriz das necessidades dos clientes com as características técnicas de qualidade do produto. Esta tem por objetivo responder o que significa um "bom produto" para os nossos clientes. Os requisitos de um "bom produto" são mapeados através da "voz do cliente" e

representadas em atributos para o produto. Estes atributos são integrados as características de qualidade do produto para indicar o maior esforço nos atributos que podem satisfazer as necessidades do cliente. Para detalhar este último passo do método USASEC, será explicado cada passo segundo a Figura 3.4.

Neste passo final, deve-se colocar os subcritérios ponderados de usabilidade elencados pelo AHP, denominada de Tabela de Valor Máximo (do inglês *Maximum Value Table*), no lado esquerdo na Matriz de Usabilidade e Segurança, onde estão especificados os requisitos de usabilidade do usuário.

Na parte superior da matriz são colocados os princípios de segurança da informação que devem ser considerados para análise em relação aos requisitos de usabilidade, caracterizando os requisitos técnicos da matriz do QFD. Para os requisitos de segurança da informação, eles serão ponderados de acordo com as necessidades da equipe de desenvolvimento da aplicação e serão relacionados com o tipo de agente externo (vulnerabilidade) considerado crítico para sua aplicação. As vulnerabilidades analisadas são aqueles previstas em [7], conforme seção 2.2.3, ou aquelas que a equipe técnica julgar como possíveis de incidirem contra a aplicação.

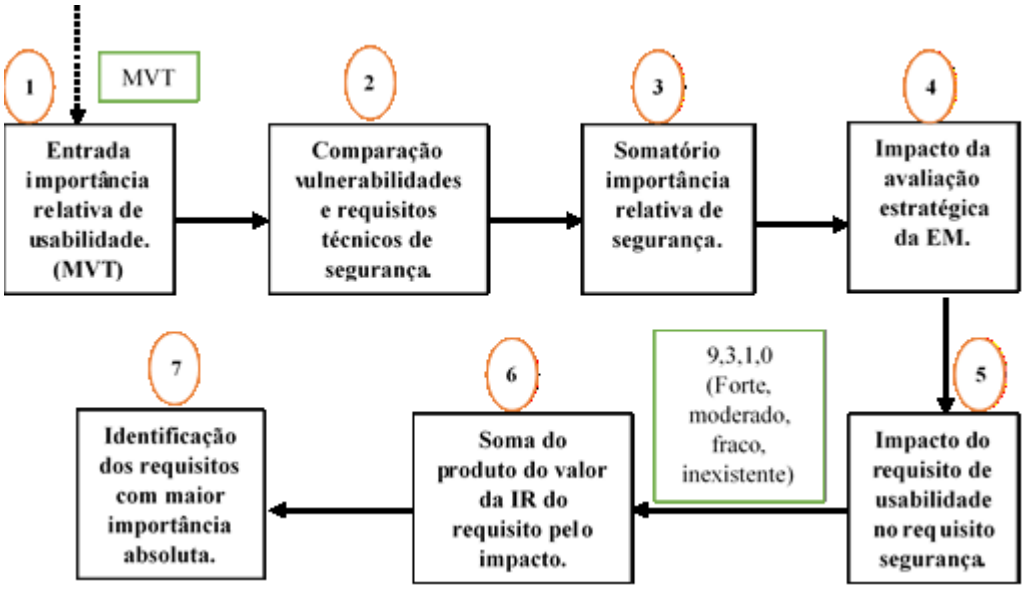


Figura 3.4 – Fluxograma dos passos da casa da qualidade.

De acordo com a Figura 3.3, para cada vulnerabilidade será relacionada com os princípios de segurança da informação. Havendo a possibilidade de ocorrer um incidente de segurança durante a análise da vulnerabilidade com o princípio de segurança que está sendo levado em consideração, a equipe técnica pode julgar que está vulnerabilidade afeta os

princípios de segurança, de acordo com a natureza da sua aplicação, quantificando-o com 1 ponto, representado com o sinal de "+" na Figura 3.3.

Desta forma, todas as vulnerabilidades serão analisadas de acordo com todos os princípios. O Somatório final da pontuação de cada vulnerabilidade que impacta o princípio de segurança dará a importância relativa destes princípios, sendo o valor máximo de 10 e mínimo de zero.

Feito os relacionamentos entre as características técnicas de segurança da informação que se aplicam aquele software, deve-se realizar o relacionamento entre os requisitos de usabilidade e de segurança que mais impactam o software. Para isso, será utilizada a métrica tradicional do QFD para software, onde se quantifica que o impacto entre o relacionamento dos requisitos de acordo com a seguinte graduação: Forte = 9, moderado = 3, fraco=1, conforme explicado na seção 2.3.1.

Por fim, do somatório do produto da importância relativa de cada requisito com o valor atribuído de seu julgamento pela equipe multidisciplinar, serão obtidos os valores absolutos para cada requisito. Com esta avaliação, é possível identificar quais requisitos de usabilidade e segurança, agora integrados, mais impactam o produto final do software. Além disso, dá suporte à decisão de quais requisitos devem ser melhorados para satisfazer o cliente e dar ênfase a segurança da aplicação.

Para detalhar melhor como é feita cada parte do passo final do método USASEC, confecção da casa da qualidade, será detalhado cada quarto de acordo com a Figura 2.8 da seção 2.3.1, que aborda cada ação de acordo com seu quarto respectivo.

Para compreender como é feita a casa da qualidade precisa-se observar cada "quarto" e suas características, conforme Figura 2.8. No lado esquerdo, para o modelo USASEC, tem-se os requisitos de usabilidades trazendo as importâncias relativas globais calculadas no passo anterior, através do Processo de Análise Hierárquica (AHP), para dentro da casa da qualidade.

Estes requisitos são a "Voz do Usuário". Todos os espaços relacionados a usabilidade estão na cor laranja e os requisitos de usabilidade estão com prefixo US e seu número correspondente a frente para identificá-los. Concomitantemente, todos os espaços relacionados à segurança estão na cor verde e os requisitos de segurança estão com prefixo SS e seu número correspondente na frente.

No quarto 2, definido na Figura 2.8 como características técnicas do produto, devem ser analisadas no método USASEC como características de segurança da informação e são pontuadas pela equipe multidisciplinar (EM) que está realizando o método.

O peso relativo destas características vem do somatório do quarto 6 (telhado), onde temos a relação dos requisitos de segurança da informação com uma análise interna dos impactos das 10 maiores vulnerabilidades para aplicações web que podem gerar problemas de segurança para a aplicação, previstas na seção 2.2 3 e preenchidas no quarto 5, conforme Figura 2.8.

O valor atribuído a cada requisito de segurança pode chegar até o valor dez de acordo com o relacionamento direto entre a vulnerabilidade e o princípio de segurança em foco, de acordo com a natureza da aplicação, como já definido para o método. Por exemplo, aplicações que necessitam de transmissão de dados sensíveis como bancos e *e-comerce* precisam ser julgadas e pontuadas com mais o "+" para princípios de segurança relacionados com estas vulnerabilidades de acordo com a tabela 2.1 da seção 2.2.3.

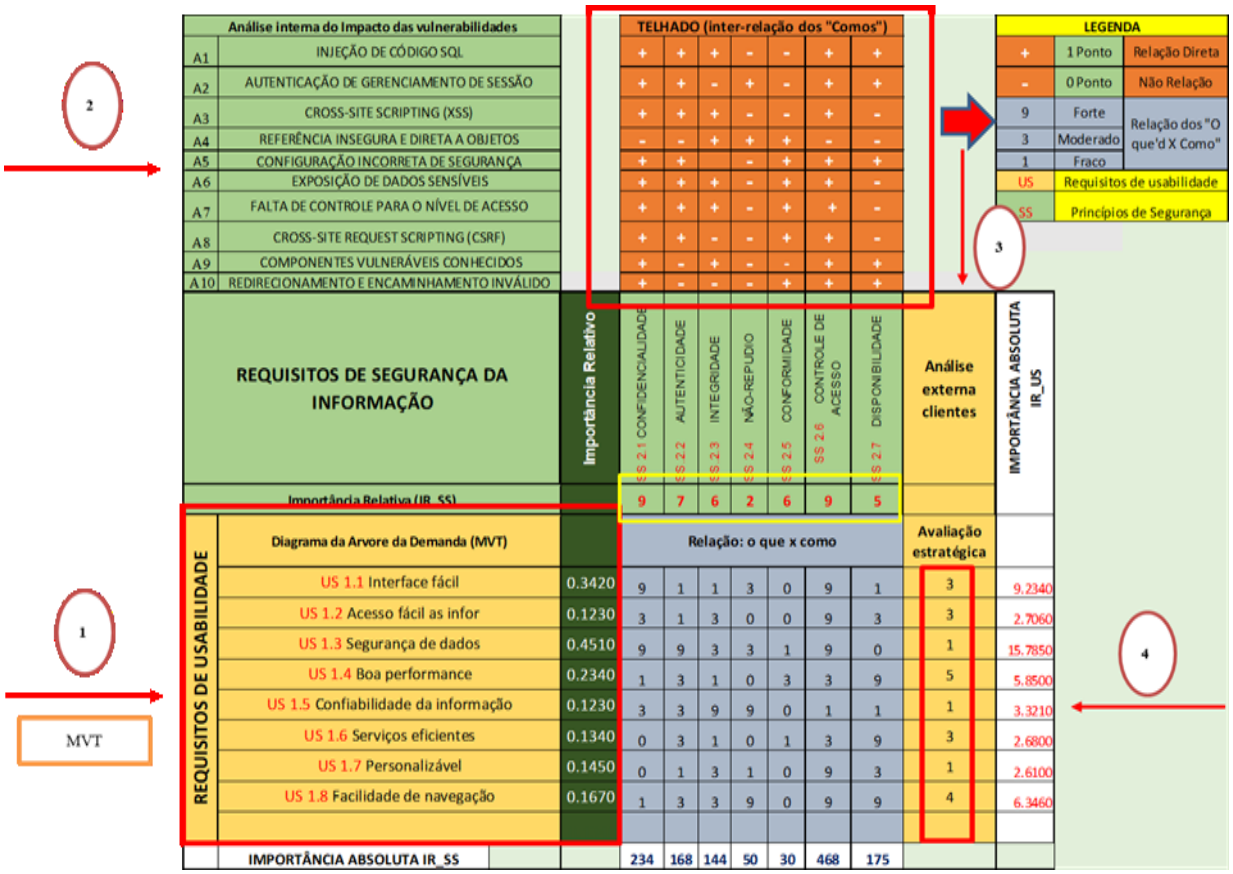


Figura 3.5 – Exemplo da casa da qualidade para o método USASEC no passo 1 a 4.

De acordo com a necessidade da estratégia de negócio outras vulnerabilidades podem ser consideradas, como por exemplo, os ataques de negação de serviço para aplicações que necessitam ter alta disponibilidade em períodos curtos.

A avaliação estratégica, no quarto 4 denominado de confronto com a concorrência, diz respeito a como a equipe multidisciplinar avalia a importância de cada um dos requisitos de usabilidade priorizados de acordo com a estratégia global da organização. Caso a equipe multidisciplinar possua características de outros sistemas que realizam tarefas semelhantes ao avaliado, pode ser realizada uma comparação entre os sistemas, chamada de *benchmarking*, para uma análise competitiva entre os softwares.

Ainda, no quarto três, chamado de matriz de relações, temos a pontuação do relacionamento entre os requisitos de usabilidade, feitos durante todos os passos anteriores, e os requisitos de segurança da informação. Esta matriz é caracterizada pelo relacionamento dos "o que x como", nela a equipe multidisciplinar, que possui todos os segmentos de usuários representados, pode relacionar uma necessidade do usuário fracamente atribuindo o valor um (1), moderadamente atribuindo o valor três (3) ou fortemente atribuindo o valor nove (9) a um requisito técnico de segurança ou zero (0), caso o requisito de usabilidade não se aplique ao de segurança.

Caso não haja relacionamento entre os requisitos pode-se se deixar em branco, ou nulo, o relacionamento entre aqueles requisitos de usabilidade e segurança.

Após preenchido todas as pontuações, segue-se a função para a multiplicação dos requisitos de usabilidade e segurança, conforme equação 2.1 da seção 2.3.1.

$$IA = \sum_{j=1}^{M} IR\_US * IR(IRai, IRaj)$$

Onde temos que IA é a importância absoluta tanto para os requisitos de usabilidade (US) como para os requisitos de segurança (SS). Sendo a importância absoluta o produto de cada importância relativa dos requisitos de usabilidade (IR_US), colocados no lado direito da casa da qualidade, e de segurança (IR_SS), colocados no quarto 5 de avaliação técnica, com os seus relacionamentos no quarto 3 da matriz de relações (IR).

Ainda, para conseguir chegar na importância absoluta dos requisitos de usabilidade devem ser considerados a pontuação da análise externa dos clientes quanto a importância estratégica deste para a organização. No exemplo da Figura 3.5, o requisito US 1.3, que aborda o requisito de usabilidade segurança de dados, fica assim calculado:

$$IA = \sum_{j=1}^{M} IR\_US * IR(IRai, IRaj)$$ 0,4510*9 + 0,4510*9 + 0,4510*3 + 0,4510*3 + 0,4510*1 + 0,4510*9 + 0,4510*0 + 0,4510*1 = 15,7850.

Como exemplificado, são calculadas todas as importâncias absolutas, tanto para os requisitos de usabilidade quanto para os de segurança.

3.4 Avaliação dos resultados do método USASEC

Para analisar a casa da qualidade para o método USASEC deve-se, depois de calculadas todas as importâncias absolutas dos requisitos de usabilidade e segurança, observar quais têm o maior valor. Feito isto, pode-se relacionar o maior requisito de usabilidade, observando-se na horizontal, no sentido da esquerda para direita, até se encontrar o maior requisito de segurança, observando-se na posição vertical, no sentido de baixo para cima, conforme mostrado na Figura 3.6.

Figura 3.6 - Exemplo da casa da qualidade para o método USASEC nos passos 5 a 7

Estes dois requisitos destacados são aqueles que devem ser tratados como os que mais impactam o projeto de forma a satisfazer o usuário e garantir a segurança da aplicação. Assim, a equipe do projeto sabe que colocando mais recurso nestes dois requisitos é possível ter maior sucesso na aplicação pois ela satisfaz o usuário de forma segura.

Ainda, pode-se observar, durante o ciclo de vida no desenvolvimento de software, o quanto de recursos estão sendo gastos para cada um dos requisitos. Podendo-se variar, de

acordo com a disponibilidade da equipe de projeto do software e da importância para cada um dos requisitos; ou seja, aumentado ou diminuindo a disponibilidade de recurso para cada requisito pontuado de acordo com a necessidade da equipe do projeto do software. Assim, pode-se melhorar o acompanhamento do projeto de melhoria da aplicação ou durante a criação de um novo software.

Contudo, isso não significa que os outros requisitos não sejam importantes e também não devam ser implementados e alinhados durante todo o ciclo de vida no desenvolvimento do software. Desta forma, é possível elencar em ordem de importância quais devem ser trabalhados primeiros para a entrega rápida de um produto que já tem características que agradam ao usuário.

Algumas contribuições deste método, além do descrito na casa da qualidade, são: assegurar que as ideias que satisfazem o usuário foram ouvidas e serão implementadas, evitando retrabalho da equipe de desenvolvimento, confecção de um diagrama de afinidade para organizar o grande número de ideias por similaridade e transformá-las em requisitos, a montagem de uma árvore hierárquica para utilização do método AHP para a priorização dos subcritérios (requisitos), a quantificação destes requisitos seguindo o processo AHP para construir uma hierarquia de prioridades entre os requisitos, discutir como a implementação destes requisitos no sistema pode afetar a segurança da aplicação observando suas vulnerabilidades e, por fim, após observar quais requisitos de usabilidade e segurança mais se destacaram no método, pode-se identificar quais requisitos mais impactam conjuntamente está aplicação.

4 Utilização do Método USASEC

Para empregar o método proposto, USASEC, foi utilizada uma aplicação *web* responsável pelo gerenciamento de investigação e prevenção de acidentes aeronáuticos do Exército. Assim, a seguir será abordado as características desta aplicação e os objetivos estratégicos que alinham a utilização do método proposto e a confecção da aplicação *Web*.

Esta aplicação *web* foi escolhida pois é responsável por um sistema crítico; uma vez que propicia o gerenciamento dos relatórios de prevenção de acidentes, bem como propicia a coordenação das Recomendações de Segurança de Voo (RSV) necessárias para se evitar ocorrências de acidentes aéreos que podem ceifar vidas.

Além disso, para o Centro de Aviação do Exército (CAVEx), o risco da atividade de voo é inerente às operações aéreas. Desta feita, os responsáveis deverão envidar esforços para que sejam minimizados. Neste contexto, deve-se ressaltar que a segurança do voo é uma responsabilidade de todos.

Sendo assim, este sistema dá suporte a uma atividade crítica, a segurança de voo, e almeja que esta seja realizada de forma segura e eficiente. Através das ações corretivas que o sistema informa, é possível tomar medidas preventivas que preservem os equipamentos, as aeronaves e principalmente, os recursos humanos.

Um pressuposto básico que orienta todos os integrantes da Aviação do Exército, e por consequência da aplicação que dá suporte ao sistema, é que todos os acidentes devem e podem ser evitados e que nenhuma missão imposta justifica um acidente. Os prejuízos causados são significativos no que concerne ao material e incomensuráveis quando à perda de vidas. As normas e procedimentos estabelecidos pelas autoridades competentes, e divulgadas através dos Relatórios de Prevenção de Acidentes (Rel Prev) da aplicação, são de grande importância pois foram criados para preservar os equipamentos e, principalmente, o que há de mais valioso na Aviação do Exército, os seus aeronavegantes.

Conforme [112], de 2016, normatiza-se a utilização da aplicação com máxima prioridade em todos os níveis, desde o soldado até o comandante da Aviação do Exército. Assim, existe um estimulo formal e irrestrito com vista a utilização e tramitação de informações de segurança de voo pela aplicação, devendo, também, estreitar a ligação entre os órgãos responsáveis pela segurança do voo em todo o território nacional.

O Sistema de Gerenciamento de Investigação e Prevenção de Acidentes Aeronáuticos (SIGIPAAerEx), feita através da aplicação *web*, tem por objetivo estruturar sua Seção de

Investigação e Prevenção de Acidentes Aeronáuticos (SIPAA) em duas subseções: uma voltada para a atividade de prevenção e outra para a investigação de acidentes aeronáuticos. Cada subseção destas deve ter, pelo menos, um indivíduo com cursos na área de segurança de voo, um substituto a este, um psicólogo e um auxiliar para tarefas administrativas. Além disso, é prevista uma fase de transição para novos chefes das subseções e, obrigatoriamente, pelo menos um indivíduo deve ter cursos na área de segurança de voo.

Os órgãos que utilizam o SIGIPAAerEX são os seguintes: Comando de Operações Terrestres (COTER), sediado em Brasília-DF; Comando Militar da Amazônia (CMA), com sede em Manaus-AM; Comando Militar do Oeste (CMO), com sede em Campo Grande-MT; a Diretoria de Material de Aviação do Exército (DMAVEx), com sede em Brasília-DF; o 1° e 2° Batalhões de Aviação do Exército (BAVEx), em Taubaté-SP; 3° BAVEx em Campo Grande-MT e o 4° BAVEx em Manaus – AM; bem como, o Centro de Instrução de Aviação do Exército (CIAVEx), Batalhão de Manutenção e Suprimento de Aviação do Exército (B MNT SUP AVEX) e Base Administrativa de Aviação do Exército (BAVT), todas situados em Taubaté-SP, conforme Figura 4.1.

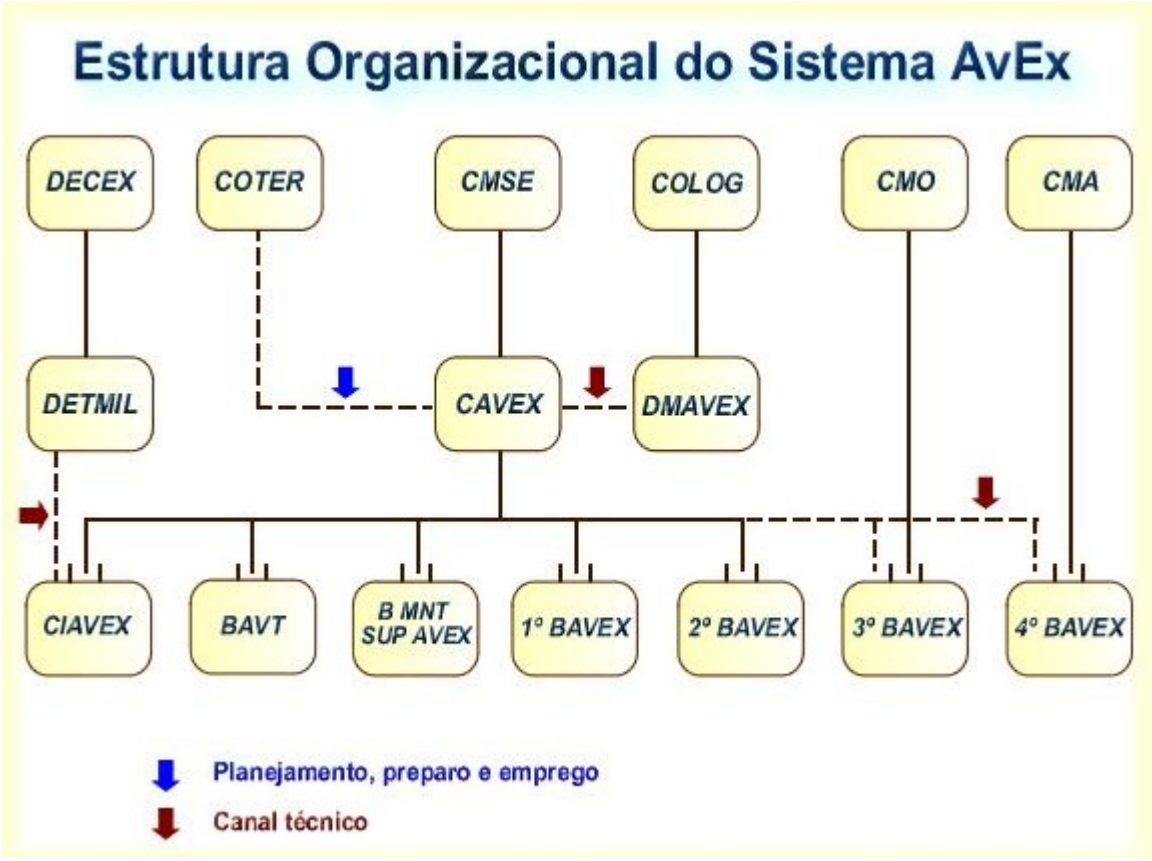


Figura 4.1 – Organograma dos órgãos da Aviação do Exército [112].

A grande contribuição da aplicação *web* que gerencia o sistema está na integração de todos estes órgãos e na troca de informações entre eles, pois está é de fundamental para importância para o acompanhamento da execução das Recomendações de Segurança de Voo (RSV) emanadas da análise de Relatórios de Prevenção (Rel Prev), bem como Relatórios Finais (RF) de acidentes, incidentes e ocorrências de solo.

Outras contribuições consistem na montagem de um grande banco de dados, com informações que podem vir a esclarecer acidentes aeronáuticos, e possibilidade de gerar dados estatísticos. Ambas podem gerar ações que devem promover a prevenção de ocorrências aeronáuticas.

Logo, aplicação do método USASEC no SIGIPAAerEX atenderá as necessidades da organização e, com maior ênfase, as características técnicas do método pois contribuirá para avaliar as principais necessidades dos usuários, aeronavegantes, e observará as carcetristicas técnicas de segurança, proteção cobernética, para esta aplicação. Dando a possibilidade, futura, de realizar estudo estatísticos e inferentes quanto a predição de possíveis incidentes tanto segurança da informação quanto de segurança de voo.

Para o estudo de caso descrito neste capitulo foram realizados no Comando de Aviação do Exército, no 1°, 2° e 3° Batalhões de Aviação do Exército, na Base de Manutenção e Suprimento de Aviação do Exército e na torre de controle de aeronaves do Exército; todos localizados na cidade de Taubaté-SP.

4.1 Ambiente do estudo de caso

Assim, pelo método USASEC, este software está ligado a um objetivo estratégico do Exército pois mantem a aviação com modernos meios tecnológicos e softwares de qualidade e, além disto, proporciona um trâmite correto e controle das informações e recomendações de segurança de voo de suas aeronaves e de seus aeronavegantes. Desta forma, com a identificação e alinhamento da aplicação com os objetivos estratégicos da aviação do Exército, o SIGIPAAerEx, cumpre a passo 1 do método, ou seja, a aplicação está voltada para o sucesso estratégico da organização.

No passo 1 foi realizada uma identificação de todas as aplicações que fazem parte do Sistema de Aviação do Exército (SisAvEx). Entre eles foi escolhido o sistema Gerencial de

Investigação e Prevenção de Acidentes Aeronaúticos do Exército (SIGIPAAerEx). A aplicação tem uma função chave na predição de possíveis ocorrências de pane em aeronaves.

O SIGIPAAerEx tem amplitude nacional e deve ser utilizado não apenas pelos aeronavegantes, aqueles que voam de alguma forma nas aeronaves, mas por qualquer pessoa que observar um incidente com uma aeronave que possa gerar um relatório de prevenção de acidente (Rel Prev). Estes incidentes podem ser qualquer observação que o indivíduo acredita atentar quanto a segurança de voo; ou seja, vai desde aeronaves que voam muito próximos de casas, prédios, aves, drones e outros objetos que podem gerar incidentes até problemas técnicos observados pelos tripulantes em solo.

A tripulação também pode ser responsável por gerar um Rel Prev quando identificado algum problema em uma região na rota do voo, ou quando ocorre alguma pane na aeronave e, inclusive, para resolver conflito onde o próprio piloto pode cometer uma imprudência ou imperícia durante o voo e os tripulantes podem gerar um Rel Prev relatando esta situação.

Desta forma, fica claro que há conflito entre as partes do Rel Prev, mas o sistema já foi criado com a possibilidade deste documento ser feito de forma anônima ou não, ou seja, para não identificar os responsáveis pela geração do Rel Prev e para focar apenas na análise e recomendações a serem tomadas com o incidente relatado (RSV).

Com base nos relatórios (Rel Prev), é possível serem feitas análises pelas autoridades competentes e determinação são emanadas no próprio sistema para que todos os batalhões tomem conhecimento e cumpram as recomendações, a fim de não ocorrerem mais incidentes de segurança quanto aquela situação.

Um exemplo de providências tomadas são medidas de alerta e segurança que devem ser passadas na reunião (*briefing*), pelas SIPAA, sobre quais locais possuem incidentes com choque de aves a aeronaves, aproximação de drones, locais de pousos modificados recentemente, trocas de cabos e peças com determinada quantidade de horas de voo e demais incidentes que podem gerar um risco a aeronave e demais pessoas envolvidas na atividade.

4.2 Contexto da Aplicação do Método

A aplicação SiGIPAAerEx foi desenvolvida há um ano e ainda se encontra na fase de pós-liberação para seus usuários. Ela possui uma tela que pode ser acessada por qualquer militar, dentro da rede coorporativa do Exército. Este militar pode gerar um Relatório de

Prevenção (Rel Prev), a qualquer momento, preenchendo um relatório de prevenção, conforme mostrado na Figura 4.2.

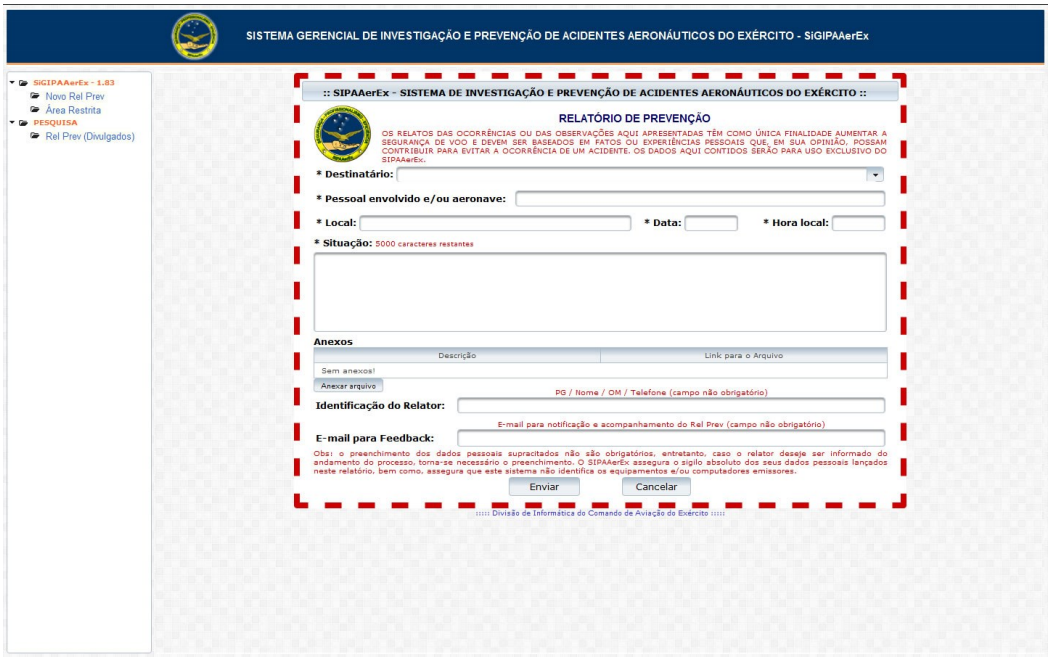


Figura 4.2 – Tela inicial do SIGIPAAerEx para confecção do Relatório de Prevenção (Rel Prev).

Esta aplicação foi criada pela divisão de informática do próprio CAVEx e tem por objetivo, não apenas gerar os Rel Prev e analisá-los, como também gerar consultas e estatísticas através destes relatórios. Através da aplicação é possível relacionar os incidentes ocorridos antes de acidentes aéreos e, se houve causa e efeito, entre eles.

Durante a realização do Rel Prev o usuário pode ou não se identificar, como dito anteriormente, caso ele decida se identificar ele pode colocar um correio eletrônico funcional para acompanhar o processo de análise e despacho do seu Rel Prev. Esta medida visa dar um retorno (*feedback)* para os usuários e mantê-lo atualizado de quais autoridades estão tomando ciência e respondendo ao incidente.

Após a análise da última autoridade, é disponibilizado um relatório final com todas as providências e recomendações cabíveis (RSV) e distribuído para cada Seção de Investigação e Prevenção de Acidentes Aéreos (SIPAA) de cada unidade aérea. Esta seção é responsável por divulgar, executar e fiscalizar se todas as medidas e ordens emanadas pela autoridade competente, através da aplicação, estão sendo executadas.

O sistema possui um relatório de visualizações onde é possível a SIPAA do CAVEx observar se todos os militares envolvidos na divulgação e execução da RSV estão cientes das ordens e das recomendações transmitidas. Isso é necessário pois algumas destas recomendações

devem ser executadas de imediato, tendo em vista que podem gerar incidentes de segurança para aeronaves e aeronavegantes.

Para a realização do método USASEC foi necessário reunir vários segmentos de usuários da aplicação, entre eles responsáveis pela segurança de voo dos SIPAA's de diversos batalhões, diversos usuários comuns que realizam Rel Prev com frequência, o chefe da seção de segurança do SIPAA do CAVEx, administradores do sistema e a equipe de desenvolvimento da aplicação e o analista de segurança de todo sistema de aviação do exército, conforme tabela 4.1.

A formação da equipe multidisciplinar (EM) para a aplicação do método USASEC envolveu profissionais voluntários de nível superior de formação e com grande capacidade técnica dentro de suas áreas de atuação, com cerca de 5 cinco horas semanais durante 5 semanas para a realização do método. Estes profissionais tem a capacidade de realizar mudanças e tomar decisões de como a aplicação pode ser aperfeiçoada de acordo com as necessidades dos usuários.

