Capítulo 1

Gestão de Riscos

José Eduardo Malta de Sá Brandão[1], Joni da Silva Fraga[2]

[1]Instituto de Pesquisa Econômica Aplicada (IPEA)
Brasília DF

[2]Departamento de Automação e Sistemas
Universidade Federal de Santa Catarina
Florianópolis SC

Abstract

The risks management process is based on the best practices principles of management and security, to assist in strategic decisions. It involves an organized and recursive process of documentation, evaluation and decision at all project life cycle steps. The objective of this course is to present the security risks management process, with its advantages and limitations. It includes the theoretical and practical aspects of the risks management, to create a knowledge base for the reader's own projects. We expects in the present course to contribute to the knowledge of the security risk management methodology.

Resumo

A gestão de riscos baseia-se em princípios e boas práticas de gerenciamento e segurança, para auxiliar na tomada de decisões estratégicas. Ela envolve um processo organizado e recursivo de documentação, avaliação e decisão durante todas as fases do ciclo de vida do projeto. O objetivo desse curso é apresentar a disciplina de gestão de riscos de segurança, bem como suas vantagens e limitações. Nesse curso são apresentados aspectos teóricos e práticos da gestão de riscos, fornecendo aos alunos uma base para desenvolverem seus próprios projetos. Espera-se, portanto, com esse curso, contribuir para um melhor entendimento da metodologia de gestão de riscos.

1.1. Introdução

1.1.1. Motivação

Quando um sistema computacional apresenta vulnerabilidades que podem ser exploradas, produzindo algum impacto negativo, afirmamos que tal sistema está em risco. Contudo, quantificar ou até mesmo identificar os riscos não é uma tarefa trivial.

A noção correta dos riscos permite que se definam caminhos e ferramentas para mitigá-los. Infelizmente, Os riscos podem ser identificados e reduzidos, mas nunca totalmente eliminados [Garfinkel et al. 2003].

É comum a aplicação de ferramentas de análise de risco em protótipos desenvolvidos em projetos de software científicos ou comerciais. Isso ocorre após a conclusão de uma versão do desenvolvimento do protótipo, com a finalidade de identificar vulnerabilidades.

Em alguns sistemas computacionais, as vulnerabilidades encontradas podem ser inerentes à tecnologia adotada. Sendo assim, a mitigação dos riscos pode incluir a troca da tecnologia, com a inevitável onerosidade do projeto, ou a aceitação de um risco maior do que o desejado. Quando um projeto de software envolve a integração de múltiplas tecnologias, a identificação e a minimização dos riscos são ainda mais complexas. Tratar os riscos deste tipo de projeto apenas no ponto de protótipo pode ser extremamente dispendioso e, em alguns casos, os resultados podem inviabilizar o próprio projeto. Muitas vezes as vulnerabilidades encontradas poderiam ter sido facilmente identificadas na etapa de planejamento do projeto.

Os resultados esperados, com este minicurso, são um melhor entendimento destas metodologias de gestão de riscos e a difusão da idéia da necessidade da avaliação dos riscos associados aos sistemas computacionais, via estes testes padronizados.

1.1.2. Conceitos

Diversos conceitos tratados nesse curso são descritos nessa seção. Tais conceitos são essenciais para a compreensão dos modelos e padrões associados à gestão de riscos. Entre esses conceitos podemos destacar aqueles relacionados à segurança em tecnologia da informação (TI) e as definições de riscos de segurança.

1.1.2.1. Propriedades de Segurança

Segurança em tecnologia da informação é identificada como a capacidade de assegurar a prevenção ao acesso e à manipulação ilegítima da informação, ou ainda, de evitar a interferência indevida na sua operação normal [ISO/IEC 2005a].A segurança é fundamentada em três propriedades básicas [Bishop 2003] [ISO/IEC 2005a]:

- **Integridade**: garante que a informação não será alterada ou destruída sem a autorização adequada.
- **Confidencialidade**: garante que a informação não será revelada sem a autorização adequada.

- **Disponibilidade**: garante que a informação estará acessível aos usuários legítimos quando solicitada.

A propriedade de integridade inclui também, mas não exclusivamente, a **autenticidade** e a **não repudiação** [US Department of Homeland Security 2002] [Barker and Lee 2004]. A propriedade de autenticidade garante que a identidade de um sujeito ou recurso é aquela alegada, sendo aplicada a entidades como usuários, processos, sistemas e informações [ISO 1989]. A não repudiação garante que uma parte neutra possa ser convencida de que uma transação particular ou um evento tenha ou não ocorrido.

Nesse curso adotamos os objetivos da segurança definidos pelo NIST[1] (*National Institute of Standards and Technology*), que preconizam a preservação da integridade, da disponibilidade e da confidencialidade dos recursos dos sistemas de informações, incluindo: *hardware*, *software*, *firmware*, informação/dados e telecomunicações [Ross et al. 2005].

1.1.2.2. Violações de Segurança

Quando há a quebra de uma ou mais propriedades de segurança, há uma **violação de segurança**. Portanto, como as violações estão relacionadas com as três propriedades básicas, as mesmas podem ser classificadas também em três categorias:

- Revelação não autorizada da informação (violação de confidencialidade);
- Modificação não autorizada da informação (violação de integridade);
- Negação de serviço (violação de disponibilidade).

1.1.2.3. Vulnerabilidade

Uma **vulnerabilidade** é um defeito ou fraqueza no design ou na implementação de um sistema de informações (incluindo procedimentos de segurança e controles de segurança associados ao sistema), que pode ser intencionalmente ou acidentalmente explorada, afetando a confidencialidade, integridade ou disponibilidade [Ross et al. 2005].

1.1.2.4. Ameaças, Ataques e Intrusão

A vulnerabilidade, por si só, não representaria perigo se não houvesse a possibilidade da mesma ser explorada. Portanto, uma **ameaça** é qualquer circunstância ou evento com o potencial intencional ou acidental de explorar uma vulnerabilidade específica em qualquer sistema computacional, resultando na perda de confidencialidade, integridade ou disponibilidade [Barker and Lee 2004]. Atos intencionais que podem produzir violações de segurança são chamados de **ataques**. Finalmente, quando um ataque é bem sucedido, afirmamos que houve uma **intrusão**.

[1] http://www.nist.gov

1.1.2.5. Risco

O **risco** é o impacto negativo da exploração de uma vulnerabilidade, considerando a probabilidade do uso do mesmo e o impacto da violação [Stoneburner et al. 2002]. Ou seja, o risco é uma tentativa de quantificar as possibilidades de violação e os prejuízos decorrentes do impacto do mesmo.

O risco pode ser expressado matematicamente como uma função da probabilidade de uma origem de ameaça (ou atacante) explorar uma vulnerabilidade potencial e do impacto resultante deste evento adverso no sistema e, conseqüentemente, na empresa ou organização.

1.1.2.6. Gestão de Riscos

A gestão de riscos ultrapassa a análise de vulnerabilidades e riscos de um produto ou protótipo. A gestão de riscos baseia-se em atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos [ISO 2002]. A mesma envolve um processo criterioso e recursivo de documentação, avaliação e decisão durante todas as fases do ciclo de vida do projeto

1.1.3. Foco do Curso

O objetivo desse curso é apresentar a disciplina de gestão de riscos de segurança, bem como suas vantagens e limitações. O enfoque do curso visa elucidar aspectos conceituais e sistemáticos nestas metodologias, porém, um estudo de caso também enfatizará a aplicabilidade das técnicas apresentadas. Esse curso deverá fornecer aos alunos uma base para desenvolverem seus próprios projetos segundo a ótica da gestão de riscos.

A seção seguinte está focada nos principais conceitos, na descrição de modelos e na comparação dos principais padrões relacionados à gestão de riscos na segurança. Associada a estes modelos e padrões, na terceira seção é apresentada uma metodologia para auxiliar na análise quantitativa dos riscos. Um estudo de caso que visa reforçar a utilidade e necessidade do uso destas metodologias é apresentado na quarta seção. Este estudo de caso envolve um projeto na área de segurança de sistemas, guiado por estas metodologias de gestão de riscos. Finalmente, na última seção são apresentadas algumas considerações finais sobre o emprego da metodologia de gestão de riscos.

1.2. Principais Padrões Relacionados à Gestão de Riscos

Os governos e a sociedade estão cada vez mais preocupados com o que pode acontecer com eventuais perdas de dados, furto de informações e até mesmo com a perda de vidas ocasionadas por possíveis falhas em sistemas computacionais. Por isso, a segurança de sistemas de TI vem sendo foco de diversas organizações voltadas à recomendação de padrões e metodologias. Entre estas organizações podemos destacar a ISO[2](*International Organization for Standardization*), o NIST[3](*National Institute of Standards and Techno-*

[2] http://www.iso.org
[3] http://www.nist.gov

logy), a BSi[4](British Standards) e a AS/NZS[5](*Australian/New Zealand Standard*). No Brasil, a ABNT[6](Associação Brasileira de Normas Técnicas) é a responsável pela recomendação dos padrões técnicos.

As principais recomendações de segurança reforçam a adoção de boas práticas de gerenciamento de sistemas de TI. As recomendações de segurança mais conhecidas são as da série BS 7799 do BSi[BSi 1999][BSi 2002]. Desenvolvidas pelo governo Britânico, essas recomendações foram referências na definição de boas práticas de gestão de segurança em sistemas de informação. Posteriormente, os dois primeiros documentos da série BS 7799 foram revistos e reorganizados na série ISO/IEC 17799.

Atualmente, há um novo esforço de revisão dos documentos de segurança da informação, que estão sendo reclassificados na série ISO/IEC 27000. O objetivo deste esforço é o alinhamento das normas de gestão da segurança da informação às normas das famílias 9000 e 14000 da ISO. A Figura 1.1 mostra a relação e a evolução das normas de segurança.

A norma ISO 27000 está em desenvolvimento e irá definir os conceitos fundamentais e o vocabulário de segurança da informação adotado nesta série de documentos. A terminologia adotada na maioria das normas de segurança da informação é baseada no guia 73[ISO 2002], que está sendo revisto.

As normas ISO 27001[ABNT 2006b] e 27002[ABNT 2006a] foram baseadas nas normas BS 17799-2 [BSi 2002] e BS/ISO 17799-1[BS/ISO 2005], respectivamente. A recomendação ISO 27001 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação.

A norma ISO 27002 introduz os conceitos de segurança da informação e faz uma discussão inicial a respeito das motivações para o estabelecimento da gestão de segurança. Na maior parte do documento são detalhadas as práticas de segurança, que são associadas aos os objetivos de controles, e os controles de segurança citados na norma ISO 27001.

A norma ISO 27003, em desenvolvimento, é baseada no anexo B da norma BS 7799-2, sendo basicamente um guia para a implantação do Sistema de Gestão de Segurança da Informação (SGSI) apresentado nas duas normas anteriores.

Em geral, as técnicas de análise de riscos são focadas em testes ou são analíticas. A avaliação por testes baseia-se na verificação de *checklists* e na execução de testes para verificar se determinado sistema ou produto pronto encontra-se de acordo com especificações mínimas de segurança, estabelecidas previamente. Outros tipos de avaliação buscam acompanhar de forma sistemática o projeto de um sistema ou produto, garantindo que o mesmo seja desenvolvido seguindo especificações e boas práticas de segurança. Enquanto a avaliação por testes se aplica em sistemas prontos, a avaliação analítica ocorre durante todas as etapas do processo de desenvolvimento.

[4]http://www.bsi-global.com
[5]http://www.standards.org.au
[6]http://www.abnt.org.br

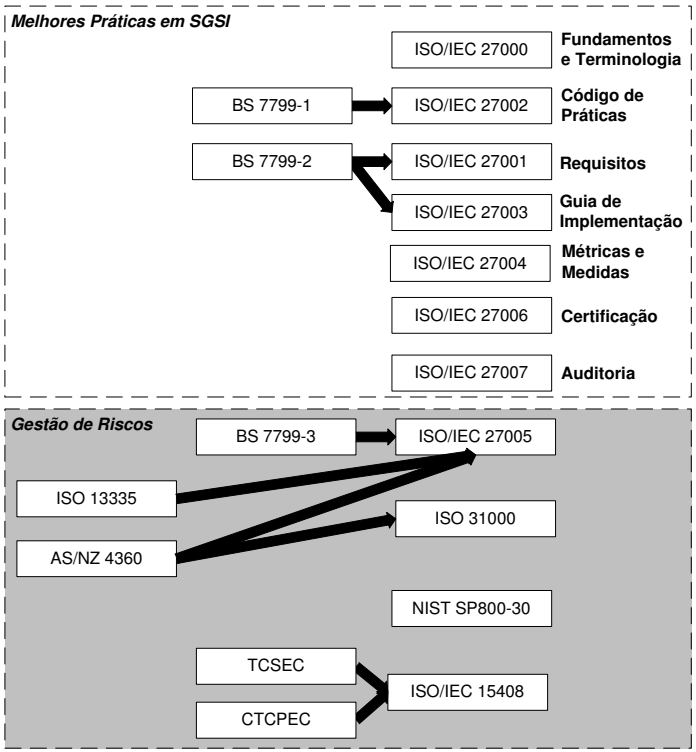

Figura 1.1. Relação entre as normas

Alguns esforços para padronização de metodologias para avaliação de sistemas de tecnologia da informação vêm sendo realizados. O *Common Criteria* (CC) [ISO/IEC 2005a] [ISO/IEC 2005b] [ISO/IEC 2005c] é um exemplo de uma metodologia de testes e acompanhamento de projeto. Ele busca avaliar produtos de segurança, fornecendo também subsídios para uma certificação de segurança destes produtos. Para cada classe de produtos, são definidos critérios que devem ser verificados.

A gestão de riscos baseia-se em princípios e boas práticas de gerenciamento e segurança [Swanson and Guttman 1996], para auxiliar na tomada de decisões. Entre as ferramentas metodológicas disponíveis para o desenvolvimento da gestão de riscos, destacamos a especificação SP800-30 [Stoneburner et al. 2002] desenvolvida pelo NIST, a especificação AS/NZ4360 [AS/NZS 2004a] desenvolvida pelos governos da Austrália e Nova Zelândia, a norma ISO/IEC 27005[ABNT 2008] e a proposta de norma ISO 31000[ISO 2007].

A seguir serão apresentados resumos das principais metodologias de avaliação de segurança em sistemas de tecnologia da informação.

1.2.1. Melhores Práticas

A norma ISO 27001 adota o modelo conhecido como PDCA (*Plan-Do-Check-Act*), ilustrado na figura 1.2, que é aplicado para estruturar todos os processos do Sistema de Gestão de Segurança da Informação (SGSI).

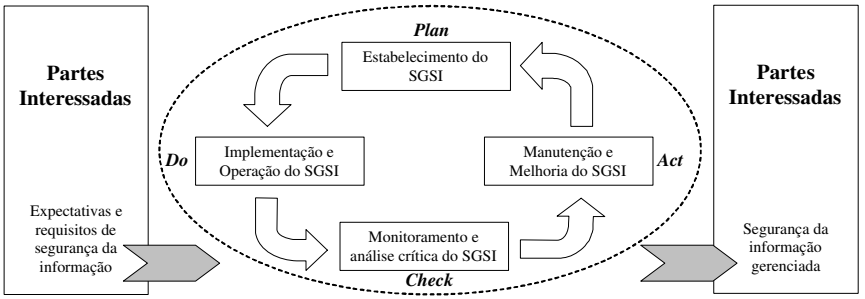

Figura 1.2. Modelo PCDA

O processo do PDCA inicia quando as partes interessadas definem os requisitos e as expectativas de segurança. Em seguida, é iniciado um procedimento cíclico de gestão, composto de quatro etapas complementares.