Devido à grande dificuldade em reunir a equipe multidisciplinar, a avaliação do método USASEC não pode ser feita de forma continua. Ou seja, acredita-se que caso os voluntários estivessem disponíveis integralmente para a avaliação era possível realizá-la em uma semana. Demonstrando a rapidez e simplicidade que o método pode ser realizado. A formação da equipe disciplinar foi feita de acordo com a tabela 4.1.

Tabela 4.1 – Formação da equipe multidisciplinar para o estudo de caso.

Capacitação do Voluntário	Função no Sistema	Número de Pessoas
Chefe de todas as seções de Segurança de Voo do Exército. Formação em segurança em Voo na Espanha e no Brasil.	Proprietário	1
Especialista em Segurança em voo, os dois voluntários são responsáveis pela maior quantidade de Rel Prev e Auditoria de segurança em voo do Exército.	Administrador do Sistema	2

Responsável pela confecção do sistema avaliado.	Desenvolvedor do Sistema	1
O voluntário possui especialidade como Analista de segurança de TI com formação acadêmica, já trabalhou diversos projetos de segurança para o governo federal, inclusive na presidência da república.	Analista de segurança	1

Em todos os passos do método, foram realizadas palestras rápidas, de cerca de uma hora, para capacitação em cada um dos passos envolvidos. Assim, o autor deste trabalho de pesquisa teve apenas que aplicar as avaliações, se limitando apenas em instruir os membros da equipe multidisciplinar (EM) na correta aplicação dos questionários, formulário de julgamentos e preenchimento na matriz da casa da qualidade. Os conceitos envolvidos em cada atividade devem ser transmitidos para EM com certa frequência para que o foco da usabilidade e segurança sejam mantidos.

Para a montagem do diagrama de afinidade e realização dos cálculos do processo de análise hierárquica, AHP, foi necessário realizar reuniões com todos os membros EM mais de uma vez. Isto deve ser feito para que todos os membros da equipe entendam, de forma sistêmica, como o método deve ser realizado e quais conceitos estão sendo aplicado em cada passo do método.

As responsabilidades de cada membro da equipe focal do método USASEC está ligada à sua especialidade. Logo, todos os voluntários têm igual peso na avaliação, independente do cargo que ocupa, de sua função no sistema e de como acredita que pode contribuir com o método.

4.2.1 Cenário do estudo de caso – SIGIPAAerEX

Uma das atividades do Sistema Gerencial de Investigação e Prevenção de Acidentes Aeronáuticos do Exército refere-se ao acompanhamento e providências tomadas sobre os Relatórios de Prevenção de Acidentes (Rel Prev) preenchidos por usuários comuns no sistema.

Um militar, ao identificar um incidente que atenta quanto a segurança do voo, pode preencher a ficha do relatório de prevenção, conforme Figura 4.1. Nesta ficha será preenchido o local, data e hora do incidente, bem como, suas características como: quem estava envolvido, tipo de aeronave, como ocorreu o incidente e todos os dados que o usuário achar necessário para análise do incidente de segurança. Um passo importante no preenchimento do relatório é colocar o máximo de características do incidente para auxiliar na elucidação do problema. Desta forma, cresce de importância que o relatório seja feito o mais rápido possível, para que nenhum detalhe do incidente seja esquecido.

Após o preenchimento da ficha inicial do relatório, o autor pode colocar seu e-mail funcional para acompanhar os resultados do despacho, de todas as autoridades competentes, sobre o seu Rel Prev. No final, todos os usuários do sistema vão receber recomendações de como devem proceder na situação relatada no Rel Prev, ou se é necessário trocar alguma peça da aeronave em que aconteceu o incidente ou, ainda, se algum procedimento de segurança deve ser imediatamente tomado para evitar, que o problema relatado, torne-se um acidente aeronáutico.

Atualmente, com já foi dito, uma importante ferramenta que tem sido utilizada pelo sistema é a capacidade de preencher a ficha do relatório de forma anônima. Isto ocorre por causa do conflito que pode ocorrer entre níveis diferentes hierárquicos, contudo, ao não se identificar na ficha do Rel Prev, o usuário passa a não receber os *feedbacks* do seu relatório em seu e-mail funcional o que pode gerar uma insatisfação ao usuário por não ver um resultado direto de sua iniciativa.

Assim, muitos usuários têm desistido de preencher os relatórios de prevenção por causa da não observação de resultados diretos feitos pelos seus relatos no Rel Prev. Ainda, por falta de uma melhor divulgação de como utilizar o sistema, muitos usuários não tem o hábito de utilizar a aplicação o que prejudica os benefícios que ela pode trazer para toda a aviação. Contudo, uma das maiores dificuldades relatadas pelo usuário está ligada ao acesso a aplicação pois a organização determina que apenas quem está ligado à rede corporativa pode acessar o sistema. Esta característica se torna uma dificuldade pois, em missões de apoio externo a organização, os Rel Prev's, geralmente, ou não são feitos ou se perdem em detalhes.

A não confecção e disponibilidade do relato de um incidente, durante uma missão, pode colocar em risco todo o sucesso da operação por causa de falhas que podem ocorrer na aeronave. A transmissão destes incidentes pode melhorar a execução da atividade, além de resguardar a vida dos integrantes que estão participando da missão.

5 Análise e Discussão dos Resultados

Neste Capítulo 5, relata-se o estudo de caso desenvolvido durante a pesquisa, envolvendo o sistema de investigação e prevenção de acidentes aeronáuticos do Exército, feito em conjunto com a equipe de tecnologia da informação e a Seção de Segurança e Prevenção de acidentes Aeronáuticos (SIPAA), do Comando de Aviação do Exército, sediada na cidade de Taubaté-SP.

5.1 Resultados obtidos na aplicação do passo 1 do método proposto USASEC

Depois de identificada a aplicação que será analisada pelo método USASEC, devemos seguir os passos previsto para o método conforme seção 3.3. Inicialmente, passo 1, foi identificado que a aplicação, SIGIPAAerEX, está alinhada com a estratégia da organização e que ela influência no sucesso da principal atividade da organização, segurança de voo, conforme descrito na seção 4.

5.2 Resultados obtidos na aplicação do passo 2 do método proposto USASEC

Para a passo 2, foram segmentados os tipos de usuários da aplicação de acordo com suas necessidades. Assim, foram identificados usuários comuns, usuários administradores, os usuários desenvolvedores, pois os desenvolvedores da aplicação trabalham no mesmo ambiente onde a aplicação é utilizada, ou seja, eles também podem confeccionar Rel Prev; e por fim, usuário analista de segurança.

Cada um deste segmento foi identificado e, devido a ter usuários em diversos pontos do território nacional, foi separada uma amostra com dezesseis usuários comuns de batalhões de aviação, quatro administradores das seções de investigações e prevenção de acidentes (SIPAA), dois voluntários da seção central da SIPAA, dois desenvolvedores e o chefe da equipe de segurança de software da organização, totalizando 25 usuários. Cabe ressaltar, todos os usuários da amostra são de organizações sediadas na cidade de Taubaté-SP.

5.3 Resultados obtidos na aplicação do passo 3 do método proposto USASEC

No passo 3, não foi necessário confeccionar um modelo da aplicação já que o SiGIPAAerEx está pronto e sendo executado no local de destino. Contudo, como a aplicação ainda está em fase de teste e melhoria junto ao usuário, foi considerado que a aplicação está na fase cinco, conforme a Figura 3.1. Nesta fase, deve-se acompanhar métricas de uso e *feedbacks* dos usuários para reunir as melhorias que devem ser consideradas para a aplicação, conforme seção 3.1.

5.4 Resultados obtidos na aplicação do passo 4 do método proposto USASEC

Para ser realizada a passo 4, foi necessário ir até o local onde a aplicação está sendo utilizada. Assim, no total foram ouvidos individualmente 25 usuários, de diferentes segmentos, utilizando os conceitos de avaliação de usabilidade em percursos pluralísticos, conforme seção 2.1.1.4. Nesta pesquisa, a aplicação já estava na fase de implantação, sendo facilitado o contato do grupo pluralístico ao sistema para avaliação.

Assim, foram obtidas as ideias de melhorias utilizando em questionário de satisfação para os usuários, o questionário aberto, conforme apêndice A. O questionário aberto de satisfação é utilizado na forma de coleta de dados, composto, em geral, por questões abertas, subjetivas, sendo aplicado a usuários de modo que a EM possa conhecer as experiências, opiniões e preferências dos usuários.

Conforme a seção 2.3.2, o questionário aberto, conforme apêndice A, visa identificar as melhorias de usabilidade para a aplicação. Na sua elaboração, teve-se o cuidado de incluir perguntas formuladas de maneira simples, sem ambiguidade e na linguagem dos entrevistados. Os principais resultados obtidos estão na tabela 5.1, e muitos aspectos excederam apenas questões de usabilidade. Sendo necessário retirar as questões que não estavam ligadas as ideias e definição de usabilidade para o método USASEC.

Após a execução do questionário aberto para obter os “verbatims” da UoV, ideias palavra por palavra de usabilidade da aplicação alvo feita na passo 4 do método; o passo seguinte é a passo 5 onde foi confeccionado o *User Voice Table* (UVT), conforme Figura 5.1.

5.5 Resultados obtidos na aplicação do passo 5 do método proposto USASEC

O acesso à Internet (AI) foi a principal melhoria identificada por diversos usuários que se mostram insatisfeitos com a utilização da aplicação apenas pela rede interna da organização. Algumas ideias associadas a esta dificuldade foram colocadas na tabela 5.1 como a não possibilidade de enviar Rel Prev em tempo real em caso de voos onde a organização não participa da rede interna, a consulta de Rel Prev's de rotas alternativas caso o piloto necessita realizar uma conduta não prevista, a integração com outros sistemas de outras organizações e a redução no tempo de processamento de despachos das autoridades competentes para a solução de incidentes.

Tabela 5.1 – Principais ideias relacionadas a melhoria da usabilidade classificadas pela EM para a aplicação (UVT)

PRINCIPAIS IDEIAS DE USABILIDADE	IDEIAS RELACIONADAS
- Acesso à Internet externa a rede coorporativa (AI);	- Reduzir o tempo de processamento das informações lançadas no sistema e as providências para evitar incidentes de segurança; - O acesso pela internet facilitaria os reporte de incidentes em tempo real; - Tratar campos que podem receber *scripts* maliciosos; - Integração a outros sistemas como a da Força Aérea; - Muito dependente da rede interna; - Limitação quanto a disponibilidade de acesso; - Preenchimento de Rel Prev's por qualquer indivíduo;
- Facilidade de Uso (FU);	- Aviso de alerta nas telas dos usuários sobre recomendações pendentes de relatórios; -Padronização dos termos técnicos na aplicação; - Telas de auxílio ao *briefing;* - Sequência de tarefas de fácil visualização no sistema; - Simples utilização; - Interface sem informações excessivas (poluída); - Preenchimento fácil e rápido dos Rel Prev's; e - Melhoria na utilização das barras de rolagem.

- Acesso por Dispositivos Móveis (DISMOV).	- Sistema Intuitivo; - Uso por *smartphones*; - Limitação quanto a disponibilidade de acesso;
- Acesso por aplicativos de Celular (COAPL).	- Criação de aplicativos; - Uso por *smartphones*; - Em missões fora do alcance da rede interna fica impossível a transmissão de Rel Prev's; - Inserção de dados por dispositivos móveis com VPN; - Limitação quanto a disponibilidade de acesso;
- Melhorar a divulgação das ferramentas e possibilidade da aplicação (DIV).	- Determinações de palestras e cartazes; - Realização de instruções; - Colocar as ordens do sistema em documentos diários; - Através dos órgãos responsáveis pelo aplicativo (SIPAA) em reuniões de segurança de voo; - Divulgação feita por *links* na intranet; - Utilização de *Pop-up* no sistema para divulgação;
- Consulta e análise de dados estatísticos (CAD).	- Consulta para análise de um banco de dados de incidentes; - Durante as reuniões de voos, passar os possíveis incidentes que podem ocorrem durante a rota prevista; - Buscas por informações especificas de incidentes e aeronaves que trabalhava; - Exportar dados estatísticos com arquivos e extensões compatíveis com outros sistemas; - Cruzamento de dados entre os incidentes;
- Inclusão de Manual do usuário (IMN).	- Não conseguir utilizar todas as funções que a aplicação permite por desconhecimento; - Falta de conhecimento que a aplicação de *feedbacks* por e-mail funcional e tornar o sistema mais autoexplicativo;
- Telas para Administradores e usuários comuns (TAU).	- Dificuldade de controle das normas que foram cumpridas pelos usuários; - Direcionar ações para setores específicos competentes;

	- Passagem de função entre administradores e usuários comuns facilitada;

Já as ideias relacionadas a Facilidade de Uso (FU) estão separadas por melhorias que visam facilitar o uso diário da interface gráfica da aplicação. Logo, ideias como fácil preenchimento de relatórios, barra de rolagens menores e telas com resumo das recomendações para *briefing* rápidos foram consideradas.

O Acesso ao sistema por dispositivos móveis (DISMOV) não está relacionada a confecção de aplicativos para o software, mas a possibilidade de acessar a aplicação por dispositivos móveis como *notebooks*, tablets e smartphones através de uma rede privada e criptografada (*Virtual Private Network* - VPN). Esta melhoria garantiria que, ao menos, um dispositivo estaria disponível para acesso durante as missões que não tiverem apoio da rede interna da organização. Com isso, será possível aos usuários, mesmo com apenas um dispositivo com acesso, realizar seus planejamentos, preencher relatórios e consulta dados em tempo real.

Para o acesso através de aplicativos de celular (COAPL), foi considerada pela EM a confecção de um aplicativo para sistemas operacionais *android* e *ios* para facilitar a consulta e preenchimento dos relatórios. Está necessidade foi identificada em casos de incidentes onde não há infraestrutura de rede para passar as informações. Logo, o usuário teria que acessar o aplicativo pela sua rede disponível no celular.

Uma ideia de melhoria observada por oitenta porcento da amostra, para aumentar a usabilidade da aplicação, foi uma melhor divulgação do aplicativo (DIV). Várias ações relacionadas a está ideia foram sugeridas e elas poderão aumentar a quantidade de usuários que aprovam e utilizam, com maior frequência, o sistema. Entre estas ações foram incluídas: palestras e seminários sobre as ferramentas do sistema, leitura diárias sobre as recomendações (RSV) que foram tomadas depois de que os Rel Prev's foram enviados e, ainda, uma divulgação de links com explicações sobre como utilizar o sistema. Assim, os usuários poderão tomar consciência da importância da informação que a aplicação pode lhe oferecer e começar a participar, ativamente, da inclusão de dados para montagem do banco de dados do sistema.

Todos os segmentos, representados na amostra questionada, reportaram uma possibilidade de acesso aos dados do banco de dados para melhorar o desempenho da aplicação (CAD) quanto ao alerta de possíveis incidentes que podem ocorrer durante uma determinada rota de voo. Cabe ressaltar, ainda, que parte da investigação de acidentes aeronáuticos utiliza os Rel Prev's para solucionar acidentes que aconteceram e que poderiam ter sido evitados caso as recomendações de segurança tivessem sido obedecidas. Neste sentido, o banco de dados

estatístico, e a consulta frequente a este, pode alertar quanto a recomendações e providências a serem tomadas em determinadas situações e incidentes; os quais podem reduzir o número de incidentes de segurança causando, consequentemente, uma melhor performance operacional do sistema.

Uma das ideias relacionadas a melhoria do uso do aplicativo está ligada à inclusão de um manual dentro do sistema (IMN). Como a aplicação é utilizada de forma rápida e, muitas das vezes, esporádica pelo usuário comum; é necessário um suporte ao usuário que possa evitar que o usuário possa realizar procedimentos não previsto pelo sistema, causando erros que podem comprometer a segurança da aplicação ou o seu bom desempenho.

Por fim, uma ferramenta que o sistema deve implementar para a melhoria da sua usabilidade é telas diferenciadas para o controle de acesso ao usuário por níveis de privilégio (TAU). Atualmente, tanto o usuário comum como o administrador têm utilizado um *login* e senha para entrar no mesmo ambiente de trabalho. Isso causa distração e incomoda o usuário comum que apenas acessa o sistema para extrair informações rápidas e de seu interesse.

Desta forma, conforme entendimento da EM que está aplicando o método, estas ideias que foram classificadas na UVT, por similaridade, englobam as necessidades dos usuários quanto a melhoria da aplicação; para análise da usabilidade como fator que assegura que ela se torne mais fáceis de usar, eficiente e agradável.

5.6 Resultados obtidos na aplicação do passo 6 do método proposto USASEC

Para organizar as ideias, através do método USASEC, utilizando o diagrama de afinidade, cada ideia é colocada em um papel e a EM deve organizá-las de acordo com suas afinidades em relação ao conceito de cada meta de usabilidade, montando o diagrama de afinidade, conforme seção 2.4. Estes decisores são os usuários capazes de realizar a tomada decisão de mudanças nos requisitos do sistema para incluir melhorias e identificar problemas.

Desta forma, para o método USASEC, a realização do diagrama de afinidade deve ter como objetivo principal, a ênfase no conceito de usabilidade e suas metas, conforme conceito de usabilidade da seção 2.1 de [30] e organizar cada ideia dentro de uma meta de usabilidade que deve ser alcançada, usando as definições da referência.

Para isso, foi necessária uma palestra de uma hora para os membros da equipe multidisciplinar com o objetivo de explicar como é feito o diagrama de afinidade, bem como, para explicar cada um dos conceitos de usabilidade e suas metas utilizados pelo método.

Por causa do grupo multidisciplinar ter várias perspectivas quanto a utilização da aplicação, muitas ideias são classificadas em categorias de metas diferentes; logo, existe um conflito entre as perspectivas de cada segmento dos usuários representados. Cabe ao aplicador do método, orientar e relembrar as definições de cada uma das metas, mostrando a equipe multidisciplinar quais ideias podem se encaixar melhor para cada meta. Cabe ressaltar que, dependendo das ideias que foram colocadas pela amostra de usuários, está pode estar em mais de uma meta de usabilidade, conforme Figura 5.1.

Para realizar a organização das ideias de melhoria de usabilidade, foi feita a pergunta que define cada uma das metas e observados quais ideias podem ser consideradas metas para se alcançar esta ideia. Por exemplo, na meta de utilidade foi utilizada a pergunta que a define: "O sistema fornece um conjunto de funções que permite aos usuários realizar todas as suas tarefas de maneira que desejam? ". Assim, a equipe multidisciplinar pode organizar as ideias que representam a resposta para esta pergunta, de acordo com as ideias da UVT, como: O acesso à Internet (AI), a consulta para análise de Dados (CAD), a inclusão de telas para administradores e usuários comuns (TAU), o acesso ao sistema por dispositivos móveis (DISMOV), a facilidade de uso (FU) e a confecção de aplicativos (COAPL), conforme Figura 5.1. A ideia de melhoria de divulgação (DIV) não foi incluída por estar relacionada a ações que propiciem treinamento e incentivo ao uso da aplicação.

Já para as metas de eficácia e eficiência todas as ideias foram consideradas pois está relacionada ao nível de produtividade que a aplicação proporciona e sua atividade de realizar de forma eficiente, ou seja, se a aplicação é boa em fazer o que se espera dela.

Para a meta de segurança foi considerada a pergunta: "Se o sistema previne o usuário de cometer erros graves e, se mesmo assim cometer, permite que esses erros possam ser recuperados facilmente? ". Observa-se que, neste caso, esta definição de segurança está relacionada ao risco (*safety*) que o usuário pode gerar caso utilize de forma inapropriada o sistema. Assim, a equipe multidisciplinar organizou as ideias de acesso à Internet, inclusão do manual, consulta para análise de dados, facilidade de uso e divulgação das ferramentas da aplicação como as melhorias necessárias para atingir esta meta. Desta forma, o acesso por dispositivos móveis e a confecção de aplicativos não foram incluídas por se considerar que as ações relacionadas a estas ideias estão ligadas a disponibilidade de acesso a aplicação e não a questões técnicas de segurança. Contudo, foi explicado pelo aplicador do método que as questões técnicas de segurança serão avaliadas no passo 9 do método, a casa da qualidade.

Para a meta de capacidade de aprendizagem da aplicação, foram consideradas as ideias de acesso à Internet, consulta para análise de dados, telas diferenciadas para administradores e

usuários comuns, facilidade de uso e divulgação como as que possuem ações relacionadas a resposta da pergunta da definição da meta: “Quão fácil é e que tempo se leva para: “iniciar tarefas fundamentais do sistema e aprender de forma rápida um conjunto de ações necessárias para realizar um conjunto amplo de tarefas? ”.

Assim, para justificar a escolha das ideias foram observados que o acesso à Internet (AI) possibilita uma maior frequência de utilização da aplicação, influenciando na aprendizagem dentro e fora da organização; a consulta de dados poderá facilitar a aprendizagem no planejamento de rota e condutas em caso de incidentes; as telas diferenciadas para administradores do sistema e usuários comuns poderão dar maior notoriedade a informação procurada e as atividades que estão sendo executadas, aumentando o interesse do usuário e sua aprendizagem; a facilidade de uso melhora a performance de aprendizagem do usuário e a divulgação aumentará o conhecimento sobre as ferramentas e possibilidade do sistema.

Contudo, não foram aplicadas as ideias de inclusão do manual pois a definição da meta está relacionada ações que produzem a rapidez de aprendizagem durante o primeiro contato com a aplicação, desta forma, a inclusão de manual significa uma aprendizagem lenta durante a leitura do mesmo.

Por fim, a meta de capacidade de memorização está relacionada a seguinte pergunta: “que tipos de suporte de interface foram fornecidos com o objetivo de auxiliar os usuários a lembrar de como realizar as tarefas, especialmente aquelas que não são utilizadas com muita frequência? ”. Para o grupo multidisciplinar as ideias que estão relacionadas a está pergunta são: a inclusão do manual, para a retirada de dúvidas e suporte rápido ao usuário; as telas de acesso diferenciadas para administradores e usuários comuns pois facilitam a identificação dos campos que querem ser pesquisados; a facilidade de uso; a confecção de uma aplicação pois aumentaria a quantidade de acesso facilitando a memorização das tarefas; e a divulgação pois daria ênfase as tarefas que precisam ser feitas pouca frequência.

Contudo, o acesso à internet não possui ideias relacionadas a memorização de tarefas poucos frequentes, e sim, a disponibilidade de acesso ao sistema e tarefas rotineiras; a consulta para a análise de dados são tarefas frequentes e, por fim, o uso de acesso por dispositivos móveis não será feito por todos os usuários, ou seja, apenas um indivíduo da organização terá o acesso por VPN e as ações realizadas serão as de rotina da aplicação.

DIAGRAMA DE AFINIDADE DE REQUISITOS DE USABILIDADE DO SIGIPAAerEx

USABILIDADE (PREECE, et.al., 2002):

Fator que assegura a aplicação web se tornar fácil de usar, eficiente e agradável.

UTILIDADE	EFICÁCIA	EFICIÊNCIA	SEGURANÇA	APRENDIZAGEM	MEMORIZAÇÃO
1. Acesso à Internet (AI)	1. Acesso à Internet (AI)	1. Acesso à Internet (AI)	1. Acesso à Internet (AI)	1. Acesso à Internet (AI)	2. Inclusão do manual (IMN)
2. Inclusão do manual (IMN)	2. Inclusão do manual (IMN)	2. Inclusão do manual (IMN)	2. Inclusão do manual (IMN)	3. Consulta para Análise de Dados (CAD)	4. Telas para Administradores e usuários comuns (TAU)
3. Consulta para Análise de Dados (CAD)	3. Consulta para Análise de Dados (CAD)	3. Consulta para Análise de Dados (CAD)	3. Consulta para Análise de Dados (CAD)	4. Telas para Administradores e usuários comuns (TAU)	6. Facilidade de uso (FU)
4. Telas para Administradores e Usuários Comuns (TAU)	4. Telas para Administradores e usuários comuns (TAU)	4. Telas para Administradores e usuários comuns (TAU)	4. Telas para Administradores e usuários comuns (TAU)	6. Facilidade de uso (FU)	7. Confecção de aplicativos (COAPL)
5. Acesso ao sistema por dispositivos móveis. (DISMOV)	5. Acesso ao sistema por dispositivos móveis. (DISMOV)	5. Acesso ao sistema por dispositivos móveis. (DISMOV)	6. Facilidade de uso (FU)	8. Melhor divulgação da aplicação (DIV)	8. Melhor divulgação da aplicação (DIV)
6. Facilidade de uso (FU)	6. Facilidade de uso (FU)	6. Facilidade de uso (FU)	8. Melhor divulgação da aplicação (DIV)	------	------
7. Confecção de aplicativos (COAPL)	7. Confecção de aplicativos (COAPL)	7. Confecção de aplicativos (COAPL)	------	------	------
------	8. Melhor divulgação da aplicação (DIV)	8. Melhor divulgação da aplicação (DIV)	------	------	------

Concordo com o Diagrama de Afinidade proposto para a aplicação web SIGIPAAerEx. Assinatura: _____

NOME: _____ Data: _____ Função no Sistema: _____

Figura 5.1 – Diagrama de afinidade da aplicação SIGIPAAerEX.

Com a organização de cada ideia de melhorias conectadas a uma meta de usabilidade, estas ideias passam a ser consideradas como requisitos de usabilidade uma vez que o requisito é uma condição ou uma capacidade com a qual o sistema deve estar de acordo para satisfazer seu usuário e o proprietário da aplicação. Assim, cada ideia se torna um requisito de usabilidade que deve ser quantificado de acordo com a importância de sua meta para aplicação, conforme seção 3.3.8.

5.7 Resultados obtidos na aplicação do passo 7 do método proposto USASEC

A partir deste diagrama de afinidade, deve-se montar o diagrama de hierarquia, passo 7 do método, onde cada meta de usabilidade passa ser um critério e cada ideia, incluída nesta meta por similaridade de definição no passo anterior, passa ser um subcritério (requisitos de usabilidade), conforme a Figura 3.3. Este passo é relativamente simples e serve para dar melhor visualização paras os requisitos de usabilidade e metas que estão relacionadas a eles.

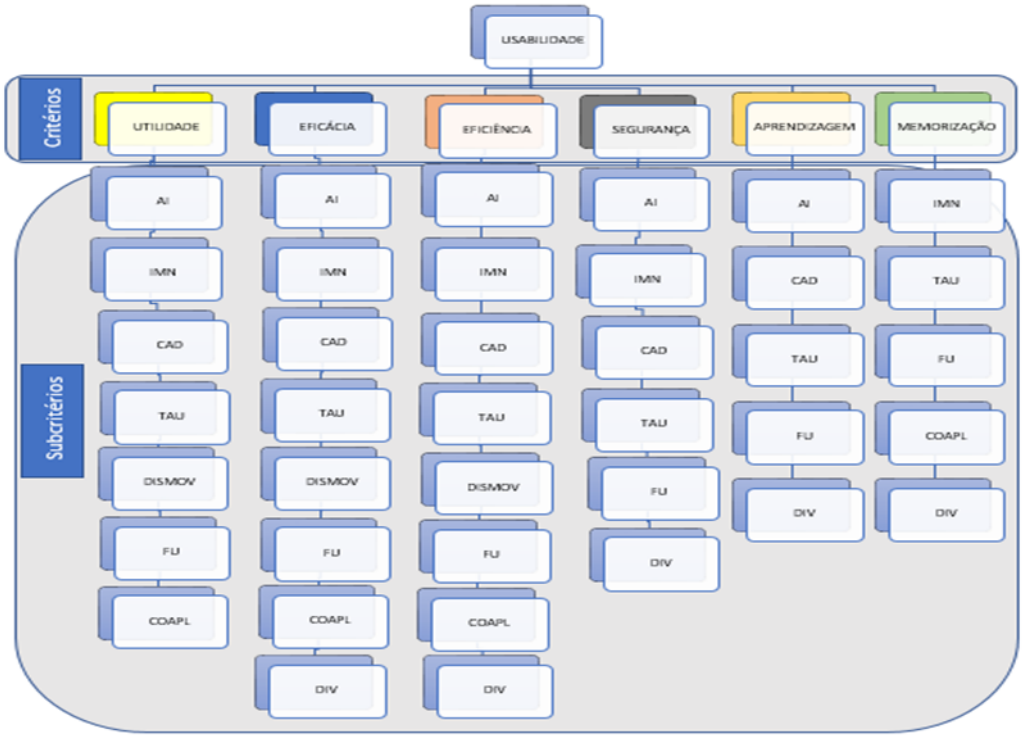


Figura 5.2 - Diagrama hierárquico do método USASEC para o SIGIPAAerEx.

5.8 Resultados obtidos na aplicação do passo 8 do método proposto USASEC

No passo 8, conhecida como processo de análise hierárquica (AHP), foi realizada a montagem da matriz de comparação. Para isso, é necessário utilizar o formulário de priorização, conforme apêndice B, para realizar o julgamento de intensidade da importância de cada critério em relação ao seu nível e de cada subcritério em relação os critérios “pai”.

Por causa do grande número de comparações necessárias, devido ao grande número de critério, conforme Figura 5.2 são seis, e subcritério, até oito, e para evitar que os julgamentos

gerassem matrizes com inconsistência e requeressem grande esforço dos decisores, foram utilizados para o cálculo a escala natural de Loostma (1990), a tabela de comparação de Olson (1995) e o método da linearização da matriz de comparação, conforme seções 2.5.2, 2.5.3 e 2.5.4.

Após isso, cada membro da equipe multidisciplinar teve que preencher, conforme a necessidade, o formulário de priorização até que as matrizes analisadas tenham sua razão de consistência menor ou igual a 0,10. Isso é necessário pois a aplicação atende a um sistema crítico que envolve tomadas de decisões que envolve a segurança em voo de passageiros e tripulantes.

Sendo assim, por mais importante que seja o julgamento feito pela autoridade representada na equipe multidisciplinar, este julgamento não pode se sobrepor a consistência do resultado final.

Feito o cálculo dos autovetores de cada subcritério (requisito de usabilidade) e critério de cada indivíduo da equipe multidisciplinar, conforme anexo C, é feita uma média geométrica dos autovetores para se chegar na MVT (tabela de máximo valor) de todos os requisitos de usabilidade dos múltiplos decisores, conforme 2.5.5.

Entretanto, para determinar quais foram os requisitos mais importantes de todos os subcritérios, requisitos de maior prioridade para o desenvolvimento da aplicação, é necessário calcular a importância relativa global de cada um deles, criando a MVT.

Para o cálculo desta importância global é necessário utilizar as fórmulas 2.10 e 2.11 da seção 2.5.1. Sendo assim, podemos associar estas duas equações da seguinte forma:

$$IR\_USj = \sum_{u=1}^{t} IR\_USi * IR\_USij / t \qquad (4.1)$$

Onde: IR_USj é a importância relativa global de cada requisito j;

IR_USi é a importância relativa de cada grupo i de requisitos;

IR_USij é a importância relativa de cada requisito j do grupo i; e

U: usuários (u = 1,2,3, …, t).

De acordo com a equação 4.1, o MVT será obtido fazendo-se o somatório dos produtos da importância deste subcritério à luz de cada critério pela importância relativa do critério correspondente, à luz do foco principal, e dividindo-se pelo total de usuários, participantes da avaliação, que fazem parta da EM.