O ciclo começa com o estabelecimento da política, dos objetivos, dos processos e dos procedimentos do SGSI (Plan), que sejam relevantes para a gestão de riscos e a melhoria da segurança da informação e que produzam resultados de acordo com as políticas e objetivos globais de uma organização.

A segunda etapa (Do) envolve a implantação e a operação da política, dos controles, dos processos e dos procedimentos estabelecidos na primeira etapa.

Na terceira fase (Check) é feita a avaliação e, quando aplicável, a medição do desempenho de um processo frente à política, aos objetivos e à experiência prática do SGSI, apresentando os resultados para a análise crítica pela direção.

No quarto passo (Act) cabe a execução das ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI. Após esta etapa, o ciclo é reiniciado, tomando como base o aprendizado do ciclo anterior. O resultado esperado da adoção do PDCA é a segurança da informação devidamente gerenciada.

A norma estabelece ainda as diretrizes para uma auditoria no SGSI, definindo os objetivos de controles e os controles necessários para o gerenciamento de segurança de diversos aspectos de um ambiente de TI.

1.2.2. Common Criteria (CC)

O conjunto de especificações ISO [ISO/IEC 2005a] [ISO/IEC 2005b] [ISO/IEC 2005c] que formam o *Common Criteria* são derivados de padrões desenvolvidos anteriormente: o TCSEC (livro laranja) desenvolvido pelo governo dos EUA; o CTCPEC, criado pelo go-

verno canadense; e o ITSEC, desenvolvido pelos países europeus. Lançado inicialmente em 1995, o CC sofreu revisões recentes.

O CC se baseia em uma linguagem e numa estrutura comuns para expressar requisitos de segurança de sistemas e produtos de tecnologia da informação (TI). Tais sistemas e produtos são chamados de **alvos da avaliação** (*target of evaluation* - ***TOE***). Baseado no CC são desenvolvidos **perfis de proteção** (*protection profiles* - ***PP***) e **alvos de segurança** (*security targets* - ***ST***), que por meio de requisitos especificam o que o sistema deve fazer. O PP especifica um conjunto de requisitos de segurança, independentes de implementação, para uma categoria de TOEs, como por exemplo, sistemas de detecção de intrusão. O ST define um conjunto de requisitos e especificações para ser usado como base para avaliação de um TOE específico, como por exemplo um IDS de determinado fabricante. Um ST de um produto pode incorporar requisitos ou declarar conformidade com um ou mais PPs.

O TOE, após ter seu ST avaliado com relação aos PPs próprios, recebe uma certificação de nível de garantia (*Evaluation Assurance Level* - *EAL*), que o classifica segundo uma escala progressiva (de EAL1 a EAL7) de características de segurança. O nível EAL1 certifica que o TOE teve seu funcionamento testado. O nível EAL2 estabelece que o sistema teve sua estrutura testada e envolve a cooperação do fabricante. O nível EAL3 certifica que o TOE foi metodicamente testado e checado. O nível EAL4 define que o sistema foi metodicamente projetado, testado e checado. O nível EAL5 prevê que o sistema seja projetado e testado de maneira semiformal. O nível EAL6 sustenta que o TOE foi projetado, verificado e testado de maneira semiformal. Por último, o nível EAL7 certifica que o sistema foi projetado, verificado e testado de maneira formal.

O CC considera que a segurança pode ser obtida durante as fases de desenvolvimento, avaliação e operação do TOE. No desenvolvimento, a segurança é obtida com refinamentos dos requisitos de segurança, gerando uma especificação sumária do TOE presente em um ST. Na fase de operação, podem surgir vulnerabilidades no TOE, exigindo modificações no sistema e a reavaliação da segurança. Na fase de avaliação, o TOE é verificado com base no ST e envolve análise e testes do produto.

1.2.3. NIST SP800-30

O NIST (*National Institute of Standards and Technology*) disponibiliza uma série de publicações relacionadas à tecnologia da informação. Entre estas publicações está a recomendação SP800-30 (*Risk Management Guide for Information Technology Systems*) [Stoneburner et al. 2002]. O documento fornece a fundamentação para o desenvolvimento de um programa de gestão de riscos, contendo as definições e as direções necessárias para avaliar e atenuar os riscos identificados em sistemas de TI.

A metodologia de gestão de riscos da especificação SP800-30 consiste de duas etapas: avaliação de riscos (ou determinação dos riscos) e atenuação de riscos. Além destas duas etapas, a revisão periódica de todo o processo é recomendada. O processo de avaliação de riscos segue um fluxo de atividades, conforme ilustrado na Figura 1.3.

O primeiro passo da metodologia consiste em caracterizar o sistema implementado, descrevendo o ambiente ao qual está vinculado, a sua missão, os seus requisitos

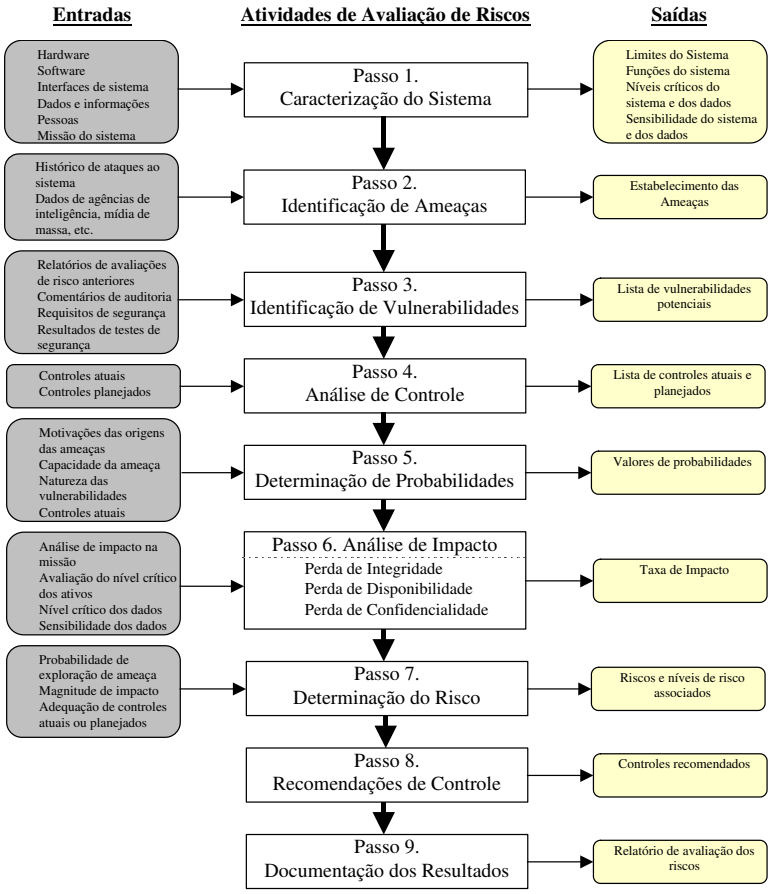

Figura 1.3. Metodologia de gestão de riscos da especificação SP800-30 [Stoneburner et al. 2002]

funcionais, as suas interfaces, as pessoas envolvidas no suporte, os dados e informações etc. As etapas 2,3,4 e 6 podem ser conduzidas em paralelo, após a caracterização do sistema.

A segunda etapa visa identificar as ameaças que podem explorar vulnerabilidades do sistema. A terceira etapa consiste na identificação de vulnerabilidades ou falhas que podem ser exploradas no sistema. Este passo também inclui a identificação da origem das vulnerabilidades e como elas podem ser exploradas.

O objetivo da quarta etapa é analisar os controles de segurança que estão implementados ou pretende-se implantar. os controles podem ser preventivos, quando inibem as tentativas de violação de segurança, ou podem visar a detecção de possíveis ataques. Os controles também podem ser classificados como técnicos e não técnicos. Os controles

técnicos podem ser incorporados no *hardware* ou *software* dos sistemas. Os controles não técnicos envolvem controles de gerenciamento e operacionais, como: políticas de segurança, procedimentos operacionais, gestão de pessoal, controles físicos ou ambientais.

A quinta etapa define os valores das probabilidades de exploração de uma potencial vulnerabilidade, por uma ameaça. A metodologia define três níveis subjetivos de probabilidade: alta, média e baixa. A probabilidade será alta se o possível atacante estiver altamente motivado e for suficientemente capaz de explorar uma vulnerabilidade cujos controles forem ineficazes. A probabilidade será média se o possível atacante estiver motivado e capaz para explorar uma vulnerabilidade, mas os controles podem impedir com sucesso que a mesma seja explorada. A probabilidade baixa será atribuída se o possível atacante não estiver motivado ou não for capaz de explorar uma vulnerabilidade ou se os controles podem prevenir ou impedir que a mesma seja explorada.

A análise de impacto corresponde à sexta etapa e visa determinar os danos potenciais que o resultado adverso de um ataque ou violação bem sucedida causa ao sistema. O impacto de um evento de segurança pode ser descrito em termos de perda ou degradação de qualquer uma, ou de uma combinação de quaisquer, das propriedades de segurança: integridade, disponibilidade e confidencialidade. A análise do impacto pode ser feita utilizando avaliações quantitativas ou qualitativas.

A determinação dos níveis de risco é a sétima etapa. Nela é determinado o grau de suscetibilidade ao risco que cada vulnerabilidade representa, considerando a probabilidade da mesma ser explorada, a magnitude do impacto adverso que o fato causaria e a adequação dos controles para reduzir ou eliminar os riscos. Matrizes ou gráficos podem ser utilizados para combinar estes fatores e determinar quantitativamente ou qualitativamente os níveis de risco.

A oitava etapa consiste em relacionar o conjunto de controles que podem reduzir ou eliminar os riscos identificados. O objetivo da recomendação de controles é reduzir o nível de risco de um sistema de TI a um patamar aceitável.

A última etapa corresponde à produção de documentação com os resultados do processo de análise de risco. Também são documentados os resultados parciais de todas as etapas anteriores.

O segundo processo da metodologia de gestão de riscos é a atenuação dos riscos, que envolve a priorização, avaliação e implementação dos controles para redução dos níveis de risco, recomendados no processo de avaliação de riscos. Como a eliminação dos riscos é inexeqüível ou próxima do impossível, cabe aos gestores da empresa usar uma abordagem de custo mínimo e implementar os controles mais apropriados para reduzir os riscos a um nível aceitável, com um impacto adverso mínimo na organização.

A metodologia SP800-30 vem sendo adotada com freqüência na segurança de projetos de TI. Porém, seu uso em projetos científicos é raro.

1.2.4. AS-NZ4360, ISO 27005 e ISO 31000

A norma AS/NZ4360 [AS/NZS 2004a] serviu de referência para o desenvolvimento de todas as demais normas de gestão de riscos que a sucederam. A norma ISO 3100, por

exemplo, segue o mesmo processo e possui os mesmos elementos. Já a norma ISO 27005 traz pequenas alterações no processo.

As fases de identificação, análise e avaliação dos riscos da especificação AS/NZ 4360 possuem similaridade com o processo de avaliação de riscos (ou determinação dos riscos) da especificação SP800-30. A etapa de tratamento também é similar à etapa de atenuação dos riscos. A especificação AS-NZ4360 e seu guia [AS/NZS 2004b] são bem mais amplos que as normas de gestão de risco que a antecederam e não estão restritas à segurança de sistemas ou mesmo à tecnologia da informação. Por isso, sua aplicação pode ser estendida a diversas áreas, como, por exemplo, meio ambiente e saúde. Seguindo essa mesma linha abrangente, está a norma ISO 3100. Por isso, a similaridade entre as duas é inevitável.

As normas AS/NZ4360 e ISO 3100 definem o processo de gestão de riscos por meio de 7 elementos (ou fases) principais, conforme ilustrado na Figura 1.4: comunicar e consultar; estabelecer o contexto; identificar os riscos; analisar os riscos; avaliar os riscos; tratar os riscos; e monitorar e rever.

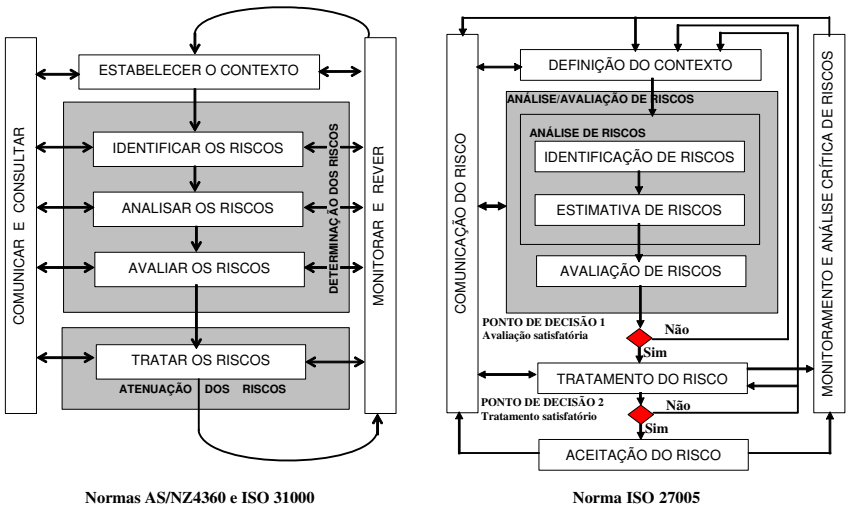

Figura 1.4. Visão Geral do Processo de Gestão de Riscos

Como pode ser observado na Figura 1.4, o processo da norma ISO 27005 traz uma pequena variação dos termos. São indicados dois pontos de decisão nos quais o processo pode ser revisto e uma nova fase de aceitação do risco. Uma contribuição significativa ao processo de gestão de riscos foi feita com a inclusão nos anexos de exemplos e métodos para a identificação de ameaças, além de modelos de análise e avaliação dos riscos.

Outra diferença é o alinhamento com a norma ISO 27001, principalmente em relação ao modelo PDCA. Dentro do modelo PDCA, as etapas da gestão de riscos são divididas nas quatro fases, conforme ilustrado na Figura 1.5. Na fase de planejamento (*Plan*) são agrupadas as etapas: de Definição do Contexto, de Análise/Avaliação de Ris-

cos, de Definição do Plano de Tratamento do Risco e de Aceitação do Risco. Na fase de Execução (*Do*) é realizada a implantação do plano de Tratamento do Risco. Na verificação (*Check*) é feito o Monitoramento Contínuo e Análise Crítica do Risco. Finalmente, a Ação (*Act*) envolve manter e melhorar o processo de Gestão de Riscos de Segurança da Informação.