Logo, de acordo com a Figura 5.3, que mostra as médias geométricas de cada critérios e subcritério calculados no Apêndice D, a importância relativa global (MVT) de cada requisito de usabilidade seria calculada de acordo com o exemplo do cálculo para o requisito AI:

$$AI = 0{,}2111 * 0{,}1170 + 0{,}0861 * 0{,}0853 + 0{,}0809 * 0{,}0844 + 0{,}1253 * 0{,}0547 + 0{,}0963 * 0{,}0700 / 5 = 0{,}0454 / 5 = 0{,}0091.$$

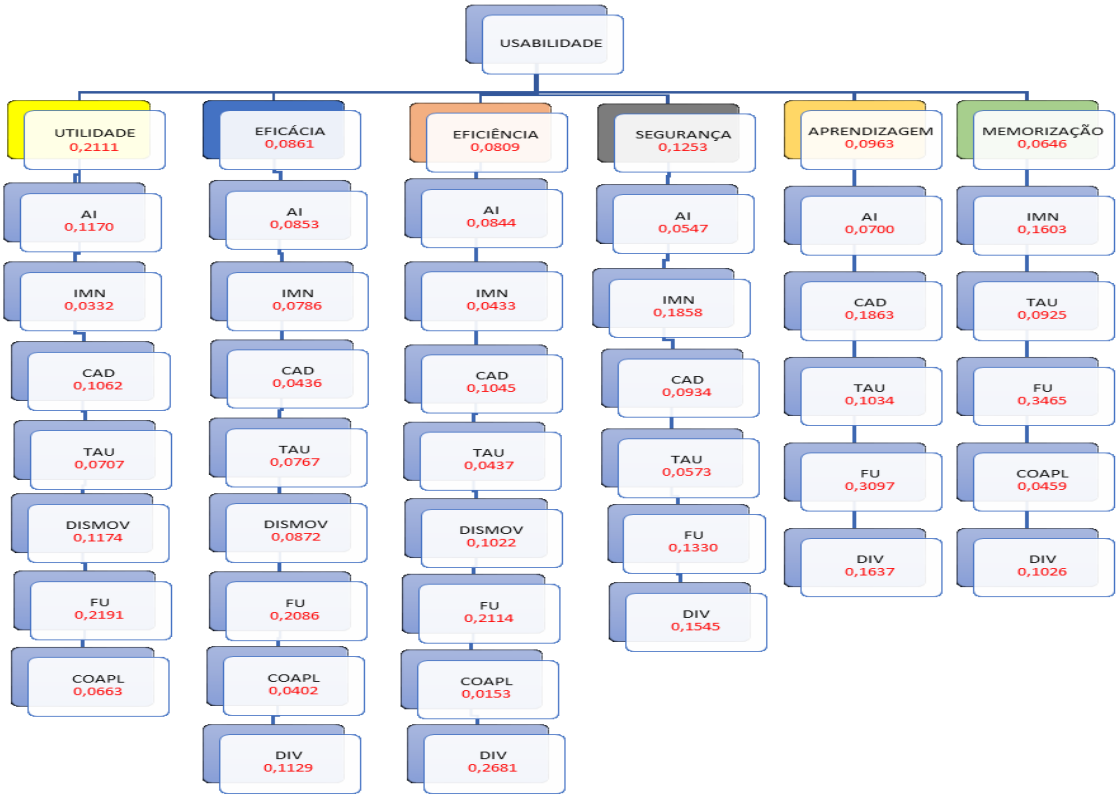


Figura 5.3 – Diagrama hierárquico com as médias dos critérios e subcritérios dos requisitos.

Desta forma, O MVT para a aplicação SIGIPAAerEx é o representado no gráfico 5.1.

Feita a classificação dos requisitos de usabilidade, é preciso comprovar se está de acordo com as necessidades dos usuários. Assim, foi aplicado o questionário fechado, conforme apêndice E, para comprovar que os julgamentos dos requisitos de usabilidade estão coerentes com as necessidades especificadas pelos tomadores de decisão.

A justificativa de realizar o AHP para o classificar os requisitos, e não apenas ouvir a usuários e colocar uma ordem nos requisitos mais coletados, seria a capacidade que a EM tem de tomar decisões de mudanças junto a aplicação e a necessidade de precisão da priorização destes requisitos para uma aplicação que apoia um sistema crítico da organização.

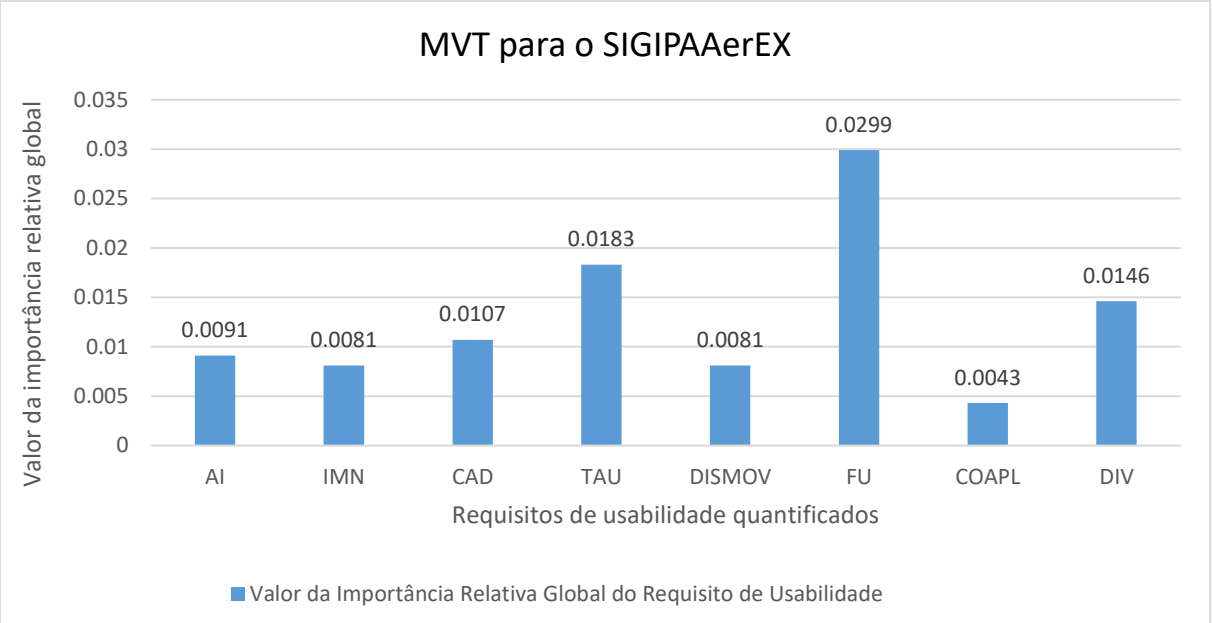


Gráfico 5.1 – Índice de importância relativa global para os requisitos para a aplicação.

Como resultado, foi possível se comprovar que os cinco usuários, que realizaram o questionário fechado, priorizaram os requisitos de usabilidade iguais aos encontrados na MVT em mais de oitenta porcento de acerto dos resultados. Ainda, foi possível classificar, dentro de cada requisito de usabilidade, quais ações eles consideram mais importantes de serem executadas na aplicação.

Tabela 5.2 – Validação da classificação dos requisitos de usabilidade.

	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV
Usuário 1	7°	5°	4°	2°	6°	1°	8°	3°
Usuário 2	1°	5°	4°	7°	3°	2°	8°	6°
Usuário 3	7°	6°	4°	3°	5°	1°	8°	3°
Usuário 4	7°	6°	4°	2°	5°	1°	8°	3°
Usuário 5	7°	5°	4°	2°	6°	1°	8°	3°
Ordem da MVT	7°	5°	4°	2°	6°	1°	8°	3°

5.9 Resultados obtidos na aplicação do passo 9 do método proposto USASEC

De posse deste último autovetor (MVT), conforme o gráfico 5.1, é encerrada o passo 8 do método USASEC. A MVT com as importâncias relativas global de cada requisito de

usabilidade deve preencher o “quarto 1” da casa da qualidade, conforme Figura 5.4, para iniciar a comparação entre a “voz do usuário” e as características técnicas de segurança da aplicação. Com isto, inicia-se o passo 9 do método USASEC.

Importância Relativa (IR_SS)		
REQUISITOS DE USABILIDADE	TABELA DE MÁXIMO VALOR (MVT)	
	US 1.1 LIBERAR O ACESSO A INTERNET (AI)	0.0092
	US 1.2 INCLUSÃO DE MANUAL NA APLICAÇÃO (IMN)	0.0081
	US 1.3 APERFEIÇOAR A CONSULTA PARA ANÁLISE DE DADOS (CAD)	0.0107
	US 1.4 CRIAR TELAS DIFERENTES PARA ADMINISTRADORES E USUÁRIOS COMUNS (TAU)	0.0183
	US 1.5 REALIZAR ACESSO POR DISPOSITIVOS MÓVEIS (DISMOV)	0.0081
	US 1.6 FACILIDADE DE USO PELO USUÁRIO (FU)	0.0299
	US 1.7 CONFECÇÃO DE UM APLICATIVO PARA O SISTEMA (COAPL)	0.0043
	US 1.8 DIVULGAÇÃO DO USO DA APLICAÇÃO (DIV)	0.0146

Figura 5.4 – Valores da MVT para os requisitos de usabilidade

Para a realização do último passo do método USASEC, com a EM reunida, é explicada a necessidade de chegar a um compromisso de entendimento para evitar conflito em busca de um objetivo comum. Este objetivo é a priorização dos requisitos já ponderados que satisfazem cada segmento de usuário sem comprometer a segurança da informação, tanto da aplicação como das informações dos usuários que trafegam pala aplicação.

Antes de começar o preenchimento da casa da qualidade para o método USASEC, foi realizada uma palestra com os membros da equipe para definir como será feito o preenchimento e foi passada uma explicação para todos os membros sobre os seguintes conceitos: o que são vulnerabilidades, quais são as vulnerabilidades que serão avaliadas no sistema e como elas acontecem, conforme tabela 2.1, bem como, qual a relação das vulnerabilidades com os sete princípios de segurança da informação e suas definições. Por fim, foi explicado como será feito a integração dos requisitos de usabilidades com os requisitos de segurança, através do quarto 3, conforme seção 3.3.9.

Assim, começa-se o passo 9 com todos os integrantes da EM juntos e relacionando a análise de segurança da aplicação com os princípios de segurança da informação. Logo, serão relacionados os itens da análise interna do impacto das vulnerabilidades com os requisitos de segurança da informação, conforme a seção 3.3.9 do método USASEC.

Inicialmente, começa-se a preencher o telhado, quarto 6, seguindo na linha horizontal relacionada a vulnerabilidade que pode gerar impacto sobre o princípio de segurança. Ou seja, conforme a Figura 5.5, é considerado o conceito de injeção de código SQL e analisado se há impacto sobre os princípios de confidencialidade, autenticidade, integridade, não-repudio, conformidade, controle de acesso e disponibilidade. Assim, conforme cada conceito destes princípios, a EM pontuará o princípio com um ponto, colocando um símbolo de (+) no cruzamento entre a vulnerabilidade e o princípio de segurança considerado. Caso não haja impacto, a equipe deve pontuar o princípio com zero ponto colocando o símbolo de (-).

Após todos os requisitos serem analisados de acordo com a vulnerabilidade prevista no quarto 5, o valor atribuído para cada princípio de segurança é o somatório de todos os pontos (+) atribuídos para aquele princípio, conforme Figura 5.5.

Neste momento, é importante que os todos os membros da equipe cheguem a um consenso de quais vulnerabilidades podem causar uma ameaça para o tipo de aplicação que está sendo utilizada. Por isso, os membros da equipe multidisciplinar que representam o segmento técnico dos usuários, analista de segurança e desenvolvedor, participam ativamente deste passo.

A função destes é mostrar como a aplicação foi desenvolvida e se aquela vulnerabilidade tem impacto em relação ao princípio de segurança que está sendo analisado. Como mostrado na Figura 5.5; para a aplicação alvo foram pontuados, no princípio de segurança de confidencialidade, as vulnerabilidades A1, A2, A5 e A6.

A vulnerabilidade A3 não foi considerada pois o sistema não utiliza *browser* para acessar conteúdo no servidor, a A4 não foi considerada pois todas as funções de acesso ao sistema estão ocultas, ou seja, não são expostas na *Uniform Resource Locator* (URL) do *browser* por ocasião dos acessos. Assim, não é possível conectar-se a dados da seção passando referência a objetos pela URL da aplicação.

Já para a vulnerabilidade A7 não foi pontuada pois o sistema possui 4 camadas de acesso para controle aos usuários. A vulnerabilidade A8 não foi considerada pelo mesmo motivo da A3, a A9 por todos os componentes da aplicação terem sido feitos pelos próprios desenvolvedores e a A10 por não existirem de redirecionamento para páginas desconhecidas na aplicação.

Análise interna do Impacto das vulnerabilidades		TELHADO (inter-relação dos "Comos")						
A1	INJEÇÃO DE CÓDIGO SQL	+	+	+	+	+	+	+
A2	AUTENTICAÇÃO DE GERENCIAMENTO DE SESSÃO	+	+	+	+	+	+	-
A3	CROSS-SITE SCRIPTING (XSS)	-	-	-	-	-	-	-
A4	REFERÊNCIA INSEGURA E DIRETA A OBJETOS	-	-	-	-	-	-	-
A5	CONFIGURAÇÃO INCORRETA DE SEGURANÇA	+	+	+	+	+	+	+
A6	EXPOSIÇÃO DE DADOS SENSÍVEIS	+	-	-	-	-	-	-
A7	FALTA DE CONTROLE PARA O NÍVEL DE ACESSO	-	-	-	-	-	-	-
A8	CROSS-SITE REQUEST SCRIPTING (CSRF)	-	-	-	-	-	-	-
A9	COMPONENTES VULNERÁVEIS CONHECIDOS	-	-	-	-	-	-	-
A10	REDIRECIONAMENTO E ENCAMINHAMENTO INVÁLIDO	-	-	-	-	-	-	-

LEGENDA		
+	1 Ponto	Relação Direta
-	0 Ponto	Não Relação
9	Forte	Relação dos "O que'd X Como"
3	Moderado	
1	Fraco	
US	Requisitos de usabilidade	
SS	Princípios de Segurança	

Figura 5.5 – Análise dos requisitos de segurança para a aplicação SIGIPAAerEx

Assim, todas as vulnerabilidades foram analisadas de acordo com o impacto que ela pode gerar no princípio de segurança correspondente. A diferença para o princípio de disponibilidade para a vulnerabilidade A2 foi colocada como negativo pois apesar do roubo de sessão ser uma vulnerabilidade que pode ameaçar a aplicação, por falta de alguns controles para mitigá-lo, ele não chega a criar uma indisponibilidade para todo o sistema.

Já a A6, por causa da natureza das informações que trafegam pela aplicação, pode ocorrer um vazamento de informações confidenciais por uma vulnerabilidade que consiga expor os dados da aplicação. Contudo, a exposição destes dados não chega a impactar os outros princípios, segundo a EM.

A partir da análise de cada um destes princípios de segurança em relação as vulnerabilidades, é possível identificar qual é o princípio que mais afeta a aplicação, no caso do SIGIPAAerEx é a confidencialidade, conforme Figura 5.5. Com todos os princípios pontuados em ordem de importância é possível observá-los como uma capacidade que se pretende alcançar para garantir a segurança das informações e dos usuários que manipulam estas. Desta forma, é possível, então, considerar estes princípios como requisitos de segurança a serem alcançados.

Cabe ressaltar, a importância destes requisitos de segurança está ligada a quantidade de vulnerabilidades do quarto 6 que podem impactá-los. Ou seja, quanto maior o número de vulnerabilidades que podem incidir sobre o requisito, maior é a sua importância para a aplicação.

Com a importância relativa global (MVT) de usabilidade e a importância relativa dos requisitos de segurança, obtidas pela soma dos pontos do quarto seis e mostrada no quarto dois, é possível realizar a integração dos impactos de cada um destes requisitos no quarto 3 (relação dos “o quê’s” *versus* “como”). Nesta matriz de relacionamentos preenche-se, de forma

consensual, a pontuação do relacionamento entre os requisitos de usabilidade e os requisitos técnicos de segurança da informação, conforme seção 3.3.9.

Assim, pode-se relacionar uma necessidade do usuário fracamente (1), moderadamente (3) ou fortemente (9) a um requisito técnico de segurança. Como exemplo, na Figura 5.6, observamos que o requisito do usuário de liberação por acesso à internet (AI) pode impactar fortemente (9) todos requisitos de segurança, uma vez que, segundo a Equipe Multidisciplinar (EM), a abertura do acesso à internet externa impacta de maneira muito forte todos os requisitos de segurança uma vez que terão que ser revistos todos os procedimentos de segurança para atender está necessidade do usuário. Desta forma, as ações que estão relacionadas a liberação de acesso pela Internet, prevista na tabela 4.2 (UVT), devem considerar impactar fortemente cada um destes requisitos de segurança.

	REQUISITOS DE SEGURANÇA DA INFORMAÇÃO	Importância Relativa	SS 2.1 CONFIDENCIALIDADE	SS.2.2 AUTENTICIDADE	SS.2.3 INTEGRIDADE	SS 2.4 NÃO-REPUDIO	SS 2.5 CONFORMIDADE	SS 2.6 CONTROLE DE ACESSO	SS 2.7 DISPONIBILIDADE	Análise interna usuários
	Importância Relativa (IR_SS)		4	3	3	3	3	3	2	
REQUISITOS DE USABILIDADE	TABELA DE MÁXIMO VALOR (MVT)		Relação: o que x como							Avaliação estratégica
	US 1.1 LIBERAR O ACESSO A INTERNET (AI)	0.0092	9	9	9	9	9	9	9	5
	US 1.2 INCLUSÃO DE MANUAL NA APLICAÇÃO (IMN)	0.0081	0	0	0	0	0	0	1	5
	US 1.3 APERFEIÇOAR A CONSULTA PARA ANÁLISE DE DADOS (CAD)	0.0107	3	0	0	0	1	0	0	5
	US 1.4 CRIAR TELAS DIFERENTES PARA ADMINISTRADORES E USUÁRIOS COMUNS (TAU)	0.0183	0	0	0	0	0	0	0	4
	US 1.5 REALIZAR ACESSO POR DISPOSITIVOS MÓVEIS (DISMOV)	0.0081	9	9	9	9	9	9	9	3
	US 1.6 FACILIDADE DE USO PELO USUÁRIO (FU)	0.0299	3	3	3	1	3	3	3	1
	US 1.7 CONFECÇÃO DE UM APLICATIVO PARA O SISTEMA (COAPL)	0.0043	1	1	1	1	1	1	1	4
	US 1.8 DIVULGAÇÃO DO USO DA APLICAÇÃO (DIV)	0.0146	3	3	3	3	3	3	3	5

Figura 5.6 – Integração e análise dos requisitos de usabilidade e segurança.

Já o requisito IMN foi considerado que não impacta a maioria dos requisitos de segurança, contudo foi atribuída uma pontuação de fracamente impactado (1) para o requisito de disponibilidade pois, segunda a EM, pode-se aumentar a quantidade de usuários que buscam entender como usar, de forma correta ou não, as ferramentas da aplicação. Assim, um aumento da quantidade de usuários utilizando o sistema pode impactar fracamente a disponibilidade da aplicação.

Para o requisito CAD, a segurança pode ser moderadamente impactada no requisito confidencialidade tendo em vista que uma maior quantidade de usuários buscando informação confidencias no sistema podem impactar este requisito, tendo em vista que a quebra de confidencialidade está relacionada a ataques passivos; ou seja, aqueles que se baseiam em monitoramento e escutas da transmissão destas informações. Logo, quanto maior a quantidade de informações que estão sendo transmitidas para consulta, maior a possibilidade de um ataque passivo obter sucesso.

Contudo, a conformidade foi fracamente impactada pois a consulta de alguns dados estatísticos são feitas apenas pelos usuários administradores do sistema. Assim, a abertura para outros níveis de usuários pode impactar a conformidade da aplicação. Logo, para ser atendido este requisito, deve-se criar novas norma e regulamentos que responsabilizem o vazamento destes dados de consulta em regulamentos internos da organização.

Os demais requisitos de segurança não foram pontuados pois apenas a consulta dos dados não impactam o conceito de cada um destes requisitos. Ou seja, a integridade e autenticidade das informações consultadas não são impactadas, bem como, o controle de acesso, não-repúdio e disponibilidade das informações não são modificados com o aperfeiçoamento da consulta a estes dados.

O requisito TAU não foi pontuado em nenhum requisito de segurança pois, segundo o desenvolvedor representante da EM e que trabalhou na confecção da aplicação, esta ferramenta seria muito simples de implementar uma vez que o sistema já possui níveis de acesso por usuários. Desta forma, a inclusão de uma tela diferenciada para usuários administradores e usuários comuns já é possível e não impacta a segurança do sistema.

Contudo o requisito DISMOV foi fortemente pontuado em todo os seus requisitos de segurança uma vez que a abertura do acesso ao sistema por uma rede VPN dependeria da inclusão de criptografia própria e de regras e normas para utilização destes dispositivos. Bem como, do descarte e procedimento em caso de perda e vazamento de informações confidencias.

Já o requisito de usabilidade FU foi moderadamente quantificada tendo em vista que a melhoria da interface do usuário pode trazer impactos como redução do controle de acesso, maior quantidade de acesso, o que pode diminuir a disponibilidade e possíveis erros internos ao sistema; mudanças nas regras internas de acesso ao sistema são necessárias para atender a conformidade integrada a facilidade de uso, contudo, a facilidade de uso exime a utilização de chaves criptográficas para evitar não-repudio uma vez que isto aumentaria a complexidade da realização de tarefas na aplicação; manter a integridade dos dados que são acessados e enviados, para assegurar a autenticidade do usuário de origem e destino das transmissões e a

confidencialidade das informações. Assim, as ações que estão relacionadas a facilidade de uso, prevista na tabela 5.1 (UVT), devem considerar impactar moderamente cada um destes requisitos de segurança.

A confecção de um aplicativo de celular para atender a necessidade do usuário (COAPL) foi considerada pela EM como um requisito que influência fracamente a segurança do sistema, uma vez que hoje a equipe de desenvolvimento do software já tem o aplicativo pronto mas não foi autorizada pela organização a utilização do mesmo pois viola regras e leis internas da organização, requisitos de conformidade. A confidencialidade seria fracamente impactada pois a aplicação seria utilizada apenas para consulta e envio dos Rel Prev's; a autenticidade, integridade, não-repudio, controle de acesso e disponibilidade seriam semelhantes a que já está sendo utilizada pelo sistema com mudanças na forma como os usuários passariam a utilizar com mais frequência a aplicação *web*.

Por fim, a EM pontuou moderadamente o atendimento do requisito de usabilidade de divulgação da aplicação pois, com uma maior divulgação com palestras, seminários e treinamentos; a quantidade de usuários acessando o sistema irá aumentar de forma contínua. Assim, a possibilidade de um usuário realizar atividades que possam comprometer a aplicação, de forma intencional ou não, também irá aumentar.

Ainda, no quarto 4, a EM deve pontuar de maneira estratégica quais os requisitos de usabilidade que eles consideram mais importante. Esta pontuação pode levar em consideração os requisitos que eles consideram mais importante, em uma escala de 1 a 5, ou podendo levar em consideração em *bechmarketing* de outras aplicações que eles já tenham tido contato e que podem gerar uma análise competitiva entre os softwares.

Para o preenchimento do quarto 4 foram considerados com nota máxima os requisitos de AI, CAD, IMN e DIV, pela EM, pois existiu um entendimento de que estes requisitos estão alinhados com a estratégia da organização de manter dados de segurança de voo atualizados e disponíveis de forma rápida para todos os usuários e em tempo real.

Para o requisito de TAU foi atribuída a nota 4 uma vez que o requisito COAPL pode atender a disponibilidade dos dados em tempo real necessárias para o usuário, contudo muitas modificações no sistema de aviação da organização teriam de ser feitas, bem como, a utilização de telas diferenciadas, requisito TAU, pode aumentar a satisfação do usuário de maneira rápida, eficiente e com um pequeno esforço.

A nota 3 foi atribuída ao requisito DISMOV pela complexidade de atender as demandas da utilização de uma rede VPN com criptografia própria para a inclusão deste requisito. Assim, ele pode uma solução viável mais exigirá um grande esforço.

A nota mais baixa foi dada para o requisito FU pois, segundo a EM todas as informações que estão sendo exibidas atualmente no sistema são necessárias a diversos tipos de usuários. Desta forma, o que seria necessário era organizar as informações em níveis e abas de forma que o usuário possa filtrar as informações que está procurando. Assim, o impacto deste requisito, de forma estratégica seria muito baixo uma vez que a informação necessária já esta sendo exibida e o que falta para o usuário é um treinamento de como chegar até esta informação.

Durante a avaliação do quarto 3 da casa da qualidade, os valores do MVT, previstos no quarto um, bem como a ordem dos requisitos de usabilidade foram colocadas de forma aleatória para não influenciar a EM em pontuar de maneira diferenciada os requisitos que aparecem primeiro na tabela de máximo valor. Logo, de acordo com a Figura 5.6, o primeiro requisito de usabilidade AI não é o mais importante segundo os valores da MVT.

Desta forma, todos os requisitos de usabilidade foram analisados de acordo com cada um dos requisitos de segurança afim de observar o impacto que a integração destes requisitos de usabilidade pode gerar nos requisitos de segurança, objetivo proposto pelo método USASEC. Com isso, é possível ter a capacidade de priorizar os requisitos que trazem maior impacto sobre a usabilidade e segurança na aplicação *web* e, ainda, pode-se atender as necessidades dos usuários quanto as implementações que devem ser realizadas, sem gerar vulnerabilidades futuras e utilizando recursos focados nos requisitos que mais impactam estas aplicações.

5.10 Resultados do estudo de caso da aplicação SIGIPAAerEX

De acordo com a Figura 5.5, o requisito de segurança de confidencialidade foi o que mais se destacou na análise feita pela EM. Isto reforça o aspecto da aplicação de manter a proteção dos dados transmitidos e a propriedade da informação pela que não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização. Ou seja, as características da aplicação, com sua forma anônima de gerar relatórios de prevenção (Rel Prev) de acidentes, corroboram com a confidencialidade de quem está confeccionando o Rel Prev, e evitando o conflito que pode surgir por erros causados por falhas humanas.

Um outro aspecto de confidencialidade do sistema que comprova a validade deste requisito é que as RSV que a aplicação gera para os usuários executarem, como realização de tarefas e divulgação de problemas em determinadas aeronaves, só podem ser expostas após todas as autoridades competentes realizarem a análise das consequências deste relatório para todo o sistema aviação da organização. Assim, o caráter sigiloso da informação, apesar de uma

certa urgência para tomada de decisão, garante a não realização de procedimentos que possam atingir de forma sistêmica toda a estrutura operacional da organização.

Com a utilização do método USASEC, apesar do processo de análise hierárquica ter encontrado o requisito de facilidade de uso FU como o mais importante, quando o requisito de usabilidade e integrado a requisitos de segurança e avaliação estratégica da EM ele perde a prioridade, sendo ultrapassado por outro requisito, quando sua importância absoluta é calculada, conforme Figura da casa da qualidade 5.7.

Este cálculo é feito através da soma do produto de cada requisito de acordo com a análise que foi feita no quarto 3 e 4. Ou seja, o cálculo pode ser feito de maneira simples de acordo com o seguinte exemplo para usabilidade:

$$AI = 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*9 + 0{,}0092*5 = 0{,}6256.$$

E pode ser feito o cálculo da seguinte maneira para os requisitos de segurança confidencialidade:

$$\text{Confidencialidade} = 4*9+4*0+4*3+4*0+4*9+4*3+4*1+4*3 = 112.$$

Estes dois exemplos mostram os dois requisitos que mais impactam a aplicação quando integrados. Logo, a interpretação do método se dá identificando os dois requisitos com maior peso absoluto, ou seja, que mais pontuaram na soma do produto de cada um deles, conforme Figura 5.7.

Identificando os requisitos que foram analisados, é possível observar que apesar dos maiores requisitos de usabilidade serem o FU e TAU quando eles são integrados com requisitos de segurança suas prioridades mudam. Ou seja, quando estes requisitos são analisados de forma integrada entre usabilidade e segurança, eles podem ser priorizados em uma ordem diferente, conforme tabela 5.2.

Logo, com a utilização do método podemos observar que existe uma diferença na priorização quando se integra segurança, do que apenas focar na usabilidade. Isso ocorre devido às características técnicas de segurança que devem ser consideradas ao analisar os impactos que os requisitos de usabilidade irão obter quando implementados na aplicação. Outro aspecto que influenciou muito a casa da qualidade, no método USASEC, foi quanto a avaliação estratégica interna dos usuários da EM sobre o requisito de usabilidade.

Para a EM, está avaliação fica diretamente relacionada aos objetivos da aplicação, conforme previstos no SIPAAEx da seção 4. Logo, o requisito IMN foi pontuado com a nota

cinco, pois além de descrever o que cada usuário deve fazer, este vai evitar que o mesmo realize atividades fora de suas atribuições.

Análise interna do Impacto das vulnerabilidades		TELHADO (inter-relação dos "Comos")						
A1	INJEÇÃO DE CÓDIGO SQL	+	+	+	+	+	+	+
A2	AUTENTICAÇÃO DE GERENCIAMENTO DE SESSÃO	+	+	+	+	+	+	-
A3	CROSS-SITE SCRIPTING (XSS)	-	-	-	-	-	-	-
A4	REFERÊNCIA INSEGURA E DIRETA A OBJETOS	-	-	-	-	-	-	-
A5	CONFIGURAÇÃO INCORRETA DE SEGURANÇA	+	+	+	+	+	+	+
A6	EXPOSIÇÃO DE DADOS SENSÍVEIS	+	-	-	-	-	-	-
A7	FALTA DE CONTROLE PARA O NÍVEL DE ACESSO	-	-	-	-	-	-	-
A8	CROSS-SITE REQUEST SCRIPTING (CSRF)	-	-	-	-	-	-	-
A9	COMPONENTES VULNERÁVEIS CONHECIDOS	-	-	-	-	-	-	-
A10	REDIRECIONAMENTO E ENCAMINHAMENTO INVÁLIDO	-	-	-	-	-	-	-

LEGENDA		
+	1 Ponto	Relação Direta
-	0 Ponto	Não Relação
9	Forte	Relação dos "O que'd X Como"
3	Moderado	
1	Fraco	
US	Requisitos de usabilidade	
SS	Princípios de Segurança	

	REQUISITOS DE SEGURANÇA DA INFORMAÇÃO	Importância Relativa	SS.2.1 CONFIDENCIALIDADE	SS.2.2 AUTENTICIDADE	SS.2.3 INTEGRIDADE	SS.2.4 NÃO-REPUDIO	SS.2.5 CONFORMIDADE	SS.2.6 CONTROLE DE ACESSO	SS.2.7 DISPONIBILIDADE	Análise interna usuários	IMPORTÂNCIA ABSOLUTA IR_US
	Importância Relativa (IR_SS)		4	3	3	3	3	3	2		
REQUISITOS DE USABILIDADE	TABELA DE MÁXIMO VALOR (MVT)		Relação: o que x como							Avaliação estratégica	
	US 1.1 LIBERAR O ACESSO A INTERNET (AI)	0.0092	9	9	9	9	9	9	9	5	0.6256
	US 1.2 INCLUSÃO DE MANUAL NA APLICAÇÃO (IMN)	0.0081	0	0	0	0	0	0	1	5	0.0486
	US 1.3 APERFEIÇOAR A CONSULTA PARA ANÁLISE DE DADOS (CAD)	0.0107	3	0	0	0	1	0	0	5	0.0963
	US 1.4 CRIAR TELAS DIFERENTES PARA ADMINISTRADORES E USUÁRIOS COMUNS (TAU)	0.0183	0	0	0	0	0	0	0	4	0.0732
	US 1.5 REALIZAR ACESSO POR DISPOSITIVOS MÓVEIS (DISMOV)	0.0081	9	9	9	9	9	9	9	3	0.5346
	US 1.6 FACILIDADE DE USO PELO USUÁRIO (FU)	0.0299	3	3	3	1	3	3	3	1	0.5980
	US 1.7 CONFECÇÃO DE UM APLICATIVO PARA O SISTEMA (COAPL)	0.0043	1	1	1	1	1	1	1	4	0.0473
	US 1.8 DIVULGAÇÃO DO USO DA APLICAÇÃO (DIV)	0.0146	3	3	3	3	3	3	3	5	0.3796
	IMPORTÂNCIA ABSOLUTA IR_SS		112	75	75	69	78	75	52		

Figura 5.7 – Casa da qualidade do método USASEC para a aplicação SIGIPAAerEX.