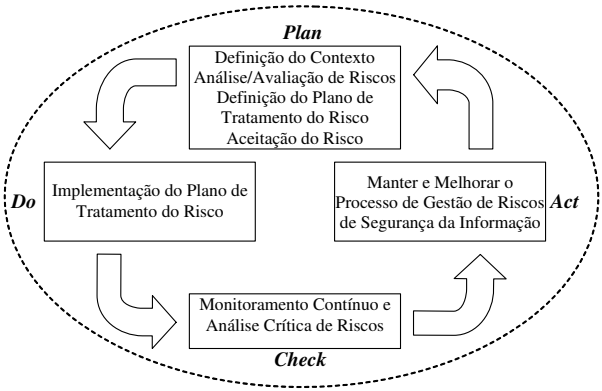

Figura 1.5. Alinhamento do processo do SGSI com o processo de Gestão de Riscos

Cada uma das fases da norma ISO 27005 será apresentada a seguir. Cada fase segue o modelo de procedimento da norma ISO 27001.

1.2.4.1. Comunicação do Risco

A gestão de riscos pode ter diversas partes interessadas. Estas partes devem ser identificadas e seus papéis e responsabilidades delimitados na fase de **Comunicação do Risco**. É importante desenvolver um plano de comunicação que permita a cada uma destas partes conhecer o andamento do processo e fornecer subsídios para seu desenvolvimento.

1.2.4.2. Definição do Contexto

A etapa de **Definição do Contexto** define os parâmetros básicos, por meio dos quais serão identificados os riscos que precisam ser geridos e qual será o escopo do restante do processo de gestão de riscos. Também são definidos os critérios os quais serão utilizados na identificação, avaliação, impacto e aceitação dos riscos.

A definição do contexto tem como entrada todas as informações relevantes sobre a organização, que sejam relevantes para a definição do contexto da gestão de riscos de segurança.

O passo principal para se obter o contexto está na descrição dos objetivos do projeto e dos ambientes nos quais eles estão contextualizados. Outro importante aspecto é a definição dos critérios que serão usados na determinação dos riscos do projeto. Estes

critérios envolvem a determinação das conseqüências de segurança e os métodos usados para a análise e avaliação dos riscos.

1.2.4.3. Identificação de Riscos

A **Identificação de Riscos** é uma das etapas mais críticas, pois os riscos não identificados não serão analisados nem tratados. O objetivo dessa etapa é determinar os eventos que possam causar perdas potenciais e deixar claro como, onde e por que a perda pode ocorrer. A identificação deve conter os riscos que estão e os que não estão sob controle do projeto de pesquisa. Na prática, a identificação de riscos é bem mais complexa, pois as informações, quase sempre, são baseadas em experiências e critérios subjetivos dos próprios responsáveis pelo projeto.

A identificação dos riscos envolve a identificação das ameaças, dos controles existentes, das vulnerabilidades e das conseqüências. Para realizar estas tarefas é desejável uma ampla revisão bibliográfica sobre o assunto, incluindo os objetivos do projeto. Quando há alguma literatura científica sobre as questões levantadas, tal literatura deve ser avaliada e citada. Se a literatura não é suficiente para a identificação dos riscos, pode ser necessária uma consulta à comunidade científica, como a submissão de trabalhos a congressos e periódicos. As questões levantadas na definição do contexto são revistas e colocadas aos participantes interessados.

Em projetos científicos, as revisões obtidas e a apresentação pública do projeto em congressos científicos também auxiliam na identificação e revisão dos riscos.

1.2.4.4. Estimativa de Riscos

Na etapa da **Estimativa de Riscos**, são produzidos dados que irão auxiliar na decisão sobre quais riscos serão tratados e as formas de tratamento com melhor eficiência de custos. Isso envolve considerações sobre a origem dos riscos, suas conseqüências e as probabilidades de ocorrência dos mesmos. As conseqüências e probabilidades são combinadas para produzir o nível de risco.

Uma metodologia de estimativa pode ser qualitativa ou quantitativa ou uma combinação de ambas, dependendo das circunstâncias. A estimativa qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das potenciais conseqüências e a probabilidade destas conseqüências ocorrerem. A estimativa quantitativa adota uma escala de valores numéricos tanto para conseqüências, quanto para a probabilidade. Na próxima seção será apresentada uma metodologia que combina os dois tipos de estimativas.

1.2.4.5. Avaliação de Riscos

O objetivo da **Avaliação de Riscos** é tomar decisões, baseadas nos resultados da análise de risco (Identificação e Estimativa de Riscos). É necessário definir as prioridades e a real necessidade de tratamento dos riscos analisados. A avaliação envolve a comparação

dos níveis de risco encontrados, com os critérios estabelecidos quando o contexto foi considerado.

Convém que sejam consideradas as propriedades da segurança da informação e a importância do processo de negócio ou a atividade suportada por um determinado ativo ou conjunto de ativos. No caso de projetos científicos, a avaliação dos riscos deve estar alinhada com os objetivos do projeto.

Ao término da avaliação é verificado se seu resultado é satisfatório. Caso não seja, uma nova rodada da Análise/Avaliação dos riscos deve ser empreendida, a partir da revisão e possível redefinição do contexto.

1.2.4.6. Tratamento do Risco

O **Tratamento do Risco** envolve a identificação de opções de tratamento, avaliação destas opções e a preparação para a implementação dos tratamentos selecionados. Esta etapa é equivalente à etapa de atenuação de riscos da especificação SP800-30.

O tratamento inicia com uma lista de riscos ordenados por prioridade, conforme os critérios de avaliação dos riscos, associados aos possíveis cenários de incidentes que os provocam.

A cada um dos riscos são relacionadas as opções de tratamento. Há quatro opções possíveis para o tratamento do risco: redução, retenção, evitação e transferência.

Ao término do tratamento são identificados os riscos residuais. Se tais riscos não forem aceitáveis, os tratamentos podem ser refeitos ou, ainda, todo o processo de gestão de riscos pode ser revisto.

1.2.4.7. Aceitação do Risco

A aceitação do risco é feita a partir da análise do risco residual. É conveniente que a decisão de aceitar os riscos seja formalmente registrada, junto com a responsabilidade pela decisão. Infelizmente, nem sempre os riscos residuais estão de acordo com o idealizado no início do processo. Porém, fatores como tempo e custos podem justificar a aceitação dos riscos.

1.2.4.8. Monitoramento e Análise Crítica dos Riscos

O **Monitoramento e Análise Crítica dos Riscos** são partes essenciais da gestão de riscos. Os riscos não são estáticos e devem ser monitorados a fim de verificar a eficácia das estratégias de implementação e mecanismos de gerenciamento utilizados no tratamento dos riscos. Portanto, o processo de monitoramento deve ser contínuo e dinâmico. Além do monitoramento contínuo, mudanças organizacionais ou externas podem alterar o contexto da análise, levando a uma revisão completa da gestão de riscos. Revisões também podem ser iniciadas periodicamente ou realizadas por terceiros.

Cada estágio do processo de gestão de riscos deve ser documentado de forma apropriada. Suposições, métodos, origens de dados, análises, resultados e justificativas das decisões tomadas devem ser registrados. Os relatórios produzidos devem ser o mais sucintos e objetivos quanto possível.

1.3. Estimando os Riscos

Todo risco tem um custo e este custo pode ser quantificado de forma mais ou menos precisa [Blakley et al. 2001]. A mensuração de riscos é bastante comum na área econômica. Porém, pouco adotada na segurança de sistemas de tecnologia da informação.

Conforme definido na primeira seção, o risco pode ser representado matematicamente como uma função da probabilidade de uma origem de ameaça explorar uma vulnerabilidade potencial e o impacto resultante deste evento adverso.

A probabilidade de um evento ocorrer durante um período de tempo determinado é expressa por um número entre zero e um. Quanto maior for o período de tempo considerado, maior será a probabilidade.

Em geral, em um sistema com múltiplas vulnerabilidades, para fins de cálculo, cada vulnerabilidade é considerada como um evento discreto. Ou seja, a probabilidade de um evento ocorrer para determinada vulnerabilidade independe da ocorrência ou não de outro evento.

As probabilidades normalmente são calculadas por meio de análises de dados de ataques ou ameaças. Tais dados podem ser obtidos por experiências na própria empresa ou por coletâneas adquiridas de organizações especializadas.

A norma ISO 27005 traz de forma didática algumas abordagens para a estimativa dos riscos de segurança da informação. Estas abordagens se assemelham às que são sugeridas pelas normas AS/NZ4360 e NIST SP800-30, apresentadas na seção anterior. Apesar das excelentes recomendações contidas nestes documentos, não é apresentada uma metodologia objetiva que possa, de fato, auxiliar o gestor de segurança na tarefa de identificar e mensurar os riscos em um ambiente real.

Para o cálculo do impacto de possíveis vulnerabilidades, é aconselhável a adoção de uma metodologia padronizada e conhecida, como o *Common Vulnerability Scoring System* (CVSS)[7]. Essa metodologia permite ao gestor de segurança da informação calcular os riscos que uma vulnerabilidade inflige no ambiente real da empresa, sem que sejam necessários dados estatísticos precisos sobre ataques anteriores ou análises financeiras complexas. Basta para isso haver um inventário atualizado dos ativos, sistemas e serviços de TI. Tal metodologia será detalhada a seguir.

[7] http://www.first.org/cvss/

1.3.1. Common Vulnerability Scoring System (CVSS)

O CVSS é adotado pelo NIST para a classificação de vulnerabilidades no *National Vulnerability Database* (NVD)[8]. A base de dados de vulnerabilidades NVD é integrada *ao Common Vulnerabilities and Exposures* (CVE)[9] [Mell and Grance 2002].

A metodologia do CVSS utiliza uma série de parâmetros e calcula uma pontuação (*score*) que irá definir o grau de risco de uma determinada vulnerabilidade. São utilizados critérios qualitativos para a caracterização das vulnerabilidades. Tais critérios são agrupados em três áreas: métricas básicas, métricas temporais e métricas ambientais. As métricas básicas contêm todas as características que são intrínsecas e fundamentais para determinada vulnerabilidade e que são invariáveis ao longo do tempo ou em ambientes diferentes. As métricas temporais contêm as características que podem mudar ao longo do tempo. No grupo da métricas ambientais estão as características que são atreladas a implementações e ao ambiente. As características são valoradas e processadas para obter uma pontuação final ajustada, que irá representar as ameaças que uma vulnerabilidade apresenta em determinado instante de tempo para um ambiente específico. A pontuação representa um valor entre 0 (sem riscos) e 10 (maior risco). O NIST realiza uma classificação de riscos[10] das vulnerabilidades baseado nesta pontuação: Baixo (valor entre 0 e 3), Médio (valor entre 4 e 7) e Alto (valor acima de 7).

1.3.1.1. Métricas Básicas

O grupo base de características é composto de seis critérios, conforme ilustrado na Figura 1.6. Estes critérios estão divididos em dois grupos: Impacto e Complexidade. O grupo do Impacto é composto pelo impacto na confidencialidade (CI), impacto na integridade (II) e impacto na disponibilidade (AI).

As métricas de **confidencialidade (CI)**, **integridade (II)** e **disponibilidade (AI)** medem o grau de impacto em cada um destes requisitos de segurança, caso a vulnerabilidade seja explorada. O impacto pode ser completo se houver comprometimento total do requisito. Pode ser parcial se houver danos consideráveis sem que haja controle total do que possa ser obtido, modificado ou totalmente interrompido. O impacto também pode ser nenhum.

O Impacto é calculado de acordo com a seguinte fórmula:

$$\textbf{Impacto} = 10{,}41 * (1 - (1 - CI) * (1 - II) * (1 - AI))$$

No grupo da Complexidade, há outros três critérios. O **vetor de acesso (AV)** identifica se a vulnerabilidade pode ser explorada tanto localmente, quanto por redes remotas (classificação Rede Remota); se pode ser explorada localmente e por uma rede adjacente, mas não de uma rede remota (Rede Adjacente); ou ainda se requer acesso físico ou *login* autenticado no sistema alvo (classificação Local). A métrica de **autenticação (AU)**

[8] http://nvd.nist.gov/
[9] http://cve.mitre.org/
[10] http://nvd.nist.gov/cvss.cfm

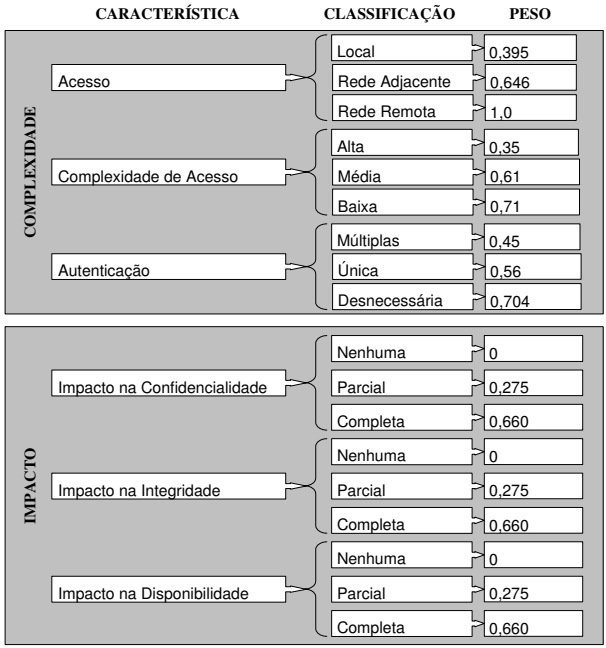

Figura 1.6. Métricas Básicas, conforme o CVSS

verifica o tipo de autenticação necessária pelo atacante no sistema alvo para que a vulnerabilidade seja explorada. A métrica pode ser classificada como: múltipla, se o atacante precisa se autenticar mais de uma vez; autenticação única; ou autenticação desnecessária.

A **complexidade de acesso (AC)** mede o esforço necessário para explorar a vulnerabilidade. Se forem necessárias circunstâncias muito específicas ou condições especiais de acesso, a complexidade é considerada alta. Se somente algumas circustâncias são necessárias para a exploração da vulnerabilidade, a complexidade é média. Se não existem circunstâncias especiais, a complexidade é baixa.

A Complexidade é calculada de acordo com a seguinte fórmula:

$$\textbf{Complexidade} = 20 * AC * AU * AV$$

Para calcular a pontuação, é utilizada a seguinte fórmula sobre os valores atribuídos a cada vulnerabilidade, de acordo com suas características:

$$\textbf{Risco Básico} = (0{,}6 * \text{Impacto} + 0{,}4 * \text{Complexidade} - 1{,}5) * f(\text{Impacto})$$

O Fator de Impacto, **f(Impacto)**, terá o valor 0 (zero) se o Impacto for igual a zero. Caso contrário, receberá o valor 1,176.

1.3.1.2. Métricas Temporais

O grupo temporal é formado por três variáveis: **Explorabilidade (EX)**, o **Nível de Remediação (RL)** e o **Grau de Confiança (RC)**. A Figura 1.7 ilustra estas variáveis e seus pesos.