Para a equipe, os requisitos AI, CAD e DIV foram pontuados com nota cinco, pois estão relacionados a integração da aviação do Exército em todo território nacional (AI), priorizar os fatores que contribuem para acidentes (CAD) e recomendar medidas preventivas e corretivas, além de, montar um programa eficiente de prevenção de acidentes (DIV).

Já os requisitos de confecção de aplicativos para o sistema e telas diferenciadas para usuários, apesar de reconhecidas como importantes, não estariam completamente ligados aos objetivos estratégicos avaliados pelos usuários internos da EM, por isso, receberam a nota quatro.

Já o acesso por dispositivos móveis foi pontuado com a nota três tendo em vista que este acesso só aconteceria em operações especificas, ou seja, apenas quando não houvesse a rede da organização para acesso a aplicação.

Por fim, a facilidade de uso que foi o requisito mais pontuado pelo MVT, foi o que teve a menor nota tendo em vista o caráter hierárquico da organização. Além de não ter nenhuma menção no objetivo do sistema sobre este requisito, para muitos membros da EM, é dever do usuário saber realizar as atividades na aplicação independente de seu grau de complexidade. Esta opinião foi reforçada tendo em vista que todos os usuários participam de uma breve explanação sobre o sistema e a necessidade de acessá-lo com frequência.

Desta forma, a avaliação estratégica interna da EM, de cada requisito de usabilidade, deve ser considerada para não redirecionar as atividades para o qual a aplicação foi criada.

Feito isso, é imprescindível a observação destes dois requisitos integrados quando for priorizar os recursos para o desenvolvimento da aplicação. Senão corre-se o risco de focar esforço demasiado em um requisito que não é tão prioritário quanto os outros.

Prioridade	REQUISITOS DE USABILIDADE ANTES DA INTEGRAÇÃO	REQUISITOS DE USABILIDADE DEPOIS DA INTEGRAÇÃO
1°	Facilidade de uso pelo usuário (FU)	Liberação do Acesso à Internet (AI)
2°	Criar telas diferentes para usuários (TAU)	Facilidade de uso pelo usuário (FU)
3°	Divulgação do uso da Aplicação (DIV)	Realizar acesso por dispositivos móveis (DISMOV)
4°	Aperfeiçoar a consulta para análise de dados (CAD)	Divulgação do uso da Aplicação (DIV)
5°	Liberar o acesso à Internet (AI)	Aperfeiçoar a consulta para análise de dados (CAD)
6°	Inclusão de manual na aplicação (IMN)	Criar telas diferentes para usuários (TAU)
7°	Realizar acesso por dispositivos móveis (DISMOV)	Inclusão de manual na aplicação (IMN)
8°	Confecção de aplicativo para o sistema (COAPL)	Confecção de aplicativo para o sistema (COAPL)

Tabela 5.3 – Comparação de priorização dos requisitos antes e depois de integrados.

Conforme a tabela 5.3, é possível observa que apesar do requisito de Facilidade de Uso (FU) ser o mais importante para a MVT, quando integrado a requisito de segurança, ele impacta de maneira inferior ao Acesso à Internet (AI). Ou seja, o esforço necessário para a equipe de segurança disponibilizar o acesso dos usuários pela Internet aberta é maior pois várias tecnologias deveram ser implementadas no sistema para que isso ocorra de forma segura.

Apesar de a avaliação estratégica o acesso à Internet a EM ter considerado a nota máxima, observa-se através do USASEC que a abertura do sistema para acesso à Internet demandaria um esforço muito grande devido à confidencialidade dos dados e, ainda, ao

consentimento de autoridades competentes, uma vez que para aplicações *Web* é necessária autorização do CDS.

Assim, a equipe multidisciplinar consegue observar que atuando Facilidade de Uso (FU) não será necessário impactar tanto a segurança e os resultados para a usabilidade e segurança da aplicação serão tão bons quanto a liberação para o acesso à Internet, ou muito próximos. Inclusive, este requisito foi considerado pela EM como de fácil execução, ou seja, não seria necessário muito esforço para implementar as ações.

Outros requisitos são observados de maneira diretamente proporcionais, tanto para o impacto na MVT, como com a integração dos requisitos de segurança. Como exemplo, pode-se observar, na tabela 5.3, que a utilização do Dispositivos Móveis (DISMOV) saiu da posição de sétimo colocado para terceiro colocado na integração dos requisitos de segurança. Logo, ao investir neste requisito atende-se as necessidades dos usuários e a de segurança da equipe técnica. Requisitos como Inclusão do Manual (IMN) e Consulta e Análise de Dados (CAD) sofreram uma pequena queda na classificação, com isso pode-se observar que eles também não são concorrentes, ou seja, a implementação destes atenderá ambos os requisitos.

Contudo, a confecção de telas diferenciadas para usuários administradores e comuns caiu de segundo colocado na MVT para a sexta colocação na integração da casa da qualidade. Isto se deve ao EM não encontrar dificuldade quanto a impactos nos requisitos de segurança da aplicação. Na verdade, a diferenciação destas telas não aumentará a segurança da aplicação pois a aplicação já diferencia, dentro de suas camadas, o acesso de cada um deste usuários. Desta forma, apesar do TAU ter caído quatro posições com a integração dos requisitos de segurança, ele também foi considerado, pela EM, de fácil implementação e considerado de pequeno esforço e impacto para segurança.

Por fim, o último requisito pontuado, a confecção de aplicativos (COAPL), apesar de impactar a segurança da aplicação fracamente, Figura 5.7, e de ter sido avaliado com nota quatro em relação ao alinhamento do requisito ao objetivo estratégico da aplicação, feito pelos usuários da EM, ele permaneceu na última colocação. Para o método, observa-se que a integração dos requisitos de segurança não muda o baixo impacto que a produção deste aplicativo poderia trazer sobre a usabilidade da aplicação.

Também, pode-se observar, uma tendência na priorização da importância relativa dos requisitos de usabilidade de acordo com o segmento representado na EM, conforme gráfico 2.

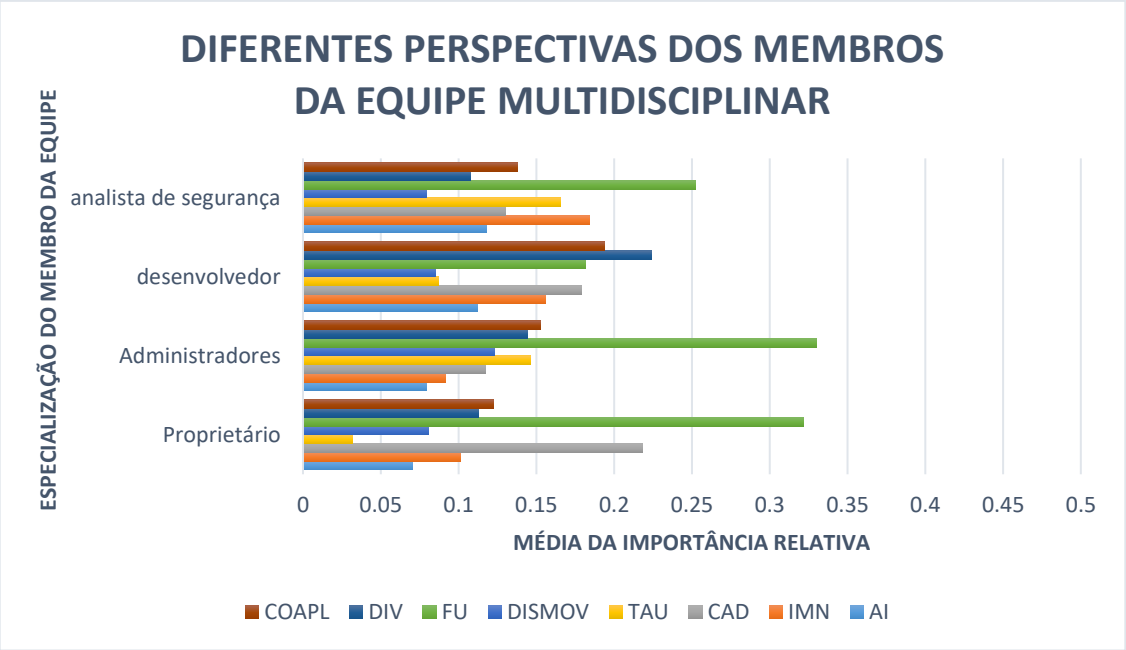


Gráfico 2 – Comparação da importância de cada requisito de usabilidade de acordo com a especialização do membro do grupo multidisciplinar.

Como pode-se observar no gráfico 2, o requisito facilidade de uso tem uma maior importância relativa para os grupos da EM de analista de segurança, administradores e proprietário. Contudo, para o desenvolvedor, a divulgação das ferramentas da aplicação é o requisito mais importante. Este gráfico mostra apenas as perspectivas dos membros da EM antes da integração dos requisitos de segurança e avaliação estratégica feita na casa da qualidade.

Comparando este gráfico 2 com a tabela 5.3 é possível observar como a priorização dos requisitos de usabilidade sofreram alteração ao incluir requisitos de segurança e a avaliação estratégica da EM.

6 Conclusão

Este trabalho de pesquisa teve por objetivo identificar, filtrar, organizar, priorizar, classificar e integrar requisitos de usabilidade e segurança para aplicações *web*, visando melhorias na qualidade do produto, priorizando as necessidades de satisfação dos usuários e analisando como os requisitos de segurança podem impactar a proteção cibernética do software.

Para alcançar este objetivo, realizou-se um estudo bibliográfico, no capitulo 2, abordando as principais definições relacionadas a usabilidade e seus métodos de avaliação, o método de Desdobramento da Função de Qualidade de Software (o Moderno QFD) e seus conceitos relacionados de diagrama de afinidade, processo de análise hierárquico e a casa da qualidade, bem como os conceitos de segurança da informação e a proteção cibernética, como vulnerabilidades para aplicação w*eb*. Em seguida, foram descritos conceitos relacionados ao processo de desenvolvimento de software com o Design Centrado no Usuário (DCU) e Interação Homem-Computador (IHC).

Alguns estudos considerados relevantes e relacionados a integração de requisitos de usabilidade e segurança para software, como a Interação Homem-Computador e Segurança (IHCSeg) também foram investigados, descritos e discutidos.

O estudo bibliográfico e a investigação dos trabalhos relacionados fundamentaram a concepção de um método para a integração de requisitos de usabilidade e segurança de softwares, envolvendo uma derivação do moderno SQFD e fornecendo subsídios para a sua aplicação.

O método de integração de requisitos de usabilidade e segurança para aplicações *web* com o objetivo de manter a proteção cibernética da aplicação, proteção esta que deve ser de caráter permanente, foi concebido e fundamentado nas características do moderno QFD para Software com ênfase nos requisitos de usabilidade e segurança para a aplicação. Este método foi nomeado, a partir do termo em inglês ***USA****bility e* ***SEC****urity* (USASEC).

O método proposto, constitui-se de nove passos, onde são realizados os passos previstos no moderno QFD com ênfase em requisitos de usabilidade e segurança. Para isto, foi necessária a realização da montagem de uma equipe multidisciplinar de usuários que possuissem o poder de tomar decisões sobre como a aplicação poderia ser refinada em proveito dos usuários. Estas características multidisciplinares da equipe atendem ao princípio de avaliação de usabilidade em percurso pluralístico e, com o uso do processo de análise hierárquica (AHP), resolveu-se as diferentes perspectivas de cada membro da equipe.

Os nove passos do método proposto, USASEC, foram compostas dos seguintes itens: identificação do alinhamento da aplicação com a estratégia da organização e identificação dos segmentos dos usuários; montagem e confecção de diagramas de fluxo e tarefas ou prototipação do software; coleta das ideias de melhoria de usabilidade no local onde o software está sendo utilizado; filtro de requisitos através da confecção de uma Tabela com Voz do Usuário (UoV); e organização dos mesmos com a realização do diagrama de afinidade. Ainda, o julgamento par-a-par de cada requisito de usabilidade com o processo AHP para a montagem da Tabela de Máximo Valor (MVT) para classificar os requisitos de usabilidade e, por fim, a análise e classificação de requisitos de segurança com a finalidade de integrá-los com uma ferramenta denominada de casa da qualidade.

A escolha da aplicação mais ligada à estratégia de negócio da organização teve por objetivo assegurar que, entre os diversos software e aplicações que ela possuía, o método foi aplicado naquele que mais vai apoiou o sucesso da organização, ou pelo menos que esteve ligado aos objetivos estratégicos. Feito isto, identificou-se qual o segmento chave de usuários atendido, afim de, utilizando-se o design centrado no usuário, ouvir suas demandas e necessidades. Como o software utilizado para a validação do método encontrava-se em fase final de desenvolvimento e implantação, não foi necessário realizar diagramas de fluxo e prototipação para análise dos usuários.

Assim, para o passo 4 do método proposto foi aplicado um questionário aberto, nos locais onde os usuários utilizaram a aplicação, para se ouvir e coletar as reais necessidades dos mesmos. Com base nestas premissas, foram filtradas as ideias com a confecção de uma tabela com a voz do usuário (UVT) para se classificar as ideias, de acordo com sua similaridade, durante o passo 5. Feito isto, foi elaborado, pela equipe multidisciplinar (EM), o diagrama de afinidade, passo 6, de acordo com os conceitos de usabilidade de [30].

A partir de metas definida por esse conceito, cada ideia foi organizada, de acordo com uma meta a ser alcançada e quantificada. Assim, estas ideias passaram a ser analisadas como requisitos que deveriam ter um certo esforço para alcançá-las. Logo, no passo 7, este diagrama de afinidade foi transformado em diagrama hierárquico onde as metas, consideradas como os critérios, e os requisitos, como subcritérios a serem avaliados no processo de análise hierárquica (AHP).

De posse, dos requisitos, no passo 8 do método, foi realizado o julgamento de cada par de requisitos para avaliação e quantificação destes. Com a realização do AHP foi possível requantificá-los, utilizando-se um método científico, de acordo com o moderno QFD para Software. Logo, por causa da grande quantidade de tomadores de decisão da equipe

multidisciplinar, foi calculada a média geométrica de cada autovetor, a fim de se obter a tabela de máximo valor (MVT) para o nono e último passo do método.

No passo 9 do USASEC, foi realizada uma análise dos requisitos de segurança da informação que podiam influenciar na aplicação, e foi possível quantificá-los, através de uma análise das principais vulnerabilidades que poderiam impactar o software. Feito isto, pode-se integrar estes requisitos de segurança com os de usabilidade da MVT utilizando-se a técnica da casa da qualidade.

Para propiciar a validação do método proposto, foi desenvolvido um estudo de caso com um software de gerenciamento de investigação e prevenção de acidentes aeronáutico do Exército, capaz de reunir os relatórios de prevenção de acidentes de toda aviação do Exército e consultas estatísticas e dados com os principais problemas e acidentes com aeronaves da instituição. Esta aplicação teve por objetivo apoiar a segurança de voo de todas as aeronaves do Exército e foi um projeto da Divisão de Tecnologia da Informação do Comando de Aviação do Exército (CAvEx), localizado em Taubaté-SP.

Durante a realização do método USASEC, na aplicação web de Gerenciamento de Investigação e Prevenção de Acidentes Aéreos do Exército (SIGIPAAerEx), foi possível obter-se resultados mostrando que somente a avaliação de requisitos de usabilidade não atende de forma completa a priorização dos requisitos. Quando os requisitos de usabilidade foram integrados aos de segurança, foi possível observar uma mudança na prioridade daqueles que mais iriam impactar a aplicação.

Assim, com a utilização do método proposto nesta pesquisa, foi possível satisfazer não apenas os usuários, mas também, os requisitos técnicos de segurança que representam as características técnicas que a aplicação necessita. Com os resultados que mostraram que a priorização atendeu a necessidade dos usuários chaves, em 80% dos casos, com matrizes consistentes conforme descrito no Capítulo 2 em sua seção 2.5.1 2, com resultados demonstrados no Apêndice C, e com a anuência dos tomadores de decisão sobre a aplicação destes requisitos na aplicação demonstrados no Capítulo 5 e seção 5.9, onde foi validada a MVT, o método USASEC atingiu com sucesso a efetividade que se propôs no estudo de caso em que foi aplicado, quanto a integração de requisitos de usabilidade e segurança da aplicação, almejando assim atender a satisfação do usuário e ouvir a equipe técnica de segurança, quanto aos requisitos de segurança para adequa-lá à a proteção cibernética da aplicação.

6.1 Principais Contribuições

Como principal contribuição deste trabalho de pesquisa, apresentam-se a concepção de um método de avaliação de usabilidade e segurança para o desenvolvimento de aplicações *Web*, capaz de integrar requisitos de usabilidade e segurança para a melhoria da qualidade do software. No método, pode-se elencar as seguintes contribuições especificas, conforme seção 1.4, a partir da integração dos requisitos de usabilidade e segurança:

1. Eles são verdadeiramente os requisitos de usabilidade que o usuário precisa pois representam a Voz do Usuário (*User of Voice*) e agregam valor aos requisitos primários do seu software;
2. Eles conseguem focar nas necessidades tanto dos usuários de usabilidade quanto dos desenvolvedores com relação à segurança. Desta forma, atendendo a estes dois aspectos com maior ênfase, e diminui-se o atraso nas entregas do projeto de software, nos conflitos e no retrabalho durante o ciclo de vida de desenvolvimento da aplicação;
3. Enriquecem a comunicação entre usuários e desenvolvedores no que diz respeito às suas necessidades;
4. Aumentam o raciocínio lógico entre as metas dos produtos e processos para elaboração de um projeto de software mais conciso e preciso;
5. Facilitam o acompanhamento do projeto e de seus conflitos para demonstrar ao proprietário do projeto como estes itens estão sendo tratados;
6. O projeto do software fica mais fácil de acompanhar, mais acordado entre as partes interessadas e com uma melhor definição do produto final;
7. O método proposto, USASEC, pode ser aplicado em novos softwares e para melhorar a satisfação e segurança dos usuários dos softwares já existentes;
8. Ajudam a ter um impacto positivo no mercado, logo no início do desenvolvimento do software, tendo em vista que os usuários participam na confecção dos requisitos para o projeto através do EM;
9. Os usuários demostraram maior interesse em utilizar a aplicação, por ter participado da elaboração de requisitos para confecção ou melhora do software; e
10. Facilitam, quando necessário, a se chegar a uma solução de interesse reciproco entre mais de um usuário (cliente) que possam ter conflitos.

6.2 Conclusões Gerais

Em função dos resultados alcançados com a aplicação do método USASEC nesta pesquisa, espera-se que o método proposto possa ser aplicado com sucesso também em outros domínios de conhecimento que envolvam o desenvolvimento de aplicações e softwares com qualidade, com ênfase na demanda da proteção cibernética.

Acredita-se também que, com a evolução do método, se possa aprofundar a utilização completa do QFD para Software (SQFD). Ou seja, que as outras matrizes do QFD, com componentes de segurança e usabilidade possam ser desdobradas, a fim de se atingir granularidades necessárias para o desenvolvimento de software com maior robustez e confiabilidade quanto a ataques cibernéticos.

6.3 Recomendações e trabalhos futuros.

Acredita-se que para melhorar ainda mais os resultados efetivos do método proposto com soluções dos problemas de requisitos concorrentes, seria interessante desenvolvê-lo com uma aplicação *web* ou software que esteja utilizando o método Ágil de desenvolvimento. Assim, as equipes de usabilidade e segurança da aplicação poderiam trabalhar juntas em soluções que agradam o usuário final e os desenvolvedores; assim como, ao proprietário da aplicação.

Com o objetivo do aprimoramento da integração dos requisitos de usabilidade e segurança para softwares a que se destina o método proposto, apresenta-se a seguir algumas sugestões para trabalhos futuros:

1. Utilização do método USASEC em aplicações na fase de elicitação de requisitos, envolvendo aplicações de banco *e-comerce* que possuem uma grande variedade de usuários;
2. Adaptação do método proposto para inclusão dos conceitos e desenvolvimento de softwares que utilizam UX, do inglês *User eXperience*;
3. Elaboração da próxima matriz de desdobramento, com os requisitos identificados no método USASEC, focando em componentes de usabilidade que possam ser incorporados para atender os requisitos, com componentes de segurança da *Application Security Verification Standard* (ASVS) para a aplicação;

4. Elaboração de uma comparação efetiva, com teste de segurança de penetração em aplicações *web*, de aplicações desenvolvidas com o método USASEC e sem o método; e
5. Aplicação do método USASEC em um projeto que utilize o desenvolvimento ágil, onde as equipes de usabilidade e segurança possam trabalhar juntos, com o método.

Referências

[1] KUROSE, J.; ROSS, K. **Computer networking**: a top-down approach featuring the internet. Boston, MA: Addison-Wesley Professional, 2002.

[2] PRESSMAN, R. S.; MAXIM, B. R. **Software engineering**: a practitioner's approach. 8th ed. New York: McGraw-Hill Education, 2015. v. 8, 933 p.

[3] FLECHAIS, I.; MASCOLO, C.; SASSE, M. A. Integrating security and usability into the requirements and design process. **International Journal of Electronic Security and Digital Forensics,** v. 1. n. 1, p. 12-26, 2007.

[4] GHERNAOUTI-HÉLIE, S. Going digital - rethinking cybersecurity and confidence in a connected world: a challenge for society. In: INTERNATIONAL CONFERENCE ON EMERGING SECURITY TECHNOLOGIES, 3., 2012, Lisbon. **Proceedings…** Psicataway: IEEE, 2012. p. 8-11.

[5] HUANG, Z.; BENYOUCEF, M. Usability and credibility of e-government websites. **Journal of Government Information Quarterly**, v. 31, n. 4, p. 584–595, Sept. 2014.

[6] STOLL, C. **The Cuckoo's Egg**: tracking a spy through the maze of computer espionage. New York: Pocket Books, 2005.

[7] OPEN WEB APPLICATION SEGURITY PROJECT. **OWASP Top 10-2013**: the ten most critical web application security risks: release. Maryland, 2013. Disponível em: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf . Acesso em: 10 abril de 2016.

[8] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes reportados ao CERT.br:** janeiro a dezembro de 2015. Brasília, 2016. Disponível em: < http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque.html>. Acesso em: 26 jun. 2016.

[9] SCHOLTE, T.; BALZAROTTI, D.; KIRDA, E. Have things changed now? An empirical study on input validation vulnerabilities in web applications. **Journal of Computers and Security**, v. 31, n. 3, p. 344–356, Dec. 2011.

[10] MORAES, M. Espionagem abre discussão sobre preparo do Brasil para uma guerra cibernética. **BBC Brasil**, São Paulo, out. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/10/131011 _defesa_ seguranca_cibernetica_brasil_mm>. Acesso em: 25 abr. 2017.

[11] MORGAN, S. Cybersecurity Market reaches $75 Billion in 2015. Expected to reach $170 Billion by 2020. **Forbes Technology**, Dec. 2015. Disponível em: < http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity-market-reaches-75-billion-in-2015-expected-to-reach-170-billion-by-2020/#1df890572191. Acesso em: 25 abr. 2017.

[12] HUGHES, B. B.; BOHL, D.; IRFAN, M.; MARGOLESE-MALIN, E.; SOLÓRZANO, J. R. ICT/Cyber benefits and costs: reconciling competing perspectives on the current

and future balance. **Journal of Technological Forecasting and Social Change**, v.115, n. 1, p. 117-130, Sept. 2016.

[13] BRASIL. Decreto Presidencial n° 6703, de 18 de dezembro de 2008. Cria a Política Nacional de Defesa e Estratégia Nacional de defesa. **Diário Oficial da União**. Brasilia, DF, 19 dez. 2008. p. 39-153.

[14] NURSE, J. R. C.; CREESE, S.; GOLDSMITH, M.; LAMBERTS, K. Trustworthy and effective communication of cybersecurity risks: a review. In: WORKSHOP ON SOCIO-TECHNICAL ASPECTS IN SECURITY AND TRUST, 2011, Milan. **Proceedings…** Psicataway: IEEE, 2011. p. 60–68.

[15] GARFINKEL, S.; SPAFFORD, G.; SCHWARTZ. A. **Practical UNIX and internet security**. 3rd ed. Sebastopol, CA: O'Reilly Media, 1996. 907 p.

[16] GABRIEL, I.; NYSHADHAM, E. A cognitive map of people's online risk perceptions and attitudes: an empirical study. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 41., 2008, Waikoloa, HI. **Proceedings…** Psicataway: IEEE, p. 274–283, 2008

[17] FARAHMAND, F.; ATALLAH, M.; KONSYNSKI, B. Incentives and perceptions of information security risks. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS (ICIS), 29., 2008, Paris. **Proceedings…** Atlanta: AIS, 2008. p. 25–41

[18] FARAHMAND, F.; DARK, M. ; LILES, S.; SORGE, B. Risk perceptions of information security: a measurement study. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND ENGINEERING, v. 3, 2009, Vancouver, BC. **Proceedings…** Psicataway: IEEE, 2009. p. 462–469.

[19] CHEN, L.; FARKAS, D. An investigation of decision-making and the tradeoffs involving computer security risk. In: AMERICAS CONFERENCE ON INFORMATION SYSTEMS (AMCIS), 5., 2009, San Francisco, CA. **Proceedings…** Atlanta: AIS, 2009. p. 610–618.

[20] WEST, J. R.; MAYHORN, C.; HARDEE, J.; MENDEL, J. The weakest link: a psychological perspective on why users make poor security decisions. In: GUPTA, M.; SHARMAN, R. **Social and human elements of information security:** emerging trends and countermeasures. Hershey, PA: IGI Global, 2009. cap. 4, p. 43–60.

[21] WEST, R. The psychology of security: why do good users make bad decisions? **Journal of Communications of the ACM**, v. 51, n. 4, p. 34–40, Apr. 2008.

[22] IBRAHIM, T.; FURNELL, S. M.; PAPADAKI, M.; CLARKE, N. L. Assessing the usability of end-user security software. In: KATSIKAS S.; LOPEZ J.; SORIANO M. (Eds). **TrustBus 2010**: trust, privacy and security in digital business. Berlin: Springer, 2010. p. 177–189. (Lecture Notes in Computer Science, v. 6264).

[23] BRAVO-LILLO, C.; CRANOR, L. F.; DOWNS, J.; KOMANDURI, S. Bridging the gap in computer security warnings: a mental model approach. **IEEE Security & Privacy**, v. 9, n. 2, p. 18–26, Dec. 2011.

[24] NURSE, J. R. C. Exploring the risks to identity security and privacy in cyberspace. **XRDS: Crossroads, The ACM Magazine for Students,** v. 21, n. 3, p. 42–47, 2015.

[25] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 12207:2009:** Engenharia de sistemas e software: processos de ciclo de vida de software. Rio de Janeiro, 2009.

[26] _____. **NBR 25030:2008:** Engenharia de software: Requisitos e Avaliação da Qualidade de Produto de Software (SQuaRE): requisitos de qualidade. Rio de Janeiro, 2008.

[27] COLUSSO, L. F.; CYBIS, A. T. P.; DANTAS, M. Segurança, usabilidade e interação. In: CONGRESSO SUL AMERICANO DE DESIGN DE INTERAÇÃO, 4., 2012, São paulo. **Anais…** São paulo: Blucher, 2012. p. 138–147, v. 1.

[28] JAYASWAL, B. K.; PATTON, P. C. **Design for trustworthy software tools techniques and methodology of developing robust software.** New York: Pearson Education, 2006. 840 p.

[29] KAINDA, R.; FLECHAIS, I.; ROSCOE, A. W. Security and usability: analysis and evaluation. In: INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY (ARE'S), 5., 2010, Krakow. **Proceedings…** Psicataway: IEEE, 2010. p. 275–282.

[30] PREECE, J.; ROGERS, Y.; SHARP, H. **Design de interação:** além da interação homem-computador. São Paulo: Bookmam, 2005. 600 p.

[31] SAATY, R. W. The analytic hierarchy process: what it is and how it is used. **Mathematical modelling**, v. 9, n. 3-5, p. 161–176, 1987.

[32] LOOTSMA, F. A.; MENSCH, T. C. A.; VOS, F. A. Multi-criteria analysis and budget reallocation in long-term research planning. **European Journal of Operational Research**, v. 47, n. 3, p. 293–305, Aug. 1990.

[33] LIU, X. F. Software quality function deployment. **IEEE Potentials,** v. 19, n. 5, p. 14–16, Jan. 2001.

[34] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 9126-1:2003:** Engenharia de software-Qualidade de produto. Rio de Janeiro, 2003.

[35] BRANDÃO, E. R. **Publicidade on-line, ergonomia e usabilidade:** o efeito de seis tipos de banner no processo humano de visualização do formato do anúncio na tela do computador e de lembrança da sua mensagem. 2006. 400 f. Dissertação (Mestrado em Design) - Pontifícia Universidade Católica, Rio de Janeiro.

[36] LOWDERMILK, T. **User-Centered Design:** a developer's guide to building user-friendly aplications. Sebastopol, CA: O' Reilly Media, 2013. 154 p.

[37] NIELSEN, J. **Usability engineering**. San Francisco, CA: Morgan Kaufmann, 1996, 362 p.

[38] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 9241-11:2013:** Guia

de especificações de usabilidade para interfaces web. Rio de Janeiro, 2013.

[39] NIELSEN, R. L.; MACK, J. **Usability inspection methods**. New York: Wiley & Sons, 1994. 448 p.

[40] NIELSEN, J. Usability engineering at a discount. In: INTERNACIONAL CONFERENCE ON HUMAN-COMPUTER INTERACTION ON DESIGNING AND USING HUMAN-COMPUTER INTERFACES AND KNOWLEDGE BASED SYSTEMS, 2., 1989, Boston, MA. **Proceedings…** New York: Elsevier Science, 1989. p. 394–401.

[41] BLACKMON, M. H.; POLSON, P. G.; KITAJIMA, M.; LEWIS, C. Cognitive walkthrough for the web. In: SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 2002, Minneapolis, MN. **Proceedings…** New York: ACM, 2002. p. 463–470.

[42] JEFFRIES, R.; MILLER, J. R.; WHARTON, C.; UYEDA, K. User interface evaluation in the real world: a comparison of four techniques. In: SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 1991, New Orleans. **Proceedings…** New York: ACM, 1991. p. 119–124.

[43] NIELSEN, J.; MOLICH, R. Heuristic evaluation of user interfaces. In: SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 1990, Seattle, WA. **Proceedings…** New York: ACM, 1990. p. 249–256.

[44] HOLLINGSED, D. G.; NOVICK, T. Usability Inspection methods after 15 years of research and practice. In: ANNUAL ACM INTERNATIONAL CONFERENCE ON DESIGN OF COMMUNICATION, 25., 2007, El Paso, TX. **Proceedings…** New York: ACM, 2007, p. 449–255.

[45] RUBIN, J.; CHISNELL, D. **Handbook of usability testing:** how to plan, design, and conduct effetive tests. 2nd ed. Indianapolis: John Wiley & Sons, 2008. 387 p.

[46] YEE, K.P. Guidelines and strategies for secure interaction design. In: CRANOR, L. F.; GARFINKEL, S. **Security and usability**: designing secure systems that people can use. Sebastopol, CA: O' Reilly Media, 2005. cap. 13. p. 253-280.