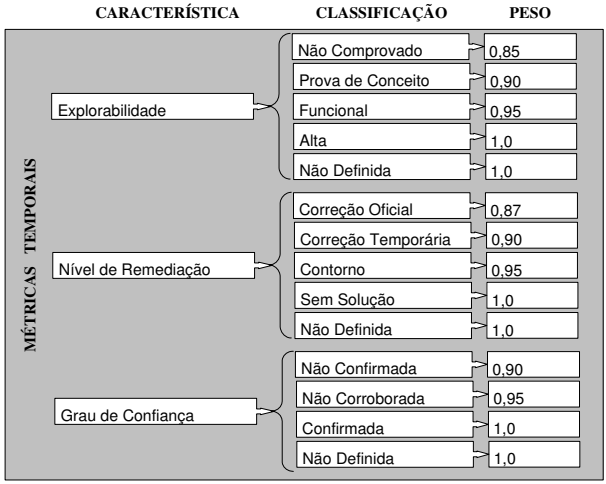

Figura 1.7. Métricas Temporais, conforme o CVSS

A Explorabilidade indica se é ou não possível explorar a vulnerabilidade. Essa variável pode ser classificada como: Não Comprovada, se não há uma ferramenta de exploração (*exploit*) conhecida; Prova de Conceito, se foi criada uma prova da vulnerabilidade; Funcional, quando há um *exploit* desenvolvido; ou Alta, se há relatos de exploração.

No Nível de Remediação é informado se há tratamentos conhecidos para a vulnerabilidade. Tais tratamentos podem ser: uma Correção Oficial do fabricante; uma Correção Temporária fornecida pelo fabricante; um Contorno ao problema; ou Sem Solução disponível.

A credibilidade da divulgação da vulnerabilidade é refletida no Grau de Confiança da existência da mesma. Essa confiança pode ser representada como Não Confirmada, quando há um único relato; Não Corroborada, quando há vários relatos não oficiais; ou Confirmada, quando é reconhecida pelo fabricante.

Caso alguma métrica temporal não seja adotada no cálculo, deve ser classificada como Não Definida.

O cálculo do risco temporal é medido pela seguinte fórmula:

Risco Temporal = Risco Básico * EX * RL * RC

1.3.1.3. Métricas Ambientais

Nem todas as vulnerabilidades são potencialmente perigosas para uma empresa. Para identificar possíveis riscos, é necessário verificar se a tecnologia vulnerável é adotada e quais os possíveis danos que a exploração da vulnerabilidade pode causar. As métricas ambientais têm por objetivo calcular o impacto da vulnerabilidade no ambiente da empresa. A Figura 1.8 ilustra as variáveis ambientais e seus pesos.

Figura 1.8. Métricas Ambientais, conforme o CVSS

A primeira métrica ambiental mede o **Potencial Dano Colateral (CD)** da exploração da vulnerabilidade, representando o risco de danos físicos a ativos ou a perda de vidas. Os danos são classificados em cinco graus diferentes, podendo ser: Nenhum; Baixo, se há danos físicos, perda de lucros ou de produtividade leves; de Baixo a Médio, com danos físicos, perda de lucros ou de produtividade moderados; de Médio a Alto, se houver danos físicos, perda de lucros ou de produtividade significativos; Alto, quando há a possibilidade de danos físicos, perda de lucros ou de produtividade catastróficos.

A segunda métrica indica a **Distribuição dos Alvos (TD)** que podem ser afetados, em termos percentuais, no ambiente empresarial, de acordo com a seguinte classificação: Baixo, entre 1% e 25%; Média, entre 26% e 75%; Alta, acima de 75%; e Nenhum, se não houver sistemas suscetíveis à vulnerabilidade ou estão restritos a ambientes de laboratório muito específicos.

Há ainda outras três métricas, que customizam os cálculos, de acordo com a importância, para a empresa, dos ativos afetados, em relação aos **Requisitos de Segurança**. Essa importância é medida em termos do **Requisito de Confidencialidade (CR)**, do **Requisito de Integridade (IR)** e do **Requisito de Disponibilidade (AR)**. O impacto da perda de cada um dos requisitos pode ser classificada como Baixa, Média ou Alta.

Caso alguma métrica ambiental não seja adotada no cálculo, deve ser classificada como Não Definida.

Se aplicada, a métrica ambiental irá ser combinada com a métrica temporal para calcular o Risco Ambiental. Para isso, o Ajuste Temporal deve ser buscado. O Ajuste Temporal é obtido, conciliando o impacto de cada requisito de segurança ao ambiente, usando a seguintes fórmulas:

Ajuste Temporal = Risco Temporal recalculado, substituindo o Risco Básico pelo Impacto Ajustado

Impacto Ajustado = min (10, 10,41 * (1 - (1 - CI*CR) * (1 - II*IR) * (1 - AI*AR)))

Finalmente, o Risco Ambiental será medido pela seguinte fórmula:

Risco Ambiental = ((Ajuste Temporal + (10 - Ajuste Temporal) * CD) * TD)

1.3.2. Exemplo de Aplicação dos Cálculos

O uso do CVSS aplicado pelo NVD possibilita localizar todas as vulnerabilidades associadas a: ambientes de desenvolvimento, linguagens de programação, servidores Web, sistemas operacionais e outras ferramentas usadas no protótipo, de acordo com o produto, a versão e o vendedor, permitindo calcular com precisão os níveis de risco. Também estão disponíveis todas as opções de tratamento para as vulnerabilidades listadas. Para a determinação do nível de risco basta pesquisar pelo produto no CVSS.

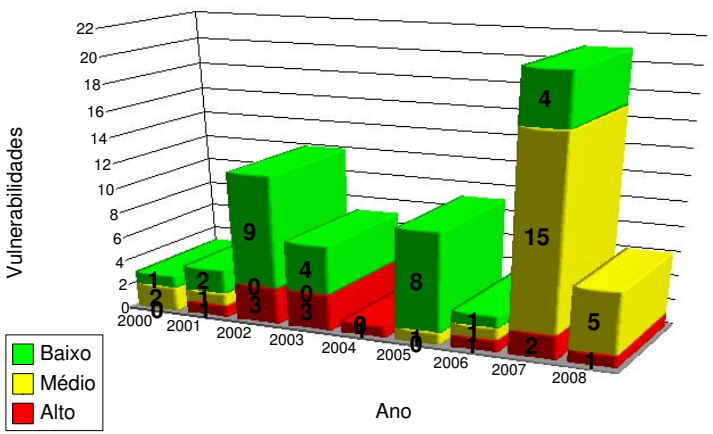

Figura 1.9. Níveis de risco das vulnerabilidades do servidor Tomcat

Tomando como exemplo a quantidade de vulnerabilidades registradas no NVD para o servidor Web *Tomcat*, foi formulado o gráfico da Figura 1.9, refletindo as características temporais de quando foram classificadas pelo NIST. No nível de risco fornecido

pelo NVD, as métricas temporais são consideradas como "Não Definidas"e não é computado o impacto ambiental.

Usando ainda como exemplo o servidor Web *Tomcat*, localizamos a vulnerabilidade *CVE-2008-1947*[11], reportada em 04/06/2008. Essa vulnerabilidade, se explorada, permite a injeção de código malicioso por meio de um parâmetro.