[47] _____. Aligning security and usability. **IEEE Security & Privacy**, v. 2, n. 5, p. 48-55, 2004.

[48] WHITTEN, A. **Making security usable**. 2004. 229 p. Thesis (PhD in Computer Science) - Carnegie Mellon University of the Princeton University, Pittsburgh, PA.

[49] NG, B. Y.; KANKANHALLI, A.; XU, Y. C. Studying user's computer security behavior: a health belief perspective. **Journal of Decision Support Systems**, v. 46, n. 4, p. 815–825, Mar. 2009.

[50] BRASIL. Ministério da Defesa. Estado-Maior Combinado das Forças Armadas. **Portaria Normativa nº 3.010/MD**, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014. Disponível em: < http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 25 de janeiro de 2017.

[51] WIERNER, N. **Cybernetics:** or the control and communication in the animal and the machine. Cambridge, MA: MIT, 1961. v. 25.

[52] OLIVEIRA, D. D. P. R. de. **Teoria geral da administração**: uma abordagem prática. São Paulo: Atlas, 2011. 464 p.

[53] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002:2013:** tecnologia da informação: técnicas de segurança: código de práticas para controles de segurança da informação. Rio de Janeiro, 2013.

[54] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 7498-2 **Information processing systems, open systems interconnection, basic reference model:** naming and addressing. Part 2: security architecture. Geneva, Switzerland, 1989.

[55] GHIYA, K. K.; TERRY BAHILL, A.; CHAPMAN, W. L. QFD: Validating robustness. **Journal of Quality Engineering**, v. 11, n. 4, p. 593–611, Oct. 2007.

[56] YILMAZ, M. R.; CHATTERJEE, S. Deming and the quality of software development. **Journal of Business Horizons,** v. 40, n. 6, p. 51–56, Dec. 1997.

[57] KING, R. Listening to the voice of the customer: using the quality function deployment system. **Global Business and Organizational Excellence,** v. 6, n. 3, p. 277–281, June 1987.

[58] AKAO, Y.; OHFUJI, T.; TOMOYOSHI, N. Surveys and reviews on quality function deployment in Japan. In: INTERNATIONAL CONFERENCE FOR QUALITY CONTROL, 1987, Tokyo. **Proceedings…** Tokyo: JUSE, 1987. p. 171–176.

[59] OHFUJI, T.; ONO, M.; AKAO, Y. **Método de desdobramento da qualidade: elaboração e exercício da matriz da qualidade**: elaboração e exercício da matriz da cualidade. Brasil: Fundação Christiano Ottoni, 1990.

[60] TUMELERO, N.; RIBEIRO, J. L. D.; DANILEVICZ, Â. D. M. F. Desdobramento da Função Qualidade (DFQ). In: CONGRESSO BRASILEIRO DE GESTÃO DE DESENVOLVIMENTO DE PRODUTO, 2., 2000, São Carlos. **Anais…** São Carlos: Universidade Federal de São Carlos, 2000. p. 226–249.

[61] EKDAHL, F.; GUSTAFSSON, A. QFD: the Swedish experience. In: SYMPOSIUM ON QUALITY FUNCTION DEPLOYMENT, 9., 1997, Novi, MI. **Proceedings…** [S.l.: s.n], 1997. p. 15-27.

[62] HAUSER, J. R.; CLAUSING, D. The house of quality. **Journal of Harvard Business Review**, v. 66, n. 3, p. 63-73, 1993.

[63] CARNEVALLI, J. A.; MIGUEL, P. A. C. Empresas de referência na utilização do desdobramento da função qualidade. **Revista Produto & Produção,** v. 10, n. 1, p. 1–18, fev. 2009.

[64] GRIFFIN, A. Evaluation QFD's use in firms as a process for developing products. **Journal of Product Innovation Management**, v. 9, n. 2, p. 177–187, Sept. 1992.

[65] HALOG, A.; SCHULTMANN, F.; RENTZ, O. Using quality function deployment for technique selection for optimum environmental performance improvement. **Journal of Cleaner Production**, v. 9, n. 5, p. 387–394, Oct. 2001.

[66] MASUI, K.; SAKAO, T.; KOBAYASHI, M.; INABA, A. Applying Quality Function Deployment to environmentally conscious design. **Journal of International Journal of Quality & Reliability Management,** v. 20, n.1, p. 90–106, 2003.

[67] RAHIMI, M.; WEIDNER, M. Integrating Design for Environment (DfE) Impact Matrix into Quality Function Deployment (QFD) Process. **The Journal of Sustainable Product Design**, v. 2, n. 1, p. 29-41, Mar. 2002.

[68] CHAO, L. P.; ISHII, K. Project quality function deployment. **International Journal of Quality & Reliability Management,** v. 21, n. 9, p. 938–958, 2004.

[69] LIN, S.; WEI, C. A Study on the linear programming in time cost analysis of product improve design- a focus on computer mouse products. **Journal of American Academy of Business**, v. 7, n. 2, p. 182–186, 2005.

[70] MARSOT, J. QFD: a methodological tool for integration of ergonomics at the design stage. **Applied Ergonomics**. v. 36, n. 2, p. 185–192, Mar. 2005.

[71] CAUCHICK, M. P. A. The state-of-the-art of the Brazilian QFD applications at the top 500 companies. **International Journal of Quality & Reliability Management**. v. 20, n. 1, p. 74–89, 2003.

[72] HSIAO, S. W.; LIU, E. A structural component-based approach for designing product family. **Computers in Industry,** v. 56, n. 1, p. 13–28, Jan. 2005.

[73] SANFORD, J. How useful is QFD. **Quality Progress**. v. 38, n. 1, p. 51–59, Jan. 2005.

[74] DELGADO, V. V.; DELGADO, N. G. G.; DEDINI, F. G. O QFD como ferramenta para aplicação do pensamento enxuto no processo de desenvolvimento de produtos. In: CONGRESSO NACIONAL DE ENGENHARIA MECÂNICA, 6., 2010, Campina Granda. **Anais…** New York: ABCM, 2010. p. 1-10.

[75] SONDA, F. A.; RIBEIRO, J. L. D.; ECHEVESTE, M. E. A aplicação do QFD no desenvolvimento de software: um estudo de caso. **Production**, v. 10, n. 1, p. 51-75, jun. 2000.

[76] ISLAM, R.; AHMED, M.; ALIAS, M. H.S. Application of Quality Function deployment in redesigning website: a case study on TV3. **International Journal of Business Information Systems,** v. 2, n. 2, p. 195-216, 2006.

[77] SUN, Y.; LIU, X. F. Business-oriented software process improvement based on CMMI using QFD. **Information and software technology**, v. 52, n. 1, p. 79-91, Jan. 2010.

[78] GENRO, P. J.; KIPPER, M. L. O uso do QFD como ferramenta para otimizar a usabilidade de produtos: um estudo exploratório. **Usabilidade em Sistemas Interativos e Organizacionais**, v. 1, n. 1, p. 24–26, set. 2015.

[79] MOUBACHIR, Y.; BOUAMI, D. A new approach for the transition between QFD

Phases. **Procedia CIRP**, v. 26, p. 82–86, Mar. 2015.

[80] ALNAHDI, A.; MELTON, A.; LIU, S. H. Web Service Description Quality Function Deployment (WSDQFD): systematic analytical approach. In: IEEE WORLD CONGRESS ON SERVICES, 2016, San Francisco, CA. **Proceedings…** Psicataway: IEEE, 2016. p. 132-133

[81] HAAG, S.; RAJA, M.; SCHKADE, L. L. Quality function deployment usage in software development. **Communications of the ACM,** v. 39, n. 1, p. 41-49, Jan. 1996.

[82] MIZUNO, S.; AKAO, Y. **Quality function deployment**: the customer-driven approach to quality planning and deployment. (Translated by Glenn H. Mazur) Tokyo: Asian Productivity Organization, 1994. p. 23.

[83] WATSON, G. H. **Design for Six Sigma**: innovation for enhanced competitiveness. Salem, NH: Goal/QPC, 2005.

[84] PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do Trabalho Científico:** métodos e técnicas da pesquisa e do trabalho acadêmico. 2 ed. Novo Hamburgo: Editora Feevale, 2013. 277 p.

[85] BOAVENTURA, E. M. **Metodologia de Pesquisa:** monografia, dissertação e Tese. Rio de Janeiro: Atlas 2004. 160 p.

[86] BARDlN, L. **Análise de Conteúdo**. Lisboa: Edições 70, 2011. 229 p. v. 70. Tradução de Luis Antero Reto e Augusto Pinheiro

[87] KAWAKITA, J. **The KJ Method:** seeking order out of chaos. Tokyo: Chuokoron-sha, 1986.

[88] GRIFFIN, A.; HAUSER, J. R. The voice of the customer. **Journal of Marketing Science**, v. 12, n. 1, p. 1-27, Feb. 1993.

[89] MEIRELES, M. A. C.; BONIFÁCIO, B. A.; KANDA, J. Y.; SILVA LEÃO, J. da. Integrando métodos de tomada de decisão no processo de elicitação de requisitos alternative title: integrating decision making methods on requerimentos elicitation process. In: BRAZILIAN SYMPOSIUM ON INFORMATION SYSTEMS, 12., 2016, Florianópolis. **Anais…** Florianópolis: IBD.DCC, 2016. p. 526–533.

[90] RODRIGUES, M. V. **Ações para a qualidade**. 5 ed. Rio de Janeiro: Elsevier, 2014. 392 p.

[91] NAGAMACHI, M. Kansei engineering as a powerful consumer-oriented technology for product development. **Journal of Applied ergonomics,** v. 33, n. 3, p. 289-294, May 2002.

[92] HOLTZBLATT, K.; WENDELL, J. B.; WOOD, S. Building an affinity diagram. In: _____. **Rapid contextual design:** a how-to guide to key techniques for user-centered design. San Francisco, CA: Morgan Kaufmann, 2004. cap. 8, p. 159–179.

[93] WIDJAJA, W.; YOSHII, K., HAGA, K.; TAKAHASHI, M. Discusys: multiple user real-time digital sticky-note affinity-diagram brainstorming system. **Procedia**

Computer Science, v. 22, p. 113–122, June 2013.

[94] AWASTHI, A.; CHAUHAN, S. S. A Hybrid approach integrating Affinity Diagram, AHP and fuzzy TOPSIS for sustainable city logistics planning. **Applied Mathematical Modelling,** v. 36, n. 2, p. 573–584, Feb. 2012.

[95] SAATY, T. L. Decision making for leaders. **IEEE Transactions on Systems, Man and Cybernetics,** n. 3, p. 450-452, May-June 1985.

[96] _____. How to make a decision: the analytic hierarchy process. **European Journal of Operational Research**, v. 48, n. 1, p. 9-26, Sept. 1990.

[97] _____. What is relative measurement? the ration Scale Phantom. **Mathematical and Computer Modelling**, v. 17, n. 4-5, p. 1-12, Mar. 1993.

[98] GOMES, L. F. A. M.; ARAYA, M. C. G.; CARIGNANO, C. **Tomada de decisão em cenários complexos:** introdução aos métodos discretos do apoio multicritério à decisão. São Paulo: Pioneira Thomson Learning, 2004. v. 107.

[99] SAATY, T. L.; GONZÁLEZ, L. **Prediction, proyection and forecasting:** applications of the analytic hierarchy process in economics, finance, politics, games and sports. New York: Springer Science, 1991.

[100] OLSON, D. L.; FLIEDNER, G.; CURRIE, K. Comparison of the REMBRANDT system with analytic hierarchy process. **European Journal of Operational Research**, v. 82, n. 3, p. 522-539, May 1995.

[101] MILLET, I.; HARKER, P. T. Globally effective questioningin the analytic hierarchy process. **European Journal of Operational Research,** v. 48, n. 1, p. 88-97, Sept. 1990.

[102] HARKER, P. T. Incomplete pairwise comparisons in the analytic hierarchy process. **Mathematical Modelling**, v. 9, n. 11, p. 837-848, Dec. 1987.

[103] WEISS, E. N.; RAO, V. R. AHP designissues for large-scale systems. **Decision Sciences**, v. 18, n. 1, p. 43-61, Jan. 1987.

[104] TOMA, T.; ASHARIF, M. R. **AHP coefficients optimization technique based on GA.** Okinawa: Department of Information Engineering of University of Ryukyus, 2003.

[105] OLIVEIRA, C. A. de; BELDERRAIN, M. C. N. Considerações sobre a obtenção de vetores de prioridade no AHP. In: ENCONTRO REGIONAL ARGENTINO BRASILEIRO DE PESQUISA OPERACIONAL, 1., 2008, Buenos Aires. **Anais...** São José dos Campos: ITA, 2008.

[106] VAN DEN HONERT, R. C. Decisional power in group decision making: a note on the allocation of group member's weight in the multiplicative AHP and SMART. **Group Decision and Negotiation**, v. 10, n. 3, p. 275-286, May 2001.

[107] DYER, R. F.; FORMAN, E. H. Group decision support with the Analytic Hierarchy Process. **Journal of Decision support systems,** v. 8, n. 2, p. 99-124, Apr. 1992.

[108] ACZÉL, J.; SAATY, T. L. Procedures for synthesizing ratio judgments. **Journal of mathematical Psychology**, v. 27, n. 1, p. 93-102, Mar. 1983.

[109] RAMANATHAN, R.; GANESH, L. S. Group preference aggregation methods employed in AHP: an evaluation and an intrinsic process for deriving members' weightages. **European Journal of Operational Research,** v. 79, n. 2, p. 249-265, Dec. 1994.

[110] VENEZIANI, A. C. **UX no processo de desenvolvimento de software**. [S.l.]: Usabilideiros, 2014. Disponível em: <http://www.usabilideiros.com.br/index.php/usabilidade/artigos /item/58-ux-no-processo-de-desenvolvimento-de-software>. Acesso em: 07 jan. 2017.

[111] FREITAS, A. L. P.; CORDEIRO, A. G. Priorização de requisitos para o desenvolvimento de software: uma abordagem multicritério utilizando o método AHP. **Produto & Produção**, v. 12, n. 2, p. 87-107, 2011.

[112] BRASIL. Ministério da Defesa. Comando de Aviação do Exército. Plano de Prevenção de Acidentes Aeronáuticos para o ano de 2016. Taubaté, 2016. (PPAA/CAvEx 2016).

Apêndice A – Questionário aberto do método USASEC

Este Apêndice apresenta o questionário aberto com questões sobre usabilidade e características da aplicação web, com base no questionário de [75], [84], [85] e [86], adaptado para a utilização em requisitos de usabilidade para aplicações web.

NOME DO RESPONDENTE: _____

E-MAIL: _____ TEL para Contato: _____

1) Qual a sua função na empresa?

( ) Diretor ( ) Gerente ( ) Supervisor ( ) Outros _____

2) Qual o nível de envolvimento que você possui com a aplicação?

( ) Proprietário ( ) Gerente ( ) Administrador ( ) Usuário Comum

( ) Outros: _____

3) Sua organização possui um sistema web de gerenciamento de investigação e prevenção de acidentes aeronáuticos?

( ) Sim ( ) Não

4) Se sim, quais as tarefas (entrada de dados, relatórios, solicitação de material e etc.) que você realiza neste sistema?

_____

_____

5) Quais características de usabilidade você identifica como sendo as mais importantes para a melhor utilização sistema?

_____

_____

6) Quais características de usabilidade você identifica como as mais deficientes na utilização do sistema?

_____

_____

7) Quais as melhorias no uso do software que poderiam ser adicionadas?

_____

_____

8) Quais as características de usabilidade que fariam você adquirir um software novo?

_____

_____

9) Quais tarefas que você realiza no sistema são as mais críticas, ou seja, aquelas que caso não fossem atendidas seria necessário a utilização de um novo sistema?

10) Qual a forma de divulgação do sistema que você acha mais eficiente?

11) Existe mais alguma característica que você acredita ser observada no sistema *web*?

Apêndice B – Formulário de priorização de requisitos

Este Apêndice apresenta o questionário de priorização de requisitos do processo de análise hierárquica (AHP) para o método USASEC. Este formulário tem por objetivo realizar o julgamento par a par de cada requisito. Comparações recíprocas par a par são usadas para expressar o grau de preferência de uma alternativa sobre outra em um determinado critério, correlacionando essa preferência em uma escala numérica, da qual o principal autovetor de prioridades é derivado e deve ser relacionado, também, entre os critérios, para os subcritérios entre os seus critérios "pai".

Formulário de Priorização dos Requisitos utilizando AHP

Nome: _____ **Data:** _____ **Função no Sistema:** _____

Critérios de usabilidade e alternativas de melhorias foram elencadas de acordo com as características do seu sistema e com o Diagrama de Afinidade confeccionado com sua colaboração. Agora, de sua opinião de quais delas são as mais importantes. Agradecemos sua contribuição.

1) Preencha os itens para indicar a intensidade da importância da primeira alternativa (X) em relação a segunda (Y) de acordo com determinado critério.

ALTERNATIVAS PAR A PAR		JULGAMENTO (INDIQUE A INTENSIDADE DA IMPORTÂNCAI)								
		X é amplamente menos desejável que Y = **(-8)**	X é muito menos desejável que Y = **(-6)**	X é menos desejável que Y = **(- 4)**	X é pouco menos desejável que Y = **(-2)**	X é indiferente a Y = **(1)**	X é pouco mais desejável que Y = **(2)**	X é mais desejável que Y = **(4)**	X é muito mais desejável que Y = **(6)**	X é amplamente mais desejável que Y = **(8)**
INTENSIDADE COM FOCO NO CRITÉRIO UTILIDADE (U)										
X. AI	Y. IMN									
X. AI	Y. CAD									

X. AI	Y. TAU									
X. AI	Y. DISMOV									
X. AI	Y. FU									
X. AI	Y. COAPL									
INTENSIDADE COM FOCO NO CRITÉRIO EFICÁCIA (EFK)										
X. AI	Y. IMN									
X. AI	Y. CAD									
X. AI	Y. TAU									
X. AI	Y. DISMOV									
X. AI	Y. FU									
X. AI	Y. COAPL									
X. AI	Y. DIV									
INTENSIDADE COM FOCO NO CRITÉRIO EFICIÊNCIA (EFI)										
X. AI	Y. IMN									
X. AI	Y. CAD									
ALTERNATIVAS PAR A PAR		JULGAMENTO (INDIQUE A INTENSIDADE DA IMPORTÂNCAI)								

		X é amplamente menos desejável que Y = **(-8)**	X é muito menos desejável que Y = **(-6)**	X é menos desejável que Y = **(- 4)**	X é pouco menos desejável que Y = **(-2)**	X é indiferente a Y = **(1)**	X é pouco mais desejável que Y = **(2)**	X é mais desejável que Y = **(4)**	X é muito mais desejável que Y = **(6)**	X é amplamente mais desejável que Y = **(8)**
X. AI	Y. TAU									
X. AI	Y. DISMOV									
X. AI	Y. FU									
X. AI	Y. COAPL									
X. AI	Y. DIV									
INTENSIDADE COM FOCO NO CRITÉRIO SEGURANÇA (S)										
X. AI	Y. IMN									
X. AI	Y. CAD									
X. AI	Y. TAU									
X. AI	Y. FU									
X. AI	Y. DIV									
INTENSIDADE COM FOCO NO CRITÉRIO APRENDIZAGEM (A)										

X. AI	Y. CAD									
X. AI	Y. TAU									
X. AI	Y. FU									
X. AI	Y. DIV									
INTENSIDADE COM FOCO NO CRITÉRIO MEMORIZAÇÃO (M)										
X. IMN	Y. TAU									
X. IMN	Y. FU									
X. IMN	Y. COAPL									
X. IMN	Y. DIV									
INTENSIDADE DOS CRITÉRIOS COM FOCO NA USABILIDADE (USA)										
X. U	Y. EFK									
X. U	Y. EFI									
X. U	Y. S									
X. U	Y. A									
ALTERNATIVAS PAR A PAR		JULGAMENTO (INDIQUE A INTENSIDADE DA IMPORTÂNCAI)								

		X é amplamente menos desejável que Y = **(-8)**	X é muito menos desejável que Y = **(-6)**	X é menos desejável que Y = **(- 4)**	X é pouco menos desejável que Y = **(-2)**	X é indiferente a Y = **(1)**	X é pouco mais desejável que Y = **(2)**	X é mais desejável que Y = **(4)**	X é muito mais desejável que Y = **(6)**	X é amplamente mais desejável que Y = **(8)**
X. U	Y. M									

ASSINATURA: _____

EMAIL: _____ TEL: _____

Apêndice C – Resultados das matrizes de normalização e consistência para os requisitos da aplicação SIGIPAAErEX.

Resultados para os membros da equipe multidisciplinar com a função de administrador do sistema, chamado administrador 1 e 2, para o analista de segurança, desenvolvedor e proprietário (diretor central do SIPAA do comando de aviação), respectivamente.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL			
1	AI	1,00	5,00000	1,00000	0,20000	1,00000	1,00000	3,00000			
2	IMN	0,20	1,00	0,20000	0,04000	0,20000	0,20000	1,66000			
3	CAD	1,00	5,00	1,00	0,20000	1,00000	1,00000	0,30000			
4	TAU	5,00	25,00	5,00	1,00	5,00000	5,00000	0,06000			
5	DISMOV	1,00	5,00	1,00	0,20	1,00	1,00000	0,30000			
6	FU	1,00	5,00	1,00	0,20	1,00	1,00	0,30000			
7	COAPL	0,33	1,60	0,33	0,07	0,33	0,33	1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	9,53	47,60	9,53	1,91	9,53	9,53	6,62			

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL				Weight
1	AI	0,10	0,11	0,10	0,10	0,10	0,10	0,45				**0,1547**
2	IMN	0,02	0,02	0,02	0,02	0,02	0,02	0,25				**0,0538**
3	CAD	0,10	0,11	0,10	0,10	0,10	0,10	0,05				**0,0964**
4	TAU	0,52	0,53	0,52	0,52	0,52	0,52	0,01				**0,4510**
5	DISMOV	0,10	0,11	0,10	0,10	0,10	0,10	0,05				**0,0964**
6	FU	0,10	0,11	0,10	0,10	0,10	0,10	0,05				**0,0964**
7	COAPL	0,03	0,03	0,03	0,04	0,03	0,03	0,15				**0,0512**
8												
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL				SUM	SUM/Weig
1	AI	0,15	0,27	0,10	0,09	0,10	0,10	0,15				0,96	6,19
2	IMN	0,03	0,05	0,02	0,02	0,02	0,02	0,08				0,25	4,56
3	CAD	0,15	0,27	0,10	0,09	0,10	0,10	0,02				0,82	8,49
4	TAU	0,77	1,35	0,48	0,45	0,48	0,48	0,00				4,02	8,91
5	DISMOV	0,15	0,27	0,10	0,09	0,10	0,10	0,02				0,82	8,49
6	FU	0,15	0,27	0,10	0,09	0,10	0,10	0,02				0,82	8,49
7	COAPL	0,05	0,09	0,03	0,03	0,03	0,03	0,05				0,20	3,89
8													
9													
10													

count	7,00
lambda max	7,003
CI	0,000
CR	**0,00**
constant	1,32

Figura 7. 1 – Julgamento dos requisitos do administrador 2 com foco na utilidade.

RC Value = 0,074 OK

MATRIX DE COMPARAÇÃO

Item Number	1	2	3	4	5	6	7	8	9	10
Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
AI	1,00	1,00000	3,0000	1,0000	1,00000	0,25000	5,00000	7,0000		
IMN	1,00	1,00	3,0000	1,0000	1,00000	0,25000	5,00000	7,0000		
CAD	0,33	0,33	1,00	0,3333	0,33330	0,08500	1,60000	2,3000		
TAU	1,00	1,00	3,00	1,00	1,00000	0,25000	5,00000	7,0000		
DISMOV	1,00	1,00	3,00	4,00	1,00	0,25000	5,00000	7,0000		
FU	4,00	4,00	12,00	4,00	4,00	1,00	20,00000	28,0000		
COAPL	0,20	0,20	0,63	0,20	0,20	0,05	1,00	1,4000		
DIV	0,14	0,14	0,42	0,14	0,14	0,03	0,71	1,00		
									1,00	
										1,00
Sum	8,67	8,68	26,05	11,67	8,67	2,17	43,31	60,70		

MATRIX NORMALIZADA

	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
AI	0,12	0,12	0,12	0,09	0,12	0,12	0,12	0,12			**0,1116**
IMN	0,12	0,12	0,12	0,09	0,12	0,12	0,12	0,12			**0,1116**
CAD	0,04	0,04	0,04	0,03	0,04	0,04	0,04	0,04			**0,0370**
TAU	0,12	0,12	0,12	0,09	0,12	0,12	0,12	0,12			**0,1116**
DISMOV	0,12	0,12	0,12	0,34	0,12	0,12	0,12	0,12			**0,1437**
FU	0,46	0,46	0,46	0,34	0,46	0,46	0,46	0,46			**0,4465**
COAPL	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			**0,0224**
DIV	0,02	0,02	0,02	0,01	0,02	0,01	0,02	0,02			**0,0154**

CI and CR Meta Utilidade

	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
AI	0,11	0,11	0,11	0,11	0,14	0,11	0,11	0,11			0,92	8,26
IMN	0,11	0,11	0,11	0,11	0,14	0,11	0,11	0,11			0,92	8,26
CAD	0,04	0,04	0,04	0,04	0,05	0,04	0,04	0,04			0,31	8,26
TAU	0,11	0,11	0,11	0,11	0,14	0,11	0,11	0,11			0,92	8,26
DISMOV	0,11	0,11	0,11	0,45	0,14	0,11	0,11	0,11			1,26	8,74
FU	0,45	0,45	0,44	0,45	0,57	0,45	0,45	0,43			3,69	8,26
COAPL	0,02	0,02	0,02	0,02	0,03	0,02	0,02	0,02			0,09	4,02
DIV	0,02	0,02	0,02	0,02	0,02	0,01	0,02	0,02			0,06	4,06

count	8,00
lambda max	7,264
CI	0,105
CR	**0,07**
constant	1,41

Figura 7. 2 – Julgamento dos requisitos do administrador 2 com foco na eficácia.

RC Value = 0,035 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	3,00000	0,33000	3,00000	1,00000	0,33000	7,00000	0,20000		
2	IMN	0,33	1,00	0,11000	1,00000	0,30000	0,11000	2,30000	0,06000		
3	CAD	3,00	9,00	1,00	9,00000	3,00000	1,00000	21,00000	0,60000		
4	TAU	0,33	1,00	0,11	1,00	0,30000	0,11000	2,30000	0,06000		
5	DISMOV	1,00	3,00	0,30	3,00	1,00	0,30000	7,00000	0,20000		
6	FU	3,00	9,00	1,00	9,00	3,00	1,00	21,00000	0,60000		
7	COAPL	0,14	0,43	0,05	0,43	0,14	0,05	1,00	0,03000		
8	DIV	5,00	15,00	1,60	15,00	5,00	1,60	45,00	1,00		
9										1,00	
10											1,00
	Sum	13,81	41,43	4,50	41,43	13,74	4,50	106,60	2,75		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,07	0,07	0,07	0,07	0,07	0,07	0,07	0,07			**0,0719**
2	IMN	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			**0,0233**
3	CAD	0,22	0,22	0,22	0,22	0,22	0,22	0,20	0,22			**0,2162**
4	TAU	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			**0,0233**
5	DISMOV	0,07	0,07	0,07	0,07	0,07	0,07	0,07	0,07			**0,0702**
6	FU	0,22	0,22	0,22	0,22	0,22	0,22	0,20	0,22			**0,2162**
7		0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			**0,0104**
8		0,36	0,36	0,36	0,36	0,36	0,36	0,42	0,36			**0,3684**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,07	0,07	0,07	0,07	0,07	0,07	0,07	0,07			0,57	7,94
2	IMN	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			0,19	7,94
3	CAD	0,22	0,21	0,22	0,21	0,21	0,22	0,22	0,22			1,72	7,94
4	TAU	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			0,19	7,94
5	DISMOV	0,07	0,07	0,06	0,07	0,07	0,06	0,07	0,07			0,56	7,95
6	FU	0,22	0,21	0,22	0,21	0,21	0,22	0,22	0,22			1,72	7,94
7	0	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			0,04	3,92
8	0	0,36	0,35	0,35	0,35	0,35	0,35	0,47	0,37			1,41	3,81
9													
10													

count	8,00
lambda max	6,925
CI	0,050
CR	**0,04**
constant	1,41

Figura 7. 3 – Julgamento dos requisitos do administrador 2 com foco na eficiência.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	FU	DIV				
1	AI	1,00	0,14000	1,00000	0,20000	0,14000	0,20000				
2	IMN	7,04	1,00	7,00000	1,40000	1,00000	1,40000				
3	CAD	1,00	0,14	1,00	0,20000	0,14000	0,20000				
4	TAU	5,00	0,71	5,00	1,00	0,72000	1,00000				
5	FU	7,04	1,00	7,00	1,40	1,00	1,45000				
6	DIV	5,00	0,72	5,00	1,00	0,72	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	26,08	3,72	26,00	5,20	3,72	5,25				

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	FU	DIV					Weight
1	AI	0,04	0,04	0,04	0,04	0,04	0,04					**0,0381**
2	IMN	0,27	0,27	0,27	0,27	0,27	0,27					**0,2688**
3	CAD	0,04	0,04	0,04	0,04	0,04	0,04					**0,0382**
4	TAU	0,19	0,19	0,19	0,19	0,19	0,19					**0,1921**
5	FU	0,27	0,27	0,27	0,27	0,27	0,28					**0,2704**
6	DIV	0,19	0,19	0,19	0,19	0,19	0,19					**0,1923**
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	FU	DIV					SUM	SUM/Weig
1	AI	0,04	0,04	0,04	0,04	0,04	0,04					0,23	6,00
2	IMN	0,27	0,27	0,27	0,27	0,27	0,27					1,61	6,00
3	CAD	0,04	0,04	0,04	0,04	0,04	0,04					0,23	6,00
4	TAU	0,19	0,19	0,19	0,19	0,19	0,19					1,15	6,00
5	FU	0,27	0,27	0,27	0,27	0,27	0,28					1,62	6,00
6	DIV	0,19	0,19	0,19	0,19	0,19	0,19					1,15	6,00
7													
8													
9													
10													

count	6,00
lambda max	6,002
CI	0,000
CR	**0,00**
constant	1,24

Figura 7. 4 – Julgamento dos requisitos do administrador 2 com foco na segurança.

RC Value = 0,000 Not OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	CAD	TAU	FU	DIV					
1	AI	1,00	0,20000	0,33300	0,14500	0,20000					
2	CAD	5,00	1,00	1,67000	0,72000	1,00000					
3	TAU	3,00	0,60	1,00	0,43000	0,60000					
4	FU	7,00	1,40	2,33	1,00	1,40000					
5	DIV	5,00	1,00	1,60	0,72	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	21,00	4,20	6,93	3,02	4,20					

MATRIX NORMALIZADA

		AI	CAD	TAU	FU	DIV						Weight
1	AI	0,05	0,05	0,05	0,05	0,05						**0,0478**
2	CAD	0,24	0,24	0,24	0,24	0,24						**0,2388**
3	TAU	0,14	0,14	0,14	0,14	0,14						**0,1431**
4	FU	0,33	0,33	0,34	0,33	0,33						**0,3335**
5	DIV	0,24	0,24	0,23	0,24	0,24						**0,2368**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	CAD	TAU	FU	DIV						SUM	SUM/Weig
1	AI	0,05	0,05	0,05	0,05	0,05						0,24	5,00
2	CAD	0,24	0,24	0,24	0,24	0,24						1,19	5,00
3	TAU	0,14	0,14	0,14	0,14	0,14						0,72	5,00
4	FU	0,33	0,33	0,33	0,33	0,33						1,67	5,00
5	DIV	0,24	0,24	0,23	0,24	0,24						1,18	5,00
6													
7													
8													
9													
10													

count	5,00
lambda max	4,998
CI	0,000
CR	**0,00**
constant	1,12

Figura 7. 5 – Julgamento dos requisitos do administrador 2 com foco na aprendizagem.

RC Value = 0,001 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	IMN	TAU	FU	COAPL	DIV					
1	IMN	1,00	0,20000	0,14000	1,00000	0,33000					
2	TAU	5,00	1,00	0,71000	5,00000	1,60000					
3	FU	7,14	1,41	1,00	7,00000	2,30000					
4	COAPL	1,00	0,20	0,15	1,00	0,33000					
5	DIV	3,00	0,63	0,43	3,00	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	17,14	3,43	2,43	17,00	5,56					

MATRIX NORMALIZADA

		IMN	TAU	FU	COAPL	DIV						Weight
1	IMN	0,06	0,06	0,06	0,06	0,06						**0,0585**
2	TAU	0,29	0,29	0,29	0,29	0,29						**0,2914**
3	FU	0,42	0,41	0,41	0,41	0,41						**0,4128**
4	COAPL	0,06	0,06	0,06	0,06	0,06						**0,0593**
5	DIV	0,18	0,18	0,18	0,18	0,18						**0,1781**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		IMN	TAU	FU	COAPL	DIV					SUM	SUM/Weig
1	IMN	0,06	0,06	0,06	0,06	0,06					0,29	5,00
2	TAU	0,29	0,29	0,29	0,30	0,28					1,46	5,00
3	FU	0,42	0,41	0,41	0,42	0,41					2,07	5,00
4	COAPL	0,06	0,06	0,06	0,06	0,06					0,30	5,00
5	DIV	0,18	0,18	0,18	0,18	0,18					0,89	5,00
6												
7												
8												
9												
10												

count	5,00
lambda max	5,004
CI	0,001
CR	**0,00**
constant	1,12

Figura 7. 6 – Julgamento dos requisitos do administrador 2 com foco na memorização.

RC Value = 0,011 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	D				
1	U	1,00	0,30000	0,20000	3,00000	5,00000	5,00000				
2	EFK	3,33	1,00	0,60000	9,00000	15,00000	15,00000				
3	EFI	5,00	1,67	1,00	15,00000	25,00000	25,00000				
4	S	0,33	0,11	0,07	1,00	1,60000	1,60000				
5	A	0,20	0,07	0,04	0,60	1,00	1,00000				
6	D	0,20	0,06	0,04	0,60	1,60	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	10,07	3,20	1,95	29,20	49,20	48,60				

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	D					Weight
1	U	0,10	0,09	0,10	0,10	0,10	0,10					**0,1005**
2	EFK	0,33	0,31	0,31	0,31	0,30	0,31					**0,3122**
3	EFI	0,50	0,52	0,51	0,51	0,51	0,51					**0,5111**
4	S	0,03	0,03	0,03	0,03	0,03	0,03					**0,0336**
5	A	0,02	0,02	0,02	0,02	0,02	0,02					**0,0204**
6	D	0,02	0,02	0,02	0,02	0,03	0,02					**0,0221**
7												
8												
9												
10												

CI and CR Meta Utilidade

		U	EFK	EFI	S	A	D					SUM	SUM/Weig
1	U	0,10	0,09	0,10	0,10	0,10	0,11					0,61	6,07
2	EFK	0,33	0,31	0,31	0,30	0,31	0,33					1,90	6,07
3	EFI	0,50	0,52	0,51	0,50	0,51	0,55					3,10	6,07
4	S	0,03	0,03	0,03	0,03	0,03	0,04					0,20	6,07
5	A	0,02	0,02	0,02	0,02	0,02	0,02					0,12	6,07
6	D	0,02	0,02	0,02	0,02	0,03	0,02					0,13	6,07
7													
8													
9													
10													

count	6,00
lambda max	6,070
CI	0,014
CR	**0,01**
constant	1,24

Figura 7. 7 – Julgamento dos critérios do administrador 2 com foco na usabilidade.

Valor de RC = 0,002 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL			
1	AI	1,00	7,00000	1,00000	0,33330	1,00000	0,20000	1,00000			
2	IMN	0,14	1,00	0,14000	0,04000	0,14000	0,02000	0,14000			
3	CAD	1,00	7,00	1,00	0,30000	1,00000	0,20000	1,00000			
4	TAU	3,00	21,00	6,33	1,00	3,00000	0,60000	3,00000			
5	DISMOV	1,00	7,00	1,00	1,33	1,00	0,20000	1,00000			
6	FU	5,00	35,00	5,00	1,67	5,00	1,00	5,00000			
7	COAPL	1,00	7,00	1,00	0,33	1,00	0,20	1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	12,14	85,00	15,47	5,01	12,14	2,42	12,14			

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL				Weight
1	AI	0,08	0,08	0,06	0,07	0,08	0,08	0,08				**0,0776**
2	IMN	0,01	0,01	0,01	0,01	0,01	0,01	0,01				**0,0103**
3	CAD	0,08	0,08	0,06	0,06	0,08	0,08	0,08				**0,0767**
4	TAU	0,25	0,25	0,41	0,20	0,25	0,25	0,25				**0,2636**
5	DISMOV	0,08	0,08	0,06	0,27	0,08	0,08	0,08				**0,1061**
6	FU	0,41	0,41	0,32	0,33	0,41	0,41	0,41				**0,3881**
7	COAPL	0,08	0,08	0,06	0,07	0,08	0,08	0,08				**0,0776**
8												
9												
10												

Tabela para Calculo do IC e CR

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL				SUM	SUM/Weig
1	AI	0,08	0,07	0,08	0,09	0,11	0,08	0,08				0,58	7,41
2	IMN	0,01	0,01	0,01	0,01	0,01	0,01	0,01				0,08	7,41
3	CAD	0,08	0,07	0,08	0,08	0,11	0,08	0,08				0,57	7,39
4	TAU	0,23	0,22	0,49	0,26	0,32	0,23	0,23				1,98	7,52
5	DISMOV	0,08	0,07	0,08	0,35	0,11	0,08	0,08				0,84	7,91
6	FU	0,39	0,36	0,38	0,44	0,53	0,39	0,39				2,88	7,41
7	COAPL	0,08	0,07	0,08	0,09	0,11	0,08	0,08				0,31	4,05
8													
9													
10													

count	7,00
lambda max	7,014
CI	0,002
CR	**0,00**
constant	1,32

Figura 7. 8 – Julgamento dos requisitos do administrador 1 com foco na utilidade.

RC Value = 0,077 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	1,00000	3,0000	1,0000	1,00000	0,25000	5,00000	0,1400		
2	IMN	1,00	1,00	3,0000	1,0000	1,00000	0,25000	5,00000	0,1400		
3	CAD	0,33	0,33	1,00	0,3333	0,33330	0,08500	1,60000	0,0400		
4	TAU	1,00	1,00	3,00	1,00	1,00000	0,25000	5,00000	0,1400		
5	DISMOV	1,00	1,00	3,00	4,00	1,00	0,25000	5,00000	0,1400		
6	FU	4,00	4,00	12,00	4,00	4,00	1,00	20,00000	0,5700		
7	COAPL	0,20	0,20	0,63	0,20	0,20	0,05	1,00	0,0200		
8	DIV	7,00	7,14	21,00	7,00	7,00	1,75	35,00	1,00		
9										1,00	
10											1,00
	Sum	15,53	15,68	46,63	18,53	15,53	3,89	77,60	2,19		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,06	0,06	0,06	0,05	0,06	0,06	0,06	0,06			**0,0629**
2	IMN	0,06	0,06	0,06	0,05	0,06	0,06	0,06	0,06			**0,0629**
3	CAD	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			**0,0205**
4	TAU	0,06	0,06	0,06	0,05	0,06	0,06	0,06	0,06			**0,0629**
5	DISMOV	0,06	0,06	0,06	0,22	0,06	0,06	0,06	0,06			**0,0832**
6	FU	0,26	0,26	0,26	0,22	0,26	0,26	0,26	0,26			**0,2523**
7	COAPL	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			**0,0122**
8	DIV	0,45	0,46	0,45	0,38	0,45	0,45	0,45	0,46			**0,4429**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,06	0,06	0,06	0,06	0,08	0,06	0,06	0,06			0,52	8,26
2	IMN	0,06	0,06	0,06	0,06	0,08	0,06	0,06	0,06			0,52	8,26
3	CAD	0,02	0,02	0,02	0,02	0,03	0,02	0,02	0,02			0,17	8,27
4	TAU	0,06	0,06	0,06	0,06	0,08	0,06	0,06	0,06			0,52	8,26
5	DISMOV	0,06	0,06	0,06	0,25	0,08	0,06	0,06	0,06			0,71	8,52
6	FU	0,25	0,25	0,25	0,25	0,33	0,25	0,24	0,25			2,08	8,26
7	COAPL	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01			0,05	4,15
8	DIV	0,44	0,45	0,43	0,44	0,58	0,44	0,43	0,44			1,76	3,98
9													
10													

count	8,00
lambda max	7,243
CI	0,108
CR	**0,08**
constant	1,41

Figura 7. 9 - Julgamento dos requisitos do administrador 1 com foco na eficácia.

RC Value = 0,006 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	1,00000	3,00000	1,00000	0,50000	1,00000	3,00000	1,00000		
2	IMN	1,00	1,00	3,00000	1,00000	0,50000	1,00000	3,00000	1,00000		
3	CAD	0,33	0,33	1,00	0,33000	0,16000	0,33000	1,00000	0,33000		
4	TAU	1,00	1,00	3,00	1,00	0,50000	1,00000	3,00000	1,00000		
5	DISMOV	2,00	2,00	6,25	2,00	1,00	2,00000	6,00000	2,00000		
6	FU	1,00	1,00	3,00	1,00	0,50	1,00	1,00000	1,00000		
7	COAPL	0,33	0,33	1,00	0,33	0,17	0,33	1,00	0,33000		
8	DIV	1,00	1,00	3,00	1,00	0,50	1,00	3,00	1,00		
9										1,00	
10											1,00
	Sum	7,66	7,67	23,25	7,66	3,83	7,66	21,00	7,66		

MATRIX NORMALIZADA

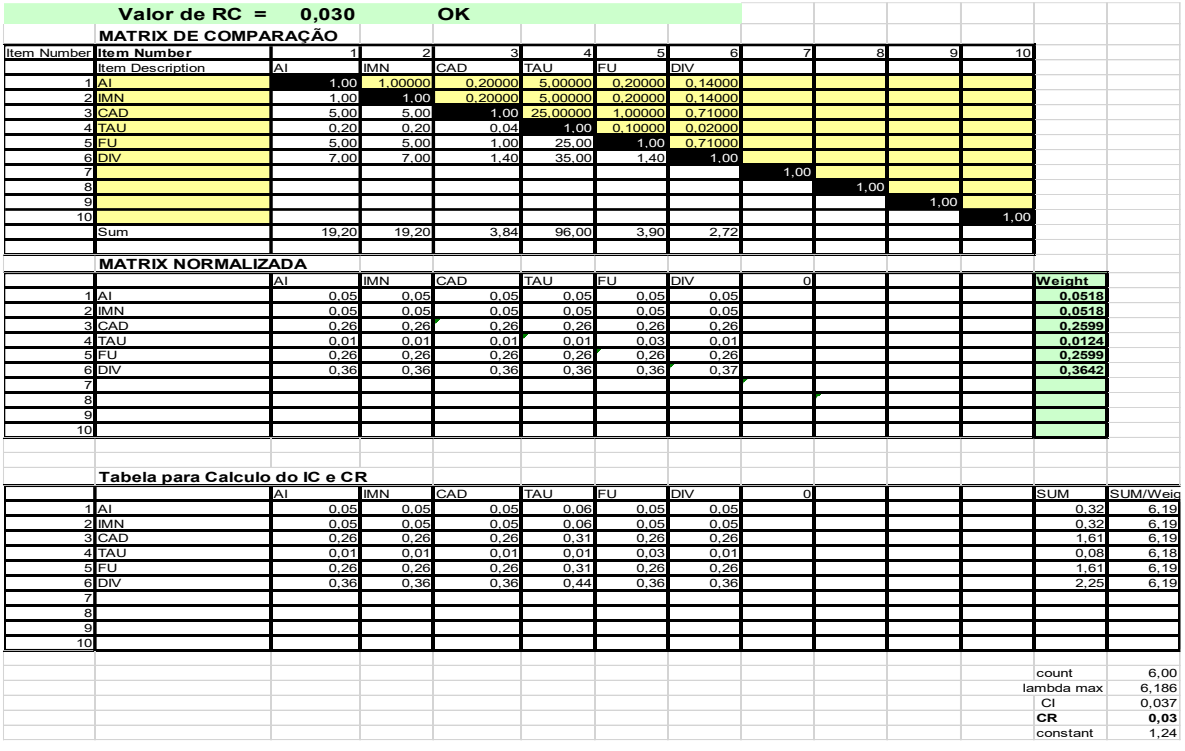
		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,13	0,13	0,13	0,13	0,13	0,13	0,14	0,13			**0,1319**
2	IMN	0,13	0,13	0,13	0,13	0,13	0,13	0,14	0,13			**0,1319**
3	CAD	0,04	0,04	0,04	0,04	0,04	0,04	0,05	0,04			**0,0436**
4	TAU	0,13	0,13	0,13	0,13	0,13	0,13	0,14	0,13			**0,1319**
5	DISMOV	0,26	0,26	0,27	0,26	0,26	0,26	0,29	0,26			**0,2651**
6	FU	0,13	0,13	0,13	0,13	0,13	0,13	0,05	0,13			**0,1200**
7	COAPL	0,04	0,04	0,04	0,04	0,04	0,04	0,05	0,04			**0,0438**
8	DIV	0,13	0,13	0,13	0,13	0,13	0,13	0,14	0,13			**0,1319**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,13	0,13	0,13	0,13	0,13	0,12	0,13	0,13			1,04	7,90
2	IMN	0,13	0,13	0,13	0,13	0,13	0,12	0,13	0,13			1,04	7,90
3	CAD	0,04	0,04	0,04	0,04	0,04	0,04	0,04	0,04			0,34	7,90
4	TAU	0,13	0,13	0,13	0,13	0,13	0,12	0,13	0,13			1,04	7,90
5	DISMOV	0,26	0,26	0,27	0,26	0,27	0,24	0,26	0,26			2,10	7,90
6	FU	0,13	0,13	0,13	0,13	0,13	0,12	0,04	0,13			0,95	7,96
7	COAPL	0,04	0,04	0,04	0,04	0,04	0,04	0,04	0,04			0,18	4,00
8	DIV	0,13	0,13	0,13	0,13	0,13	0,12	0,13	0,13			0,53	3,99
9													
10													

count	8,00
lambda max	6,932
CI	0,009
CR	**0,01**
constant	1,41

Figura 7. 10 – Julgamento dos requisitos do administrador 1 com foco na eficiência.



Valor de RC = 0,030 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	FU	DIV				
1	AI	1,00	1,00000	0,20000	5,00000	0,20000	0,14000				
2	IMN	1,00	1,00	0,20000	5,00000	0,20000	0,14000				
3	CAD	5,00	5,00	1,00	25,00000	1,00000	0,71000				
4	TAU	0,20	0,20	0,04	1,00	0,10000	0,02000				
5	FU	5,00	5,00	1,00	25,00	1,00	0,71000				
6	DIV	7,00	7,00	1,40	35,00	1,40	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	19,20	19,20	3,84	96,00	3,90	2,72				

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	FU	DIV	0				Weight
1	AI	0,05	0,05	0,05	0,05	0,05	0,05					**0,0518**
2	IMN	0,05	0,05	0,05	0,05	0,05	0,05					**0,0518**
3	CAD	0,26	0,26	0,26	0,26	0,26	0,26					**0,2599**
4	TAU	0,01	0,01	0,01	0,01	0,03	0,01					**0,0124**
5	FU	0,26	0,26	0,26	0,26	0,26	0,26					**0,2599**
6	DIV	0,36	0,36	0,36	0,36	0,36	0,37					**0,3642**
7												
8												
9												
10												

Tabela para Calculo do IC e CR

		AI	IMN	CAD	TAU	FU	DIV	0				SUM	SUM/Weig
1	AI	0,05	0,05	0,05	0,06	0,05	0,05					0,32	6,19
2	IMN	0,05	0,05	0,05	0,06	0,05	0,05					0,32	6,19
3	CAD	0,26	0,26	0,26	0,31	0,26	0,26					1,61	6,19
4	TAU	0,01	0,01	0,01	0,01	0,03	0,01					0,08	6,18
5	FU	0,26	0,26	0,26	0,31	0,26	0,26					1,61	6,19
6	DIV	0,36	0,36	0,36	0,44	0,36	0,36					2,25	6,19
7													
8													
9													
10													

count	6,00
lambda max	6,186
CI	0,037
CR	**0,03**
constant	1,24

Figura 7. 11 – Julgamento dos requisitos do administrador 1 com foco na segurança.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	CAD	TAU	FU	DIV					
1	AI	1,00	0,30000	1,00000	0,11000	0,14000					
2	CAD	3,33	1,00	3,00000	0,30000	0,44000					
3	TAU	1,00	0,33	1,00	0,11000	0,14000					
4	FU	9,09	3,33	9,09	1,00	1,28000					
5	DIV	7,0	2,27	7,14	0,78	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	21,45	7,24	21,23	2,30	3,00					

MATRIX NORMALIZADA

		AI	CAD	TAU	FU	DIV						Weight
1	AI	0,05	0,04	0,05	0,05	0,05						**0,0459**
2	CAD	0,16	0,14	0,14	0,13	0,15						**0,1424**
3	TAU	0,05	0,05	0,05	0,05	0,05						**0,0468**
4	FU	0,42	0,46	0,43	0,43	0,43						**0,4347**
5	DIV	0,33	0,31	0,34	0,34	0,33						**0,3302**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	CAD	TAU	FU	DIV						SUM	SUM/Weig
1	AI	0,05	0,04	0,05	0,05	0,05						0,23	5,00
2	CAD	0,15	0,14	0,14	0,13	0,15						0,71	5,00
3	TAU	0,05	0,05	0,05	0,05	0,05						0,23	5,00
4	FU	0,42	0,47	0,43	0,43	0,42						2,18	5,00
5	DIV	0,32	0,32	0,33	0,34	0,33						1,65	5,00
6													
7													
8													
9													
10													

count	5,00
lambda max	5,000
CI	0,000
CR	**0,00**
constant	1,12

Figura 7. 12–Julgamento dos requisitos do administrador 1 com foco na aprendizagem.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	IMN	TAU	FU	COAPL	DIV					
1	IMN	1,00	3,00000	0,20000	3,00000	3,00000					
2	TAU	0,33	1,00	0,06000	1,00000	1,00000					
3	FU	5,00	16,67	1,00	15,00000	15,00000					
4	COAPL	0,33	1,00	0,07	1,00	1,00000					
5	DIV	0,33	1,00	0,07	1,00	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	7,00	22,67	1,39	21,00	21,00					

MATRIX NORMALIZADA

		IMN	TAU	FU	COAPL	DIV						Weight
1	IMN	0,14	0,13	0,14	0,14	0,14						**0,1409**
2	TAU	0,05	0,04	0,04	0,05	0,05						**0,0460**
3	FU	0,71	0,74	0,72	0,71	0,71						**0,7192**
4	COAPL	0,05	0,04	0,05	0,05	0,05						**0,0470**
5	DIV	0,05	0,04	0,05	0,05	0,05						**0,0470**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		IMN	TAU	FU	COAPL	DIV						SUM	SUM/Weig
1	IMN	0,14	0,14	0,14	0,14	0,14						0,70	5,00
2	TAU	0,05	0,05	0,04	0,05	0,05						0,23	5,00
3	FU	0,70	0,77	0,72	0,70	0,70						3,60	5,00
4	COAPL	0,05	0,05	0,05	0,05	0,05						0,23	5,00
5	DIV	0,05	0,05	0,05	0,05	0,05						0,23	5,00
6													
7													
8													
9													
10													

count	5,00
lambda max	5,001
CI	0,000
CR	**0,00**
constant	1,12

Figura 7. 13– Julgamento dos requisitos do administrador 1 com foco na memorização.

Valor de RC = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	M				
1	U	1,00	1,00000	3,00000	3,00000	1,00000	1,00000				
2	EFK	1,00	1,00	3,00000	3,00000	1,00000	1,00000				
3	EFI	0,33	0,33	1,00	1,00000	0,30000	0,33300				
4	S	0,33	0,33	1,00	1,00	0,33330	0,33300				
5	A	1,00	1,00	3,33	3,00	1,00	1,00000				
6	M	1,00	1,00	3,00	3,00	1,00	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	4,67	4,67	14,34	14,00	4,63	4,67				

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	M	0				Weight
1	U	0,21	0,21	0,21	0,21	0,22	0,21					**21,4%**
2	EFK	0,21	0,21	0,21	0,21	0,22	0,21					**21,4%**
3	EFI	0,07	0,07	0,07	0,07	0,06	0,07					**7,0%**
4	S	0,07	0,07	0,07	0,07	0,07	0,07					**7,1%**
5	A	0,21	0,21	0,23	0,21	0,22	0,21					**21,8%**
6	M	0,21	0,21	0,21	0,21	0,22	0,21					**21,4%**
7												
8												
9												
10												

Tabela para Calculo do IC e CR

		U	EFK	EFI	S	A	M	0				SUM	SUM/Weig
1	U	0,21	0,21	0,21	0,21	0,22	0,21					1,28	6,00
2	EFK	0,21	0,21	0,21	0,21	0,22	0,21					1,28	6,00
3	EFI	0,07	0,07	0,07	0,07	0,07	0,07					0,42	6,00
4	S	0,07	0,07	0,07	0,07	0,07	0,07					0,43	6,00
5	A	0,21	0,21	0,23	0,21	0,22	0,21					1,31	6,00
6	M	0,21	0,21	0,21	0,21	0,22	0,21					1,28	6,00
7													
8													
9													
10													

count	6,00
lambda max	6,001
CI	0,000
CR	**0,00**
constant	1,24

Figura 7. 14 – Julgamento dos critérios do administrador 1 com foco na usabilidade.

RC Value = 0,024 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	D	F			
1	U	1,00	5,00000	5,00000	3,00000	1,00000	0,20000	1,00000			
2	EFK	0,20	1,00	1,00000	0,60000	0,20000	0,04000	0,20000			
3	EFI	0,20	1,00	1,00	0,60000	0,20000	0,04000	0,20000			
4	S	0,33	1,67	1,67	1,00	0,33000	0,06000	0,33000			
5	A	1,00	5,00	5,00	3,00	1,00	0,20000	1,00000			
6	D	5,00	25,00	25,00	20,00	5,00	1,00	5,00000			
7	F	5,00	5,00	5,00	3,00	1,00	0,20	1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	12,73	43,67	43,67	31,20	8,73	1,74	8,73			

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	D	F				Weight
1	U	0,08	0,11	0,11	0,10	0,11	0,11	0,11				**0,1068**
2	EFK	0,02	0,02	0,02	0,02	0,02	0,02	0,02				**0,0214**
3	EFI	0,02	0,02	0,02	0,02	0,02	0,02	0,02				**0,0214**
4	S	0,03	0,04	0,04	0,03	0,04	0,03	0,04				**0,0349**
5	A	0,08	0,11	0,11	0,10	0,11	0,11	0,11				**0,1068**
6	D	0,39	0,57	0,57	0,64	0,57	0,57	0,57				**0,5570**
7		0,39	0,11	0,11	0,10	0,11	0,11	0,11				**0,1517**
8												
9												
10												

CI and CR Meta Utilidade

		U	EFK	EFI	S	A	D	F				SUM	SUM/Weig
1	U	0,11	0,11	0,11	0,10	0,11	0,11	0,15				0,80	7,44
2	EFK	0,02	0,02	0,02	0,02	0,02	0,02	0,03				0,16	7,44
3	EFI	0,02	0,02	0,02	0,02	0,02	0,02	0,03				0,16	7,44
4	S	0,04	0,04	0,04	0,03	0,04	0,03	0,05				0,26	7,45
5	A	0,11	0,11	0,11	0,10	0,11	0,11	0,15				0,80	7,44
6	D	0,53	0,53	0,53	0,70	0,53	0,56	0,76				4,15	7,45
7	0	0,53	0,11	0,11	0,10	0,11	0,11	0,15				0,85	5,62
8	0												
9													
10													

count	7,00
lambda max	7,186
CI	0,031
CR	**0,02**
constant	1,32

Figura 7. 15 – Julgamento dos requisitos do analista com foco na utilidade.

RC Value = 0,088 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	3,00000	1,00000	0,33000	3,00000	1,00000	3,00000	5,00000		
2	IMN	0,33	1,00	0,33000	0,13000	1,00000	0,33000	1,00000	1,70000		
3	CAD	1,00	3,00	1,00	0,33000	3,00000	1,00000	3,00000	5,00000		
4	TAU	3,00	9,00	3,00	1,00	9,00000	3,00000	9,00000	15,00000		
5	DISMOV	0,33	1,00	0,30	0,13	1,00	0,33000	1,00000	1,70000		
6	FU	1,00	6,00	1,00	0,33	3,00	1,00	3,00000	5,00000		
7	COAPL	0,33	1,00	0,33	0,13	1,00	0,33	1,00	1,70000		
8	DIV	0,20	0,60	0,20	0,06	0,60	0,20	0,60	1,00		
9										1,00	
10											1,00
	Sum	7,20	24,60	7,16	2,44	21,60	7,19	21,60	36,10		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,14	0,12	0,14	0,14	0,14	0,14	0,14	0,14			**0,1364**
2	IMN	0,05	0,04	0,05	0,05	0,05	0,05	0,05	0,05			**0,0465**
3	CAD	0,14	0,12	0,14	0,14	0,14	0,14	0,14	0,14			**0,1364**
4	TAU	0,42	0,37	0,42	0,41	0,42	0,42	0,42	0,42			**0,4097**
5	DISMOV	0,05	0,04	0,04	0,05	0,05	0,05	0,05	0,05			**0,0460**
6	FU	0,14	0,24	0,14	0,14	0,14	0,14	0,14	0,14			**0,1516**
7		0,05	0,04	0,05	0,05	0,05	0,05	0,05	0,05			**0,0465**
8		0,03	0,02	0,03	0,02	0,03	0,03	0,03	0,03			**0,0270**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,14	0,14	0,14	0,14	0,14	0,15	0,14	0,13			1,11	8,15
2	IMN	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05			0,38	8,14
3	CAD	0,14	0,14	0,14	0,14	0,14	0,15	0,14	0,13			1,11	8,15
4	TAU	0,41	0,42	0,41	0,41	0,41	0,45	0,42	0,40			3,34	8,15
5	DISMOV	0,05	0,05	0,04	0,05	0,05	0,05	0,05	0,05			0,37	8,15
6	FU	0,14	0,28	0,14	0,14	0,14	0,15	0,14	0,13			1,25	8,25
7	0	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05			0,19	4,09
8	0	0,03	0,03	0,03	0,02	0,03	0,03	0,03	0,03			0,11	3,97
9													
10													

count	8,00
lambda max	7,130
CI	0,124
CR	**0,09**
constant	1,41

Figura 7. 16 – Julgamento dos requisitos do analista com foco na eficácia.

RC Value = 0,099 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	3,00000	0,33000	3,00000	1,00000	0,34000	7,00000	0,33000		
2	IMN	0,33	1,00	0,11000	1,00000	0,34000	0,11000	2,30000	0,11000		
3	CAD	3,00	9,00	1,00	9,00000	3,00000	1,00000	21,00000	1,00000		
4	TAU	0,33	1,00	0,11	1,00	0,34000	0,12000	2,30000	0,11000		
5	DISMOV	1,00	3,00	0,34	3,00	1,00	0,34000	7,00000	0,33000		
6	FU	3,00	9,00	1,00	9,00	3,00	1,00	21,00000	1,00000		
7	COAPL	0,14	0,43	0,05	0,43	0,14	0,05	1,00	0,05000		
8	DIV	3,00	9,00	1,00	9,00	3,00	1,00	21,00	1,00		
9										1,00	
10											1,00
	Sum	11,80	35,43	3,94	35,43	11,82	3,96	82,60	3,93		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,08	0,08	0,08	0,08	0,08	0,09	0,08	0,08			**0,0846**
2	IMN	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			**0,0281**
3	CAD	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25			**0,2539**
4	TAU	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			**0,0284**
5	DISMOV	0,08	0,08	0,09	0,08	0,08	0,09	0,08	0,08			**0,0849**
6	FU	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25			**0,2539**
7		0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			**0,0122**
8		0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25			**0,2539**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,08	0,08	0,08	0,09	0,08	0,09	0,09	0,08			0,68	8,02
2	IMN	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			0,23	8,02
3	CAD	0,25	0,25	0,25	0,26	0,25	0,25	0,26	0,25			2,04	8,02
4	TAU	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			0,23	8,02
5	DISMOV	0,08	0,08	0,09	0,09	0,08	0,09	0,09	0,08			0,68	8,02
6	FU	0,25	0,25	0,25	0,26	0,25	0,25	0,26	0,25			2,04	8,02
7	0	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			0,05	3,98
8	0	0,25	0,25	0,25	0,26	0,25	0,25	0,26	0,25			1,02	4,01
9													
10													

count	8,00
lambda max	7,011
CI	0,140
CR	**0,10**
constant	1,41

Figura 7. 17 – Julgamento dos requisitos do analista com foco na eficiência.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	FU	DIV				
1	AI	1,00	0,14000	0,20000	0,20000	0,14000	0,20000				
2	IMN	7,00	1,00	1,40000	1,40000	1,00000	1,40000				
3	CAD	5,00	0,71	1,00	1,00000	0,73000	1,00000				
4	TAU	5,00	0,71	1,00	1,00	0,73000	1,00000				
5	FU	7,00	1,00	1,40	1,40	1,00	1,40000				
6	DIV	5,00	0,72	1,00	1,00	0,71	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	30,00	4,29	6,00	6,00	4,31	6,00				

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	FU	DIV					Weight
1	AI	0,03	0,03	0,03	0,03	0,03	0,03					**0,0331**
2	IMN	0,23	0,23	0,23	0,23	0,23	0,23					**0,2331**
3	CAD	0,17	0,17	0,17	0,17	0,17	0,17					**0,1671**
4	TAU	0,17	0,17	0,17	0,17	0,17	0,17					**0,1671**
5	FU	0,23	0,23	0,23	0,23	0,23	0,23					**0,2331**
6	DIV	0,17	0,17	0,17	0,17	0,16	0,17					**0,1665**
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	FU	DIV					SUM	SUM/Weig
1	AI	0,03	0,03	0,03	0,03	0,03	0,03					0,20	6,00
2	IMN	0,23	0,23	0,23	0,23	0,23	0,23					1,40	6,00
3	CAD	0,17	0,17	0,17	0,17	0,17	0,17					1,00	6,00
4	TAU	0,17	0,17	0,17	0,17	0,17	0,17					1,00	6,00
5	FU	0,23	0,23	0,23	0,23	0,23	0,23					1,40	6,00
6	DIV	0,17	0,17	0,17	0,17	0,17	0,17					1,00	6,00
7	0												
8	0												
9													
10													

count	6,00
lambda max	6,001
CI	0,000
CR	**0,00**
constant	1,24

Figura 7. 18 – Julgamento dos requisitos do analista com foco na segurança.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	CAD	TAU	FU	DIV					
1	AI	1,00	3,00000	1,00000	1,00000	1,0000					
2	CAD	0,33	1,00	0,3333	0,3333	0,3333					
3	TAU	1,00	3,00	1,00	1,00000	1,0000					
4	FU	1,00	3,00	1,00	1,00	1,0000					
5	DIV	1,00	3,00	1,00	1,00	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	4,33	13,00	4,33	4,33	4,33					

MATRIX NORMALIZADA

		AI	CAD	TAU	FU	DIV						Weight
1	AI	0,23	0,23	0,23	0,23	0,23						**0,2308**
2	CAD	0,08	0,08	0,08	0,08	0,08						**0,0769**
3	TAU	0,23	0,23	0,23	0,23	0,23						**0,2308**
4	FU	0,23	0,23	0,23	0,23	0,23						**0,2308**
5	DIV	0,23	0,23	0,23	0,23	0,23						**0,2308**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	CAD	TAU	FU	DIV						SUM	SUM/Weig
1	AI	0,23	0,23	0,23	0,23	0,23						1,15	5,00
2	CAD	0,08	0,08	0,08	0,08	0,08						0,38	5,00
3	TAU	0,23	0,23	0,23	0,23	0,23						1,15	5,00
4	FU	0,23	0,23	0,23	0,23	0,23						1,15	5,00
5	DIV	0,23	0,23	0,23	0,23	0,23						1,15	5,00
6													
7	0												
8	0												
9													
10													

count	5,00
lambda max	5,000
CI	0,000
CR	**0,00**
constant	1,12

Figura 7. 19 – Julgamento dos requisitos do analista com foco na aprendizagem.

RC Value = 0,002 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	IMN	TAU	FU	COAPL	DIV					
1	IMN	1,00	5,00000	7,00000	5,00000	7,00000					
2	TAU	0,20	1,00	1,40000	1,00000	1,40000					
3	FU	0,15	0,71	1,00	0,71000	1,00000					
4	COAPL	0,20	1,00	1,41	1,00	1,40000					
5	DIV	0,14	0,71	1,00	0,71	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	1,69	8,43	11,81	8,42	11,80					

MATRIX NORMALIZADA

		IMN	TAU	FU	COAPL	DIV						Weight
1	IMN	0,59	0,59	0,59	0,59	0,59						**0,5928**
2	TAU	0,12	0,12	0,12	0,12	0,12						**0,1186**
3	FU	0,09	0,08	0,08	0,08	0,08						**0,0854**
4	COAPL	0,12	0,12	0,12	0,12	0,12						**0,1187**
5	DIV	0,08	0,08	0,08	0,08	0,08						**0,0846**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		IMN	TAU	FU	COAPL	DIV						SUM	SUM/Weig
1	IMN	0,59	0,59	0,60	0,59	0,59						2,97	5,01
2	TAU	0,12	0,12	0,12	0,12	0,12						0,59	5,01
3	FU	0,09	0,08	0,09	0,08	0,08						0,43	5,01
4	COAPL	0,12	0,12	0,12	0,12	0,12						0,59	5,01
5	DIV	0,08	0,08	0,09	0,08	0,08						0,42	5,01
6													
7	0												
8	0												
9													
10													

count	5,00
lambda max	5,009
CI	0,002
CR	**0,00**
constant	1,12

Figura 7. 20 – Julgamento dos requisitos do analista com foco na memorização.

RC Value = 0,026 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	M				
1	U	1,00	9,00000	7,00000	3,00000	3,00000	5,00000				
2	EFK	0,11	1,00	0,70000	0,30000	0,30000	0,55000				
3	EFI	0,14	1,43	1,00	0,42000	0,42000	0,71000				
4	S	0,33	3,33	2,38	1,00	1,00000	1,00000				
5	A	0,33	3,33	2,30	1,00	1,00	1,60000				
6	M	0,20	1,80	1,40	1,60	0,60	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	2,12	19,90	14,78	7,32	6,32	9,86				

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	M					Weight
1	U	0,47	0,45	0,47	0,41	0,47	0,51					**0,4649**
2	EFK	0,05	0,05	0,05	0,04	0,05	0,06					**0,0490**
3	EFI	0,07	0,07	0,07	0,06	0,07	0,07					**0,0671**
4	S	0,16	0,17	0,16	0,14	0,16	0,10					**0,1470**
5	A	0,16	0,17	0,16	0,14	0,16	0,16					**0,1562**
6	M	0,09	0,09	0,09	0,22	0,09	0,10					**0,1157**
7												
8												
9												
10												

CI and CR Meta Utilidade

		U	EFK	EFI	S	A	M					SUM	SUM/Weig
1	U	0,46	0,44	0,47	0,44	0,47	0,58					2,86	6,16
2	EFK	0,05	0,05	0,05	0,04	0,05	0,06					0,30	6,16
3	EFI	0,07	0,07	0,07	0,06	0,07	0,08					0,41	6,16
4	S	0,15	0,16	0,16	0,15	0,16	0,12					0,90	6,10
5	A	0,15	0,16	0,15	0,15	0,16	0,19					0,96	6,15
6	M	0,09	0,09	0,09	0,24	0,09	0,12					0,72	6,22
7	0												
8	0												
9													
10													

count	6,00
lambda max	6,160
CI	0,032
CR	**0,03**
constant	1,24

Figura 7. 21 – Julgamento dos critérios do analista com foco na usabilidade.

RC Value = 0,023 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	D	G			
1	U	1,00	5,00000	1,00000	9,00000	3,00000	5,00000	7,00000			
2	EFK	0,20	1,00	0,20000	1,80000	0,60000	1,00000	1,40000			
3	EFI	1,00	5,00	1,00	9,00000	3,00000	5,00000	7,00000			
4	S	0,12	0,56	0,12	1,00	1,00000	0,56000	0,77000			
5	A	0,33	1,67	0,34	3,00	1,00	1,60000	2,30000			
6	D	0,20	1,00	0,20	1,80	0,66	1,00	1,40000			
7	G	0,20	1,00	0,20	1,80	0,66	1,00	1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	3,05	15,22	3,06	27,40	9,92	15,16	20,87			

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	D	G				Weight
1	U	0,33	0,33	0,33	0,33	0,30	0,33	0,34				**0,3256**
2	EFK	0,07	0,07	0,07	0,07	0,06	0,07	0,07				**0,0651**
3	EFI	0,33	0,33	0,33	0,33	0,30	0,33	0,34				**0,3256**
4	S	0,04	0,04	0,04	0,04	0,10	0,04	0,04				**0,0466**
5	A	0,11	0,11	0,11	0,11	0,10	0,11	0,11				**0,1080**
6	D	0,07	0,07	0,07	0,07	0,07	0,07	0,07				**0,0660**
7	G	0,07	0,07	0,07	0,07	0,07	0,07	0,05				**0,0632**
8												
9												
10												

CI and CR Meta Utilidade

		U	EFK	EFI	S	A	D	G				SUM	SUM/Weig
1	U	0,33	0,33	0,33	0,42	0,32	0,33	0,44				2,49	7,66
2	EFK	0,07	0,07	0,07	0,08	0,06	0,07	0,09				0,50	7,66
3	EFI	0,33	0,33	0,33	0,42	0,32	0,33	0,44				2,49	7,66
4	S	0,04	0,04	0,04	0,05	0,11	0,04	0,05				0,35	7,61
5	A	0,11	0,11	0,11	0,14	0,11	0,11	0,15				0,83	7,65
6	D	0,07	0,07	0,07	0,08	0,07	0,07	0,09				0,50	7,65
7	G	0,07	0,07	0,07	0,08	0,07	0,07	0,06				0,28	4,42
8													
9													
10													

count	7,00
lambda max	7,186
CI	0,031
CR	**0,02**
constant	1,32

Figura 7. 22 – Julgamento dos requisitos do desenvolvedor com foco na utilidade.

RC Value = 0,008 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	1,00000	3,00000	1,00000	1,00000	0,25000	5,00000	0,14000		
2	IMN	1,00	1,00	3,00000	1,00000	1,00000	0,25000	5,00000	0,14000		
3	CAD	0,33	0,33	1,00	0,33330	0,33330	0,08000	1,60000	0,04000		
4	TAU	1,00	1,00	3,00	1,00	1,00000	0,25000	5,00000	0,14000		
5	DISMOV	1,00	1,00	3,00	1,00	1,00	0,25000	5,00000	0,14000		
6	FU	4,00	4,00	12,00	4,00	4,00	1,00	20,0000	0,57000		
7	COAPL	0,20	0,20	0,63	0,20	0,20	0,95	1,00	0,04000		
8	DIV	7,00	7,00	21,00	7,00	7,00	1,75	35,00	1,00		
9										1,00	
10											1,00
	Sum	15,53	15,53	46,63	15,53	15,53	4,78	77,60	2,21		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,06	0,06	0,06	0,06	0,06	0,05	0,06	0,06			**0,0627**
2	IMN	0,06	0,06	0,06	0,06	0,06	0,05	0,06	0,06			**0,0627**
3	CAD	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			**0,0203**
4	TAU	0,06	0,06	0,06	0,06	0,06	0,05	0,06	0,06			**0,0627**
5	DISMOV	0,06	0,06	0,06	0,06	0,06	0,05	0,06	0,06			**0,0627**
6	FU	0,26	0,26	0,26	0,26	0,26	0,21	0,26	0,26			**0,2515**
7	COAPL	0,01	0,01	0,01	0,01	0,01	0,20	0,01	0,02			**0,0368**
8	DIV	0,45	0,45	0,45	0,45	0,45	0,37	0,45	0,45			**0,4403**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,06	0,06	0,06	0,06	0,06	0,06	0,18	0,06			0,62	9,89
2	IMN	0,06	0,06	0,06	0,06	0,06	0,06	0,18	0,06			0,62	9,89
3	CAD	0,02	0,02	0,02	0,02	0,02	0,02	0,06	0,02			0,20	9,86
4	TAU	0,06	0,06	0,06	0,06	0,06	0,06	0,18	0,06			0,62	9,89
5	DISMOV	0,06	0,06	0,06	0,06	0,06	0,06	0,18	0,06			0,62	9,89
6	FU	0,25	0,25	0,24	0,25	0,25	0,25	0,74	0,25			2,49	9,89
7	COAPL	0,01	0,01	0,01	0,01	0,01	0,24	0,04	0,02			0,05	1,37
8	DIV	0,44	0,44	0,43	0,44	0,44	0,44	1,29	0,44			1,74	3,96
9													
10													

count	8,00
lambda max	8,081
CI	0,012
CR	**0,01**
constant	1,41

Figura 7. 23 – Julgamento dos requisitos do desenvolvedor com foco na eficácia.

RC Value = 0,100 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	3,000	0,333	3,00	1,00	0,33	7,00	0,33		
2	IMN	0,33	1,00	0,110	1,00	0,30	0,12	2,34	0,11		
3	CAD	3,00	9,00	1,00	9,00	3,00	1,00	21,00	1,00		
4	TAU	0,33	1,00	0,12	1,00	0,33	0,12	2,35	0,11		
5	DISMOV	1,00	3,00	0,33	3,00	1,00	0,33	7,00	0,33		
6	FU	3,00	9,00	1,00	9,00	3,00	1,00	21,00	1,00		
7	COAPL	0,14	0,43	0,05	0,43	0,14	0,05	1,00	0,04		
8	DIV	3,00	9,00	1,00	9,00	3,00	1,00	21,00	1,00		
9										1,00	
10											1,00
	Sum	11,81	35,43	3,94	35,43	11,78	3,95	82,69	3,93		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08			**0,0846**
2	IMN	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			**0,0281**
3	CAD	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25			**0,2541**
4	TAU	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			**0,0288**
5	DISMOV	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08			**0,0846**
6	FU	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25			**0,2541**
7		0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			**0,0118**
8		0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25			**0,2541**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,08	0,08	0,08	0,09	0,08	0,08	0,08	0,08			0,68	7,99
2	IMN	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			0,22	7,99
3	CAD	0,25	0,25	0,25	0,26	0,25	0,25	0,25	0,25			2,03	7,99
4	TAU	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03			0,23	7,99
5	DISMOV	0,08	0,08	0,08	0,09	0,08	0,08	0,08	0,08			0,68	7,99
6	FU	0,25	0,25	0,25	0,26	0,25	0,25	0,25	0,25			2,03	7,99
7	0	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			0,05	4,08
8	0	0,25	0,25	0,25	0,26	0,25	0,25	0,25	0,25			1,02	4,01
9													
10													

count	8,00
lambda max	7,003
CI	0,141
CR	**0,10**
constant	1,41

Figura 7. 24 – Julgamento dos requisitos do desenvolvedor com foco na eficiência.

RC Value = 0,008 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	FU	DIV				
1	AI	1,00	0,11000	9,00000	1,00000	1,00000	0,20000				
2	IMN	9,00	1,00	81,00000	9,00000	9,00000	1,80000				
3	CAD	0,12	0,01	1,00	0,12000	0,12000	0,02000				
4	TAU	1,00	0,12	9,00	1,00	1,00000	0,20000				
5	FU	1,00	0,12	9,00	1,00	1,00	0,20000				
6	DIV	5,00	0,56	45,00	5,00	5,00	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	17,12	1,92	154,00	17,12	17,12	3,42				

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	FU	DIV					Weight
1	AI	0,06	0,06	0,06	0,06	0,06	0,06					**0,0582**
2	IMN	0,53	0,52	0,53	0,53	0,53	0,53					**0,5249**
3	CAD	0,01	0,01	0,01	0,01	0,01	0,01					**0,0066**
4	TAU	0,06	0,06	0,06	0,06	0,06	0,06					**0,0591**
5	FU	0,06	0,06	0,06	0,06	0,06	0,06					**0,0591**
6	DIV	0,29	0,29	0,29	0,29	0,29	0,29					**0,2920**
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	FU	DIV					SUM	SUM/Weig
1	AI	0,06	0,06	0,06	0,06	0,06	0,06					0,35	6,05
2	IMN	0,52	0,52	0,54	0,53	0,53	0,53					3,18	6,05
3	CAD	0,01	0,01	0,01	0,01	0,01	0,01					0,04	6,05
4	TAU	0,06	0,06	0,06	0,06	0,06	0,06					0,36	6,05
5	FU	0,06	0,06	0,06	0,06	0,06	0,06					0,36	6,05
6	DIV	0,29	0,29	0,30	0,30	0,30	0,29					1,77	6,05
7													
8													
9													
10													

count	6,00
lambda max	6,050
CI	0,010
CR	**0,01**
constant	1,24

Figura 7. 25 – Julgamento dos requisitos do desenvolvedor com foco na segurança.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	CAD	TAU	FU	DIV					
1	AI	1,00	0,11000	0,14000	0,20000	0,11000					
2	CAD	9,09	1,00	1,28000	1,80000	1,00000					
3	TAU	7,14	0,78	1,00	1,41000	0,78000					
4	FU	5,00	0,56	0,71	1,00	0,56000					
5	DIV	9,09	1,00	1,28	1,80	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	31,32	3,45	4,41	6,21	3,45					

MATRIX NORMALIZADA

		AI	CAD	TAU	FU	DIV						Weight
1	AI	0,03	0,03	0,03	0,03	0,03						**0,0319**
2	CAD	0,29	0,29	0,29	0,29	0,29						**0,2901**
3	TAU	0,23	0,23	0,23	0,23	0,23						**0,2269**
4	FU	0,16	0,16	0,16	0,16	0,16						**0,1610**
5	DIV	0,29	0,29	0,29	0,29	0,29						**0,2901**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	CAD	TAU	FU	DIV						SUM	SUM/Weig
1	AI	0,03	0,03	0,03	0,03	0,03						0,16	5,00
2	CAD	0,29	0,29	0,29	0,29	0,29						1,45	5,00
3	TAU	0,23	0,23	0,23	0,23	0,23						1,13	5,00
4	FU	0,16	0,16	0,16	0,16	0,16						0,81	5,00
5	DIV	0,29	0,29	0,29	0,29	0,29						1,45	5,00
6													
7													
8													
9													
10													

count	5,00
lambda max	5,002
CI	0,000
CR	**0,00**
constant	1,12

Figura 7. 26–Julgamento dos requisitos do desenvolvedor com foco na aprendizagem.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	IMN	TAU	FU	COAPL	DIV					
1	IMN	1,00	1,00000	0,3333	7,00000	0,20000					
2	TAU	1,00	1,00	0,3333	7,00000	0,20000					
3	FU	3,00	3,00	1,00	21,00000	0,60000					
4	COAPL	0,14	0,14	0,05	1,00	0,03000					
5	DIV	5,00	5,00	1,60	35,00	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	10,14	10,14	3,31	71,00	2,03					

MATRIX NORMALIZADA

		IMN	TAU	FU	COAPL	DIV						Weight
1	IMN	0,10	0,10	0,10	0,10	0,10						**0,0990**
2	TAU	0,10	0,10	0,10	0,10	0,10						**0,0990**
3	FU	0,30	0,30	0,30	0,30	0,30						**0,2969**
4	COAPL	0,01	0,01	0,01	0,01	0,01						**0,0143**
5	DIV	0,49	0,49	0,48	0,49	0,49						**0,4909**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		IMN	TAU	FU	COAPL	DIV						SUM	SUM/Weig
1	IMN	0,10	0,10	0,10	0,10	0,10						0,50	5,00
2	TAU	0,10	0,10	0,10	0,10	0,10						0,50	5,00
3	FU	0,30	0,30	0,30	0,30	0,29						1,49	5,00
4	COAPL	0,01	0,01	0,01	0,01	0,01						0,07	5,00
5	DIV	0,49	0,49	0,48	0,50	0,49						2,46	5,00
6													
7													
8													
9													
10													

count	5,00
lambda max	5,002
CI	0,000
CR	**0,00**
constant	1,12

Figura 7. 27– Julgamento dos requisitos do desenvolvedor com foco na memorização.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	M				
1	U	1,00	7,00000	7,00000	0,14000	1,00000	9,00000				
2	EFK	0,15	1,00	1,00000	0,02000	0,15000	1,29000				
3	EFI	0,15	1,00	1,00	0,02000	0,15000	1,29000				
4	S	7,14	50,00	50,00	1,00	7,00000	63,00000				
5	A	1,00	6,67	7,00	0,15	1,00	9,00000				
6	M	0,12	0,78	0,78	0,01	0,12	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	9,56	66,45	66,78	1,34	9,42	84,58				

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	M					Weight
1	U	0,10	0,11	0,10	0,10	0,11	0,11					**0,1053**
2	EFK	0,02	0,02	0,01	0,01	0,02	0,02					**0,0153**
3	EFI	0,02	0,02	0,01	0,01	0,02	0,02					**0,0153**
4	S	0,75	0,75	0,75	0,75	0,74	0,74					**0,7471**
5	A	0,10	0,10	0,10	0,11	0,11	0,11					**0,1057**
6	M	0,01	0,01	0,01	0,01	0,01	0,01					**0,0113**
7												
8												
9												
10												

CI and CR Meta Utilidade

		U	EFK	EFI	S	A	M					SUM	SUM/Weig
1	U	0,11	0,11	0,11	0,10	0,11	0,10					0,63	6,00
2	EFK	0,02	0,02	0,02	0,01	0,02	0,01					0,09	6,00
3	EFI	0,02	0,02	0,02	0,01	0,02	0,01					0,09	6,00
4	S	0,75	0,77	0,77	0,75	0,74	0,71					4,48	6,00
5	A	0,11	0,10	0,11	0,11	0,11	0,10					0,63	6,00
6	M	0,01	0,01	0,01	0,01	0,01	0,01					0,07	6,00
7													
8													
9													
10													

count	6,00
lambda max	6,000
CI	0,000
CR	**0,00**
constant	1,24

Figura 7. 28 – Julgamento dos critérios do desenvolvedor com foco na usabilidade.

RC Value = 0,010 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL			
1	AI	1,00	1,00000	0,20000	5,00000	0,20000	0,14000	3,00000			
2	IMN	1,00	1,00	0,20000	5,00000	0,20000	0,14000	3,00000			
3	CAD	5,00	5,00	1,00	25,00000	1,00000	0,70000	15,00000			
4	TAU	0,20	0,20	0,04	1,00	0,04000	0,02000	0,60000			
5	DISMOV	5,00	5,00	1,00	25,00	1,00	0,70000	15,00000			
6	FU	7,00	7,00	1,40	35,00	1,40	1,00	21,00000			
7	COAPL	0,33	0,33	0,06	8,00	0,06	0,04	1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	19,53	19,53	3,90	104,00	3,90	2,74	58,60			

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL				Weight
1	AI	0,05	0,05	0,05	0,05	0,05	0,05	0,05				**0,0508**
2	IMN	0,05	0,05	0,05	0,05	0,05	0,05	0,05				**0,0508**
3	CAD	0,26	0,26	0,26	0,24	0,26	0,26	0,26				**0,2538**
4	TAU	0,01	0,01	0,01	0,01	0,01	0,01	0,01				**0,0097**
5	DISMOV	0,26	0,26	0,26	0,24	0,26	0,26	0,26				**0,2538**
6	FU	0,36	0,36	0,36	0,34	0,36	0,36	0,36				**0,3564**
7	COAPL	0,02	0,02	0,02	0,08	0,02	0,01	0,02				**0,0247**
8												
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL				SUM	SUM/Weig
1	AI	0,05	0,05	0,05	0,05	0,05	0,05	0,07				0,38	7,40
2	IMN	0,05	0,05	0,05	0,05	0,05	0,05	0,07				0,38	7,40
3	CAD	0,25	0,25	0,25	0,24	0,25	0,25	0,37				1,88	7,40
4	TAU	0,01	0,01	0,01	0,01	0,01	0,01	0,01				0,07	7,43
5	DISMOV	0,25	0,25	0,25	0,24	0,25	0,25	0,37				1,88	7,40
6	FU	0,36	0,36	0,36	0,34	0,36	0,36	0,52				2,64	7,40
7	COAPL	0,02	0,02	0,02	0,08	0,02	0,01	0,02				0,13	5,12
8													
9													
10													

count	7,00
lambda max	7,080
CI	0,013
CR	**0,01**
constant	1,32

Figura 7. 29 – Julgamento dos requisitos do proprietário com foco na utilidade.

RC Value = 0,013 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	0,50000	1,00000	5,00000	0,50000	1,00000	0,33000	0,33000		
2	IMN	2,00	1,00	2,00000	10,00000	1,00000	2,00000	0,60000	0,60000		
3	CAD	1,00	0,50	1,00	5,00000	0,50000	1,00000	0,33000	0,33000		
4	TAU	0,20	0,10	0,20	1,00	0,10000	0,20000	0,06000	0,06000		
5	DISMOV	2,00	1,00	2,00	10,00	1,00	2,00000	0,60000	0,60000		
6	FU	1,00	0,50	1,00	5,00	0,50	1,00	1,00000	0,33000		
7	COAPL	3,00	1,50	3,00	15,00	1,50	3,00	1,00	1,00000		
8	DIV	3,00	1,50	3,00	15,00	1,50	3,00	1,00	1,00		
9										1,00	
10											1,00
	Sum	13,20	6,60	13,20	66,00	6,60	13,20	4,92	4,25		

MATRIX NORMALIZADA

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,08	0,08	0,08	0,08	0,08	0,08	0,07	0,08			**0,0749**
2	IMN	0,15	0,15	0,15	0,15	0,15	0,15	0,12	0,14			**0,1465**
3	CAD	0,08	0,08	0,08	0,08	0,08	0,08	0,07	0,08			**0,0749**
4	TAU	0,02	0,02	0,02	0,02	0,02	0,02	0,01	0,01			**0,0147**
5	DISMOV	0,15	0,15	0,15	0,15	0,15	0,15	0,12	0,14			**0,1465**
6	FU	0,08	0,08	0,08	0,08	0,08	0,08	0,20	0,08			**0,0919**
7	COAPL	0,23	0,23	0,23	0,23	0,23	0,23	0,20	0,24			**0,2253**
8	DIV	0,23	0,23	0,23	0,23	0,23	0,23	0,20	0,24			**0,2253**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,07	0,07	0,07	0,07	0,07	0,09	0,07	0,07			0,61	8,15
2	IMN	0,15	0,15	0,15	0,15	0,15	0,18	0,14	0,14			1,19	8,14
3	CAD	0,07	0,07	0,07	0,07	0,07	0,09	0,07	0,07			0,61	8,15
4	TAU	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01			0,12	8,14
5	DISMOV	0,15	0,15	0,15	0,15	0,15	0,18	0,14	0,14			1,19	8,14
6	FU	0,07	0,07	0,07	0,07	0,07	0,09	0,23	0,07			0,76	8,28
7	COAPL	0,22	0,22	0,22	0,22	0,22	0,28	0,23	0,23			0,89	3,95
8	DIV	0,22	0,22	0,22	0,22	0,22	0,28	0,23	0,23			0,89	3,95
9													
10													

count	8,00
lambda max	7,112
CI	0,019
CR	**0,01**
constant	1,41

Figura 7. 30 – Julgamento dos requisitos do proprietário com foco na eficácia.

RC Value = 0,077 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV		
1	AI	1,00	1,00000	3,0000	1,0000	1,00000	0,25000	5,00000	0,1400		
2	IMN	1,00	1,00	3,0000	1,0000	1,00000	0,25000	5,00000	0,1400		
3	CAD	0,33	0,33	1,00	0,3333	0,33330	0,08500	1,60000	0,0400		
4	TAU	1,00	1,00	3,00	1,00	1,00000	0,25000	5,00000	0,1400		
5	DISMOV	1,00	1,00	3,00	4,00	1,00	0,25000	5,00000	0,1400		
6	FU	4,00	4,00	12,00	4,00	4,00	1,00	20,00000	0,5700		
7	COAPL	0,20	0,20	0,63	0,20	0,20	0,05	1,00	0,0300		
8	DIV	7,00	7,14	21,00	7,00	7,00	1,75	35,00	1,00		
9										1,00	
10											1,00
	Sum	15,53	15,68	46,63	18,53	15,53	3,89	77,60	2,20		

MATRIX NORMALIZADA

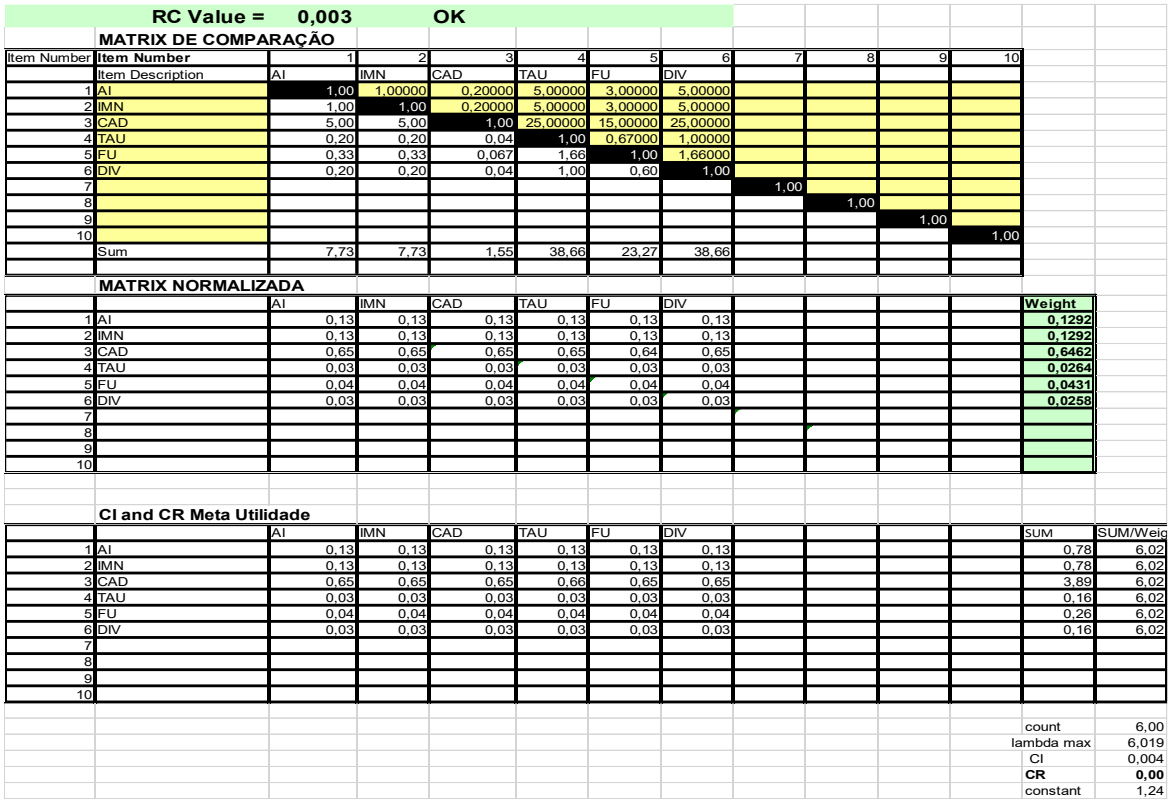
		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			Weight
1	AI	0,06	0,06	0,06	0,05	0,06	0,06	0,06	0,06			**0,0629**
2	IMN	0,06	0,06	0,06	0,05	0,06	0,06	0,06	0,06			**0,0629**
3	CAD	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02			**0,0205**
4	TAU	0,06	0,06	0,06	0,05	0,06	0,06	0,06	0,06			**0,0629**
5	DISMOV	0,06	0,06	0,06	0,22	0,06	0,06	0,06	0,06			**0,0831**
6	FU	0,26	0,26	0,26	0,22	0,26	0,26	0,26	0,26			**0,2522**
7	COAPL	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01			**0,0128**
8	DIV	0,45	0,46	0,45	0,38	0,45	0,45	0,45	0,45			**0,4426**
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV			SUM	SUM/Weig
1	AI	0,06	0,06	0,06	0,06	0,08	0,06	0,06	0,06			0,52	8,30
2	IMN	0,06	0,06	0,06	0,06	0,08	0,06	0,06	0,06			0,52	8,30
3	CAD	0,02	0,02	0,02	0,02	0,03	0,02	0,02	0,02			0,17	8,31
4	TAU	0,06	0,06	0,06	0,06	0,08	0,06	0,06	0,06			0,52	8,30
5	DISMOV	0,06	0,06	0,06	0,25	0,08	0,06	0,06	0,06			0,71	8,55
6	FU	0,25	0,25	0,25	0,25	0,33	0,25	0,26	0,25			2,09	8,30
7	COAPL	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01			0,05	3,96
8	DIV	0,44	0,45	0,43	0,44	0,58	0,44	0,45	0,44			1,76	3,98
9													
10													

count	8,00
lambda max	7,252
CI	0,108
CR	**0,08**
constant	1,41

Figura 7. 31 – Julgamento dos requisitos do proprietário com foco na eficiência.



RC Value = 0,003 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	IMN	CAD	TAU	FU	DIV				
1	AI	1,00	1,00000	0,20000	5,00000	3,00000	5,00000				
2	IMN	1,00	1,00	0,20000	5,00000	3,00000	5,00000				
3	CAD	5,00	5,00	1,00	25,00000	15,00000	25,00000				
4	TAU	0,20	0,20	0,04	1,00	0,67000	1,00000				
5	FU	0,33	0,33	0,067	1,66	1,00	1,66000				
6	DIV	0,20	0,20	0,04	1,00	0,60	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	7,73	7,73	1,55	38,66	23,27	38,66				

MATRIX NORMALIZADA

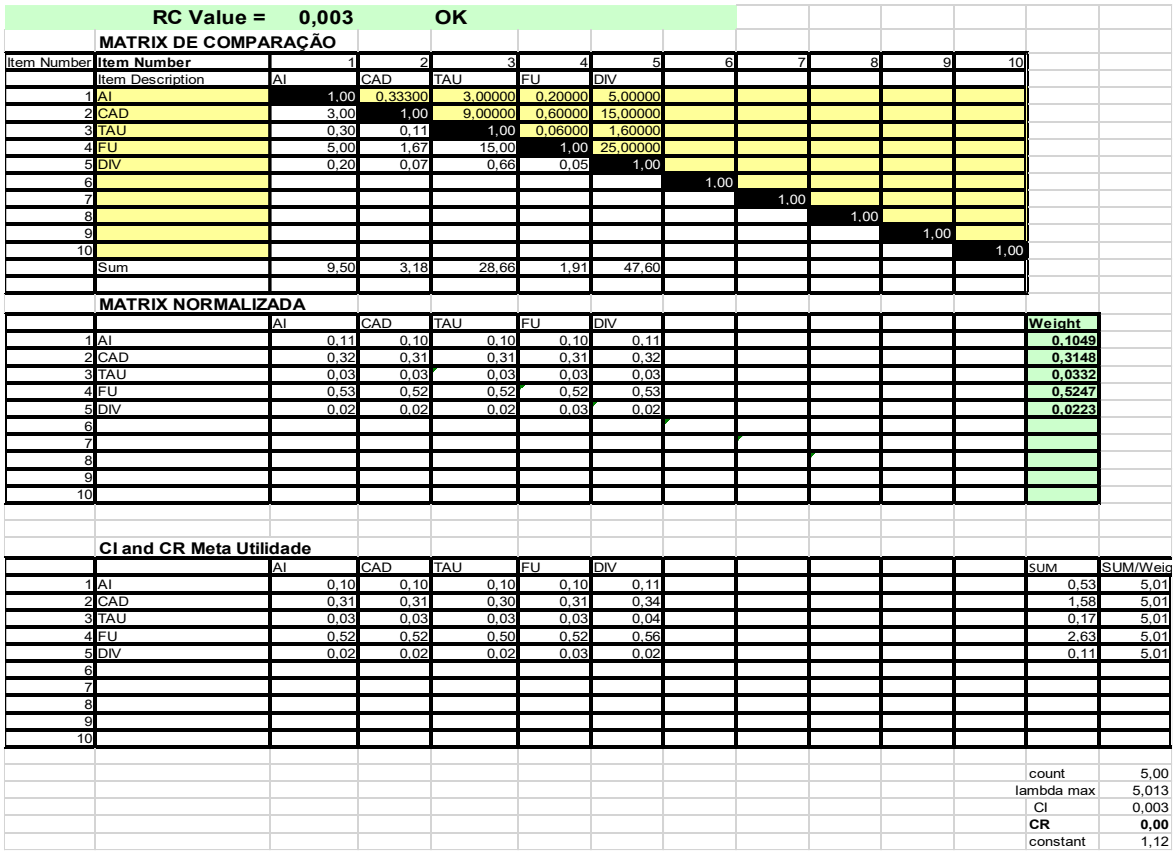
		AI	IMN	CAD	TAU	FU	DIV					Weight
1	AI	0,13	0,13	0,13	0,13	0,13	0,13					**0,1292**
2	IMN	0,13	0,13	0,13	0,13	0,13	0,13					**0,1292**
3	CAD	0,65	0,65	0,65	0,65	0,64	0,65					**0,6462**
4	TAU	0,03	0,03	0,03	0,03	0,03	0,03					**0,0264**
5	FU	0,04	0,04	0,04	0,04	0,04	0,04					**0,0431**
6	DIV	0,03	0,03	0,03	0,03	0,03	0,03					**0,0258**
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	IMN	CAD	TAU	FU	DIV					SUM	SUM/Weig
1	AI	0,13	0,13	0,13	0,13	0,13	0,13					0,78	6,02
2	IMN	0,13	0,13	0,13	0,13	0,13	0,13					0,78	6,02
3	CAD	0,65	0,65	0,65	0,66	0,65	0,65					3,89	6,02
4	TAU	0,03	0,03	0,03	0,03	0,03	0,03					0,16	6,02
5	FU	0,04	0,04	0,04	0,04	0,04	0,04					0,26	6,02
6	DIV	0,03	0,03	0,03	0,03	0,03	0,03					0,16	6,02
7													
8													
9													
10													

count	6,00
lambda max	6,019
CI	0,004
CR	**0,00**
constant	1,24

Figura 7. 32 – Julgamento dos requisitos do proprietário com foco na segurança.



RC Value = 0,003 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	AI	CAD	TAU	FU	DIV					
1	AI	1,00	0,33300	3,00000	0,20000	5,00000					
2	CAD	3,00	1,00	9,00000	0,60000	15,00000					
3	TAU	0,30	0,11	1,00	0,06000	1,60000					
4	FU	5,00	1,67	15,00	1,00	25,00000					
5	DIV	0,20	0,07	0,66	0,05	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	9,50	3,18	28,66	1,91	47,60					

MATRIX NORMALIZADA

		AI	CAD	TAU	FU	DIV						Weight
1	AI	0,11	0,10	0,10	0,10	0,11						**0,1049**
2	CAD	0,32	0,31	0,31	0,31	0,32						**0,3148**
3	TAU	0,03	0,03	0,03	0,03	0,03						**0,0332**
4	FU	0,53	0,52	0,52	0,52	0,53						**0,5247**
5	DIV	0,02	0,02	0,02	0,03	0,02						**0,0223**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		AI	CAD	TAU	FU	DIV						SUM	SUM/Weig
1	AI	0,10	0,10	0,10	0,10	0,11						0,53	5,01
2	CAD	0,31	0,31	0,30	0,31	0,34						1,58	5,01
3	TAU	0,03	0,03	0,03	0,03	0,04						0,17	5,01
4	FU	0,52	0,52	0,50	0,52	0,56						2,63	5,01
5	DIV	0,02	0,02	0,02	0,03	0,02						0,11	5,01
6													
7													
8													
9													
10													

count	5,00
lambda max	5,013
CI	0,003
CR	**0,00**
constant	1,12

Figura 7. 33 – Julgamento dos requisitos do proprietário com foco na aprendizagem.

RC Value = 0,001 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	IMN	TAU	FU	COAPL	DIV					
1	IMN	1,00	5,00000	0,33000	5,00000	7,00000					
2	TAU	0,20	1,00	0,06000	1,00000	1,40000					
3	FU	3,03	15,00	1,00	15,00000	21,00000					
4	COAPL	0,20	1,00	0,06	1,00	1,40000					
5	DIV	0,14	0,71	0,06	0,70	1,00					
6							1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	4,57	22,71	1,51	22,70	31,80					

MATRIX NORMALIZADA

		IMN	TAU	FU	COAPL	DIV						Weight
1	IMN	0,22	0,22	0,22	0,22	0,22						**0,2196**
2	TAU	0,04	0,04	0,04	0,04	0,04						**0,0431**
3	FU	0,66	0,66	0,66	0,66	0,66						**0,6614**
4	COAPL	0,04	0,04	0,04	0,04	0,04						**0,0431**
5	DIV	0,03	0,03	0,04	0,03	0,03						**0,0328**
6												
7												
8												
9												
10												

CI and CR Meta Utilidade

		IMN	TAU	FU	COAPL	DIV						SUM	SUM/Weig
1	IMN	0,22	0,22	0,22	0,22	0,23						1,10	5,00
2	TAU	0,04	0,04	0,04	0,04	0,05						0,22	5,00
3	FU	0,67	0,65	0,66	0,65	0,69						3,31	5,00
4	COAPL	0,04	0,04	0,04	0,04	0,05						0,22	5,00
5	DIV	0,03	0,03	0,04	0,03	0,03						0,16	5,00
6													
7													
8													
9													
10													

count	5,00
lambda max	5,003
CI	0,001
CR	**0,00**
constant	1,12

Figura 7. 34 – Julgamento dos requisitos do proprietário com foco na memorização.

RC Value = 0,000 OK

MATRIX DE COMPARAÇÃO

Item Number	Item Number	1	2	3	4	5	6	7	8	9	10
	Item Description	U	EFK	EFI	S	A	M				
1	U	1,00	3,00000	3,00000	5,00000	1,00000	5,00000				
2	EFK	0,33	1,00	1,00000	1,67000	0,33330	1,67000				
3	EFI	0,33	1,00	1,00	1,67000	0,33330	1,67000				
4	S	0,20	0,60	0,60	1,00	0,20000	1,00000				
5	A	1,00	3,00	3,00	5,00	1,00	5,00000				
6	M	0,20	0,60	0,60	1,00	0,20	1,00				
7								1,00			
8									1,00		
9										1,00	
10											1,00
	Sum	3,07	9,20	9,20	15,34	3,07	15,34				

MATRIX NORMALIZADA

		U	EFK	EFI	S	A	M					Weight
1	U	0,33	0,33	0,33	0,33	0,33	0,33					**0,3260**
2	EFK	0,11	0,11	0,11	0,11	0,11	0,11					**0,1088**
3	EFI	0,11	0,11	0,11	0,11	0,11	0,11					**0,1088**
4	S	0,07	0,07	0,07	0,07	0,07	0,07					**0,0652**
5	A	0,33	0,33	0,33	0,33	0,33	0,33					**0,3260**
6	M	0,07	0,07	0,07	0,07	0,07	0,07					**0,0652**
7												
8												
9												
10												

CI and CR Meta Utilidade

		U	EFK	EFI	S	A	M					SUM	SUM/Weig
1	U	0,33	0,33	0,33	0,33	0,33	0,33					1,96	6,00
2	EFK	0,11	0,11	0,11	0,11	0,11	0,11					0,65	6,00
3	EFI	0,11	0,11	0,11	0,11	0,11	0,11					0,65	6,00
4	S	0,07	0,07	0,07	0,07	0,07	0,07					0,39	6,00
5	A	0,33	0,33	0,33	0,33	0,33	0,33					1,96	6,00
6	M	0,07	0,07	0,07	0,07	0,07	0,07					0,39	6,00
7													
8													
9													
10													

count	6,00
lambda max	6,001
CI	0,000
CR	**0,00**
constant	1,24

Figura 7. 35 – Julgamento dos critérios do proprietário com foco na usabilidade.

Apêndice D – Média geométrica dos autovetores com múltiplos decisores.

PESOS DOS JULGAMENTOS DO GRUPO MULTIDISCIPLINAR COM FOCO NA UTILIDADE							
CRITÉRIOS	AI	IMN	CAD	TAU	DISMOV	FU	COAPL
PROPRIETÁRIO	0,0508	0,0508	0,2539	0,0097	0,2539	0,3565	0,0243
ADMINISTRADOR 1	0,0805	0,0106	0,0794	0,2462	0,0794	0,4006	0,1034
ADMINISTRADOR 2	0,1547	0,0538	0,0964	0,4510	0,0964	0,0964	0,0512
DESENVOLVEDOR	0,3248	0,0650	0,3248	0,0466	0,1073	0,0658	0,0658
ANALISTA DE SEGURANÇA	0,1068	0,0214	0,0214	0,0349	0,1068	0,5570	0,1517
PESO RELATIVO (MVT)	0,1170	0,0332	0,1062	0,0707	0,1174	0,2191	0,0663

Figura 8. 1 – Média geométrica dos autovetores com foco na utilidade da aplicação.

PESOS DOS JULGAMENTOS DO GRUPO MULTIDISCIPLINAR COM FOCO NA EFICÁCIA								
CRITÉRIOS	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV
PROPRIETÁRIO	0,0749	0,1465	0,0749	0,0147	0,1465	0,0919	0,2253	0,2253
ADMINISTRADOR 1	0,0629	0,0629	0,0205	0,0629	0,0832	0,2523	0,0122	0,4429
ADMINISTRADOR 2	0,1116	0,1116	0,0370	0,1116	0,1437	0,4465	0,0224	0,0154
DESENVOLVEDOR	0,0627	0,0627	0,0203	0,0627	0,0627	0,2515	0,0368	0,4403
ANALISTA DE SEGURANÇA	0,1364	0,0465	0,1364	0,4097	0,0460	0,1516	0,0465	0,0270
PESO RELATIVO (MVT)	0,0853	0,0786	0,0436	0,0767	0,0872	0,2086	0,0402	0,1129

Figura 8. 2 - Média geométrica dos autovetores com foco na eficácia da aplicação.

PESOS DOS JULGAMENTOS DO GRUPO MULTIDISCIPLINAR COM FOCO NA EFICIÊNCIA								
CRITÉRIOS	AI	IMN	CAD	TAU	DISMOV	FU	COAPL	DIV
PROPRIETÁRIO	0,0629	0,0629	0,0205	0,0629	0,0831	0,2522	0,0128	0,4426
ADMINISTRADOR 1	0,1319	0,1319	0,0436	0,1319	0,2651	0,1200	0,0438	0,1319
ADMINISTRADOR 2	0,0719	0,0233	0,2162	0,0233	0,0702	0,2162	0,0104	0,3684
DESENVOLVEDOR	0,0846	0,0281	0,2541	0,0288	0,0846	0,2541	0,0118	0,2541
ANALISTA DE SEGURANÇA	0,0849	0,0281	0,2537	0,0284	0,0852	0,2537	0,0122	0,2537
PESO RELATIVO (MVT)	0,0844	0,0433	0,1045	0,0437	0,1022	0,2114	0,0153	0,2681

Figura 8. 3 - Média geométrica dos autovetores com foco na eficiência da aplicação.

PESOS DOS JULGAMENTOS DO GRUPO MULTIDISCIPLINAR COM FOCO NA SEGURANÇA						
CRITÉRIOS	AI	IMN	CAD	TAU	FU	DIV
PROPRIETÁRIO	0,1292	0,1292	0,6462	0,0264	0,0431	0,0258
ADMINISTRADOR 1	0,0518	0,0518	0,2599	0,0124	0,2599	0,3642
ADMINISTRADOR 2	0,0381	0,2695	0,0382	0,1921	0,2695	0,1924
DESENVOLVEDOR	0,0582	0,5249	0,0066	0,0591	0,0591	0,2920
ANALISTA DE SEGURANÇA	0,0330	0,2337	0,1666	0,1666	0,2337	0,1664
PESO RELATIVO (MVT)	0,0547	0,1858	0,0934	0,0573	0,1330	0,1545

Figura 8. 4 - Média geométrica dos autovetores com foco na segurança da aplicação.

PESOS DOS JULGAMENTOS DO GRUPO MULTIDISCIPLINAR COM FOCO NA APRENDIZAGEM					
CRITÉRIOS	AI	CAD	TAU	FU	DIV
PROPRIETÁRIO	0,1049	0,3148	0,0332	0,5247	0,0223
ADMINISTRADOR 1	0,0458	0,1406	0,0467	0,4335	0,3333
ADMINISTRADOR 2	0,0478	0,2388	0,1431	0,3335	0,2368
DESENVOLVEDOR	0,0320	0,2902	0,2270	0,1605	0,2902
ANALISTA DE SEGURANÇA	0,2293	0,0732	0,2341	0,2341	0,2293
PESO RELATIVO (MVT)	0,0700	0,1863	0,1034	0,3097	0,1637

Figura 8. 5- Média geométrica dos autovetores com foco na aprendizagem da aplicação.

PESOS DOS JULGAMENTOS DO GRUPO MULTIDISCIPLINAR COM FOCO NA MEMORIZAÇÃO					
CRITÉRIOS	IMN	TAU	FU	COAPL	DIV
PROPRIETÁRIO	0,2196	0,0431	0,6614	0,0431	0,0328
ADMINISTRADOR 1	0,1409	0,0460	0,7192	0,0470	0,0470
ADMINISTRADOR 2	0,0585	0,2913	0,4126	0,0593	0,1784
DESENVOLVEDOR	0,0987	0,0987	0,2979	0,0143	0,4905
ANALISTA DE SEGURANÇA	0,5928	0,1186	0,0854	0,1187	0,0846
PESO RELATIVO (MVT)	0,1603	0,0925	0,3465	0,0459	0,1026

Figura 8. 6 - Média geométrica dos autovetores com foco na memorização da aplicação.

Apêndice E – Questionário fechado do método USASEC

Este Apêndice apresenta o questionário fechado com questões sobre os requisitos de usabilidade da aplicação web, com base no questionário de [75], [84], [85] e [86], adaptado para a utilização em requisitos de usabilidade, este questionário serve de validação da priorização e classificação encontrada após o passo 8 do método.

Nome: _____
Email: _____
Cargo que ocupa na organização: _____ **Data:** _____
Organização: _____ **Nível de Experiência no SIGIPAAerEX:** _____

De acordo com as características do seu sistema, várias hipóteses de melhorias foram elencadas. De sua opinião de quais delas são as mais importantes. Agradecemos sua contribuição. Obrigado!!

Ordene de 1 (mais importante) a 8 (menos importante) os itens que você considera mais importante para a usabilidade do seu sistema web.

1- Na melhoria da usabilidade do software, o que você considera mais importante?
[ ] – Acesso à Internet acesso.
[ ] – Consulta para a Análise estatística de dados.
[ ] – Inclusão de um manual de instruções para usuários.
[ ] – Telas diferenciadas para administradores e usuários comuns.
[ ] – Acesso à aplicação por dispositivos móveis.
[ ] – Facilidade de uso.
[ ] – Confeccionar aplicativos móveis.
[ ] – Melhorar a divulgação das ferramentas da aplicação.

Para as questões 2 – 8, ordene de 1 (como mais importante) até 5 (como menos importante), se for o caso, as ações que você considera mais importante para a usabilidade do seu sistema web de acordo com cada requisito avaliado anteriormente.

2- Quais as características mais importantes em relação a acesso à Internet?

1. [ ] – Passagem dos relatórios de prevenção em tempo real.
2. [ ] – Acesso de qualquer localidade.
3. [ ] – Integração com outros sistemas de prevenção de incidentes como o CENIPA por exemplo.
4. [ ] – Facilidade de acessar os relatórios para realização dos *briefing* dos pilotos.
5. [ ] – Possibilidade de ter acesso a informações corretivas para evitar acidentes em tempo real.

3- O que você considera mais importante em relação a consulta para análise estatísticos de dado?

1. [ ] – Gerar gráficos e relatórios específicos de suas aeronaves.
2. [ ] – Buscar informações que ocorreram em rotas que serão percorridas.
3. [ ] – Gerar estatísticas anuais de incidentes e principais causas para a SIPAA.
4. [ ] – Manter um banco de dados atual de todos os incidentes.
5. [ ] – Possibilidade de tentar predizer quando um incidente pode ocorrer (mineração de dados).

4- Quais as características mais importantes em relação a inclusão de manual?

1. [ ] – Tirar dúvidas dos usuários.
2. [ ] – Divulgar as possibilidades das ferramentas que a aplicação possui.
3. [ ] – Relembrar como determinada atividade é feita.
4. [ ] – Manter a aplicação usável pela leitura do manual.
5. [ ] – Possibilidade de o usuário aprender sozinho a utilizar as ferramentas da aplicação.

5- O que você considera mais importante em relação a confecção de telas diferenciadas para usuários administradores e comuns?

1. [ ] – Facilitar a visualização das normas que foram expedidas.
2. [ ] – Facilidade de encontrar as informações necessárias.
3. [ ] – Direcionar as ações corretivas para setores específicos competentes.
4. [ ] – Devido à grande rotatividade de pessoal, facilitar a troca de usuários por causa da mudança de função ou ausência do mesmo.

6- Quais as características mais importantes em relação a utilização de dispositivos móveis para acesso a aplicação?

1. [ ] – Utilização de tablets.
2. [ ] – Permitir a utilização de computadores móveis com rede VPN.
3. [ ] – Acesso a aplicação por *smartphones*.

7- Quais as características mais importantes em relação a facilidade de uso?

1. [ ] – Aviso aos usuários da aplicação sobre tarefas a cumprir por e-mail.
2. [ ] – Padronização de termos técnicos que devem ser utilizados na aplicação.
3. [ ] – Relatório com as RSV pendentes dos usuários.
4. [ ] – Diminuição das barras de rolagem.
5. [ ] – Telas de auxílio aos *briefing'*s.

8- Quais as características mais importantes em relação a confecção de aplicativo móveis?

1. [ ] – Uso através do *smartphone*.
2. [ ] – Utilização da aplicação mesmo em ambiente fora da rede interna de dados.
3. [ ] – Melhorar o acesso diário as recomendações de segurança.
4. [ ] – Possibilidade de ter acesso rápido e fácil a aplicação.

9- O que você considera como meio mais importante na divulgação das ferramentas que a aplicação possuí?

1. [ ] – Realização de instruções e palestras
2. [ ] – Avisos na rede interna através de links

3. [ ] – Instruções periódicas com os órgãos responsáveis (SIPAA)
4. [ ] – Mudança na cultura de acesso, colocar nas atividades diárias a consulta como obrigatória.

Glóssario

A

ANÁLISE DOS MODOS DE FALHAS E DE SEUS EFEITOS (*Failure Mode and Effect Analyses* (FMEA)) - uma ferramenta para prevenir falhas e analisa riscos de um processo ou produto [90].

APRENDIZAGEM – Facilidade do usuário em aprender as tarefas do sistema [30].

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT) - um órgão privado e sem fins-lucrativos que se destina a padronizar as técnicas de produção feitas no país [38].

PROCESSO DE ANÁLISE HIERÁRQUICA (AHP) - processo para auxiliar as pessoas na tomada de decisões complexas [95].

C

CASA DA QUALIDADE (*House of Quality - HoQ*) - método para balancear forças concorrentes de uma determinada caracterísa técnica e de qualidade de um produto [55].

FALSIFICAÇÃO DE SOLICTAÇÃO ENTRE SITES (*Cross-Site Request Forgery* (CRFS)) - exploração maliciosa de um website pelo qual comandos não autorizados são transmitidos para um site malicioso [7].

CENTRO DE ESTRATÉGIA E ESTUDOS INTERNACIONAIS (*Center for Strategic and International Studies (*CSIS)) – Conduz estudos de políticas e análises estratégicas de questões políticas, econômicas e de segurança em todo o mundo, com foco específico em questões relacionadas às relações internacionais, comércio, tecnologia, finanças, energia e geoestratégia [12].

D

DESDOBRAMENTO DA FUNÇÃO DA QUALIDADE (*Quality Function Deployment*) – mé todo que traduz as exigências dos clientes em características da qualidade do produto por intermédio de desdobramentos sistemáticos em suas matrizes [28].

DESDOBRAMENTO DA FUNÇÃO DE QUALIDADE DE SOFTWARE (*Software Quality Function Deployment* (SQFD)) – método que permite às organizações priorizarem as deman das dos usuários e especificações técnicas para produtos de softwares [57].

DESIGN CENTRADO NO USUÁRIO (*User-Centered Design* (UCD)) - é o método onde o

foco permance nas necessidades, desejos e limitações dos usuários durante todo o projeto, a cada tomada de decisão, desde a concepção até o lançamento do produto [36].

DESIGN DE SEIS SIGMA (*Design For Six Sigma* (DFSS)) - é um método que visa manter a qualidade em projetos de novos produtos, o modelo pode ser aplicado em processos produtivos ou na execução de serviços que precisam ser elaborados de tal forma que ao entrarem em funcio namento já atinjam a excelência dos seis sigmas [28].

H

INTERAÇÃO HOMEM-COMPUTADOR E SEGURANÇA (*Human-Computer Interaction Security* (HCISEG)) – método hibrido de avaliação de sistemas computacionais interativos pa ra uso humano que utiliza atributos de usabilidade e segurança [29].

INTERAÇÃO HOMEM-COMPUTADOR (*HUMAN-COMPUTER INTERACTION* (HCI)) - disciplina relacionada ao projeto, implementação e avaliação de sistemas computacionais interativos para uso humano, juntamente com os fenômenos relacionadosa esse uso [30].

I

ÍNDICE DE CONSISTÊNCIA IC – Magnitude de perturbação incidente na matriz de comparação do Processo de Análise Hierárquica (AHP) [95].

INTERNET DAS COISAS (*Internet of Things* – (IoT)) - é uma revolução tecnológica a fim de conectar dispositivos eletrônicos utilizados no dia-a-dia [11].

ÍNDICE DE CONSISTÊNCIA RANDÔMICO (IR) - um índice aleatório, calculado para matrizes quadradas de ordem “n” pelo Laboratório de Oak Ridge, nos estados Unidos [99].

M

MÉTODO - aglomerado de regras básicas dos procedimentos que produzem o conhecimento científico, quer um novo conhecimento, quer uma correção (evolução) ou um aumento na área de incidência de conhecimentos anteriormente existentes [84].

MÉTODO DE MELHORAMENTO DE PRODUTOS PARA DEFINIR, MEDIR, ANALISAR, APERFEIÇOAR E CONTROLAR (*Define Measure Analyse Improve and Control* DMAIC) - método que faz parte do conjunto de práticas dos Seis Sigmas e tem como meta melhorar um processo existente na empresa [28].

MÉTODO DE MELHORAMENTO DE PRODUTOS PARA DEFINIR, MEDIR, ANALISAR,

DESENHAR E VERIFICAR (*Define Measure Analyse Design and Verify* (DMADV)) – méto do útil para melhorar processo de redução de defeitos já existentes em uma empresa [28].

METODOLOGIA - campo em que se estuda os melhores métodos praticados em determinada área para a produção do conhecimento [85].

MODERNO SQFD - método que relaciona às necessidades dos clientes (voz do usuário) e os pontos fortes do projeto, aqueles que devem receber foco em recursos, indeferindo estes requisitos no software final [28].

MODULO ROBUSTO DE DESENVOLVIMENTO DE SOFTWARE (*Robust Software Deployment Model* (RSDM)) - Modelo que busca dar suporte na produção e desenvolvimento de softwares [28].

MELHORES PRÁTICAS DE CODIFICAÇÃO DE SEGURA (*Application Security Verification Standard* (ASVS)) – o padrão de verificação de segurança em aplicações web é o conjunto de codificações e regras que visa dirimir as vulnerabilidades [7].

O

OPORTUNIDADE – ocasião favorável para a inserção e análise de riscos cibernéticos [14].

MODELO DE INTERLIGAÇÃO DE SISTEMAS ABERTOS (*Open System Interconnection* (OSI)) – modelo para padronizar a comunicação entre sistemas de processamento heterogêneos, que vem sendo utilizado em diversas aplicações [54].

PROJETO ABERTO DE SEGURANÇA EM APLICAÇÕES WEB (*Open Web Application Security Project* (OWASP)) – Entidade sem fins lucrativos que publica prátics e procedimentos de segurança em aplicações web periodicamente [7].

P

PASSOS – Sequências lógicas organizadas de forma a realizar a resolução de um problema [2].

PARADIGMA - onceito sobre algo ou alguma coisa ou determinados preconceitos pré-estabelecidos por uma sociedade [85]

PRÍNCIPIOS DE SEGURANÇA DA INFORMAÇÃO – propriedades da segurança da informação que visam garantir a continuidade do negócio e seus ativos [53].

PROCESSO DE ANÁLISE HIERARQUICA MULTIPLICATIVO (*Multiple Analysis Hierarchy Process* (MAHP)) – evolução do método AHP com utilização da função geométrica da tabela de Lootsma [32].

R

RELEVÂNCIA – particularidade relevante para a interação entre o software e o usuário que deve garantir uma análise dos riscos cibernéticos que essa pode gerar [14].

S

SEGURANÇA DA INFORMAÇÃO - proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização [53].

SISTEMA DE SUPERVISÃO E AQUISIÇÃO DE DADOS (*Supervisory Control and Data Acquisition* (SCADA)) - são sistemas que utilizam software para monitorar e supervisionar as variáveis e os dispositivos de sistemas de controle conectados através de controladores (drivers) específicos [4].

SISTEMA MILITAR DE COMANDO E CONTROLE (SISMC²) – Plataformas e softwares para apoio às operações de comando e controle de uma força componente [50].

T

TABELA DE MÁXIMO VALOR (*Maximum Voice Table* (MVT)) - tabela com os requisitos de usabilidade priorizados pelo método AHP [28].

TABELA DE VOZ DO USUÁRIO (*User Voive Table* (UVT)) – tabela com as declarações de usabilidade colhidas por questionários, para a melhoria do sistema, organizadas em um diagrama de árvore [28].

TABELA DA VOZ DO CLIENTE (*Customer Value Table* (CVT)) – tabela com as declarações colhidas por questionário de forma bruta [28].

GESTÃO DA QUALIDADE TOTAL (*Total Quality Management* (TQM)) - é uma opção para a reorientação gerencial das organizações [28].

U

USABILIDADE - termo usado para definir a facilidade com que as pessoas podem empregar uma ferramenta ou objeto a fim de realizar uma tarefa específica e importante [30].

FOLHA DE REGISTRO DO DOCUMENTO

1. CLASSIFICAÇÃO/TIPO	2. DATA	3. REGISTRO N°	4. N° DE PÁGINAS
DM	14 de Julho de 2017	DCTA/ITA/DM-042/2017	182

5. TÍTULO E SUBTÍTULO:
USASEC: Um Método Para Integração De Requisitos De Usabilidade E Segurança Para Proteção Cibernética Em Aplicações WEB.

6. AUTOR(ES):
Ricardo Férre Lacerda Ferreira

7. INSTITUIÇÃO(ÕES)/ÓRGÃO(S) INTERNO(S)/DIVISÃO(ÕES):
Instituto Tecnológico de Aeronáutica - ITA

8. PALAVRAS-CHAVE SUGERIDAS PELO AUTOR:
Requisitos de usabilidade e segurança da informação, Desdobramento da Função de Qualidade de Software (SQFD), Proteção Cibernética.

9.PALAVRAS-CHAVE RESULTANTES DE INDEXAÇÃO:
Segurança da informação de computadores; Desdobramento da função qualidade; Integração de dados; Detecção de intrusão (computadores); Redes de comunição; Computação.

10. APRESENTAÇÃO: **X Nacional** **Internacional**
ITA, São José dos Campos. Curso de Mestrado. Programa de Pós-Graduação em Engenharia Eletrônica e Computação. Área de Informática. Orientador: Carlos Henrique Quartucci Forster ; co-orientador: Edgar Toshiro Yano. Defesa em 23/06/2017. Publicada em 2017.

11. RESUMO:
A presteza das informações e as recentes tecnologias integradas de dados estabeleceram um ambiente mundial interconectado de alta concorrência onde requisitos como prazo, qualidade e segurança dos softwares precisam ser atendidos. Nesse intuito, organizações investem recursos para que suas soluções de tecnologias possam oferecer qualidade para seus usuários e segurança da informação. Ainda, por causa da migração para a plataforma web de vários serviços e atividades, tem crescido o número de incidentes de segurança como ataques cibernéticos a estes sistemas. Para mitigá-los, é necessário manter os sistemas em constante aperfeiçoamento e atualizados contra as novas ameaças e vulnerabilidades apresentadas diariamente no ambiente virtual. Esses avanços nas regras de segurança obrigam os usuários a realizar tarefas cada vez mais complexas, impactando a usabilidade dos usuários. Para garantir a usabilidade, sem empenhar padrões oportunos de segurança, mostra-se necessária um método capaz de acoplar os requisitos de usabilidade aos requisitos de segurança. Com o método proposto, denominado USASEC, é possível priorizar e integrar quais requisitos de usabilidade e segurança mais impactam as tarefas do usuário. Para isso, este método utiliza uma derivação de um método para qualidade de software; o Desdobramento da Função de Qualidade de Software (o moderno SQFD), para identificar, filtrar, classificar, organizar, priorizar e integrar estes requisitos. Em cada uma destas, foram definidos métodos específicos como: Avaliação em Percurso Pluralístico da aplicação web, Diagrama de Árvore, Diagrama de Afinidade, Diagrama de Hierarquia, Processo de Análise Hierárquica e o método da Casa da Qualidade. Para validação do USASEC foi realizado um estudo de caso: no Sistema de Gerenciamento de Investigação e Prevenção de Acidentes Aeronáuticos (SIGIPAAerEx), uma aplicação web do Comando de Aviação do Exército Brasileiro, Taubaté, Brasil. Com uma amostra de usuários, os resultados mostraram uma taxa de acerto de oitenta porcento na priorização dos requisitos de usabilidade, após a aplicação do método.

12. GRAU DE SIGILO:
(X) OSTENSIVO **( ) RESERVADO** **( ) SECRETO**