A vulnerabilidade em questão, possui as seguintes características de risco:

- Vetor de Acesso (AV) = Remota = 1,0
- Complexidade de Acesso (AC) = Média = 0,61
- Autenticação (AU) = Desnecessária = 0,704
- Impacto na Confidencialidade (CI) = Nenhuma = 0
- Impacto na Integridade (II) = Parcial = 0,275
- Impacto na Disponibilidade (AI) = Nenhuma = 0
- Métricas Temporais = Não Definidas = 1
- Potencial Dano Colateral (CD) = Baixo = 0,1
- Distribuição dos Alvos (TD) = 5% = 0,25
- Requisito de Disponibilidade (AR) = Alta = 1,51
- Requisito de Integridade (IR) = Alta = 1,51
- Requisito de Confidencialidade (CR) = Alta = 1,51

Calculando o Impacto:

$$\textbf{Impacto} = 10{,}41 * (1 - (1 - CI) * (1 - II) * (1 - AI)) =$$
$$10{,}41 * (1 - (1 - 0) * (1 - 0{,}275) * (1 - 0)) = 2{,}9$$

Calculando a Complexidade:

$$\textbf{Complexidade} = 20 * AC * AU * AV =$$
$$20 * 1 * 0{,}61 * 0{,}704 = 8{,}6$$

Finalmente pode ser calculado o nível de Risco Básico, usando o fator de impacto de valor 1,176:

$$\textbf{Risco Básico} = (0{,}6 * \text{Impacto} + 0{,}4 * \text{Complexidade} - 1{,}5) * f(\text{Impacto}) =$$
$$(0{,}6 * 2{,}86 + 0{,}4 * 8{,}59 - 1{,}5) * 1{,}176 = 4{,}3$$

O valor **4,3** corresponde ao Risco Básico **Médio**.

Para ajustar os riscos ao ambiente da empresa, calcula-se então o Impacto Ajustado e o Risco Básico Ajustado:

[11] http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1947

Impacto Ajustado = min(10, 10,41 * (1 - (1 - CI*CR) * (1 - II*IR) * (1 - AI*AR))) =
min(10, 10,41 * (1 - (1 - 0 * 1,51) * (1 - 0,275 * 1,51) * (1 - 0 * 1,51))) = 4,3

Risco Básico Ajustado = (0,6 * 4,3 + 0,4 * 8,59 - 1,5) * 1,176 = 5,3

Com as variáveis da métrica temporal Não Definidas, o Risco Temporal e o Risco Temporal Ajustado são iguais:

Risco Temporal = Risco Básico * EX * RL * RC =
5,3 * 1 * 1 * 1 = 5,3

Resta agora calcular o Risco Ambiental:

Risco Ambiental = ((Ajuste Temporal + (10 - Ajuste Temporal) * CD) * TD) =
((5,3 + (10 - 5,3) * 0,1) * 0,25) = 1,4

Como se pode perceber, apesar do Risco Básico ser alto, quando a vulnerabilidade é avaliada no ambiente da empresa, a mesma recebe uma pontuação baixa. Contudo, o inverso também pode ocorrer. Uma vulnerabilidade com Risco Básico baixo pode afetar elementos críticos da empresa e receber uma pontuação de Risco Ambiental alta.

1.3.3. Considerações Sobre o CVSS

O CVSS sofre atualizações periódicas, tanto na classificação das métricas, quanto no seu peso e cálculo. A versão atual do CVSS é a 2.0.

Entre a versão 1.0 e a 2.0 há diferenças consideráveis, principalmente na Métrica Básica. Na primeira versão havia uma variável de tendência de impacto, que permitia atribuir um peso maior a determinado requisito de segurança. O Acesso, a Complexidade de Acesso e a Autenticação possuíam apenas duas classificações. A fórmula de cálculo e os pesos das variáveis também eram bastante diferentes da versão atual.

1.4. Estudo de caso: Gestão de Riscos no Projeto de Composições de IDSs

O aumento da complexidade dos atuais sistemas de detecção de intrusão, com códigos cada vez maiores, interações diversificadas e o uso de componentes externos, torna a tarefa de avaliá-los cada vez mais difícil. Na literatura científica são apresentadas diversas tentativas de avaliar a eficiência de sistemas de detecção de intrusão [Puketza et al. 1996, Debar et al. 1998, Durst et al. 1999, Lippmann et al. 2000a, Lippmann et al. 2000b, McHugh 2000, Athanasiades et al. 2003]. Nestes casos, uma implementação é avaliada por baterias de testes para verificar o comportamento do IDS e suas reações. Porém, nenhuma destas experiências foca o desenvolvimento seguro dos sistemas de detecção de intrusão ou avalia a segurança dos mesmos.

Infelizmente a avaliação de segurança não pode provar que um sistema é invulnerável a ataques, mas somente que o mesmo mostra um certo grau de confiança nos propósitos a que se destina.

A avaliação de segurança em projetos científicos é particularmente difícil, pois os mesmos são freqüentemente desenvolvidos como provas de conceito e não como produtos acabados. Quando um projeto de software científico, como o apresentado neste curso, envolve a integração de múltiplas tecnologias, a identificação e a minimização das vulnerabilidades é ainda mais complicada. Tratar este tipo de projeto apenas no ponto de protótipo pode ser extremamente dispendioso e, em alguns casos, os resultados podem inviabilizar o próprio projeto.

Nesta seção adotamos a metodologia de gestão de riscos para o acompanhamento e a avaliação dos requisitos de segurança envolvidos em um projeto de Composições de Sistemas de Detecção de Intrusão em ambientes de larga-escala [Brandão 2007]. A metodologia apresentada nessa seção foi inicialmente baseada na norma AS/NZ4360 e posteriormente adaptada para o padrão ISO 27005. Na avaliação original foi adotada a versão 1.0 do CVSS, que também foi atualizada nessa seção, para a versão 2.0.

Nessa seção são apresentados todos os passos da metodologia, ilustrados com a documentação contendo o resultado da aplicação da mesma no desenvolvimento do projeto.

1.4.1. Comunicação do Risco

No desenvolvimento de pesquisas acadêmicas, podem ser identificados pelo menos cinco tipos de papéis associados aos interessados no projeto de pesquisa:

1. **Membros do projeto de pesquisa** – pessoas diretamente relacionadas ao desenvolvimento do projeto;
2. **Membros do grupo de pesquisa** – pessoas que pertencem ao mesmo grupo de pesquisa, mas não estão diretamente relacionados à pesquisa em desenvolvimento;
3. **Comunidade científica** – pessoas interessadas nos resultados da pesquisa, como membros de comitês de programa e revisores de simpósios e periódicos, participantes de congressos científicos e leitores dos trabalhos publicados;
4. **Instituições e órgãos de pesquisa** – instituições e órgãos de pesquisa aos quais o projeto de pesquisa está vinculado;
5. **Instituições e órgãos de fomento** – responsáveis pelo custeio do projeto.

Para a elaboração do plano de comunicação e consulta, neste projeto de pesquisa foram considerados apenas os três primeiros papéis, conforme a Tabela 1.1. Para cada papel (participantes) são traçados os objetivos da consulta e comunicação, a perspectiva dos participantes na consulta, os métodos utilizados e como serão avaliados os resultados obtidos.

1.4.2. Definição do Contexto

Nesta etapa cabe inicialmente definir o projeto, seu escopo e seus objetivos.

As composições de IDSs [Brandão et al. 2006a, Brandão et al. 2006b, Brandão 2007] envolvem a combinação de diversos sistemas de monitoramento que coletam e analisam dados de forma distribuída e oferecem a flexibilidade da configuração dinâmica para atender a novas situações, mesmo que temporárias. As composições

Tabela 1.1. Plano de comunicação e consulta

Objetivos	Participantes	Perspectivas dos Participantes	Métodos Usados	Avaliação
Estabelecimento de diretrizes e revisão contínua do projeto	Membros do projeto de pesquisa	Processo contínuo de avaliação dos riscos	Reuniões periódicas e apresentação de relatórios técnicos.	Auto-avaliação
Identificação de possíveis falhas, troca de experiências e obtenção de críticas e sugestões	Membros do grupo de pesquisa	Conhecimento de novas tecnologias	Seminários e encontros.	Análise periódica das contribuições apresentadas.
Obtenção de críticas e sugestões, identificação de novas aplicações, troca de experiências e avaliação do projeto	Comunidade científica	Divulgação e conhecimento de novas tecnologias	Submissão de artigos científicos para prospecção, publicação de resultados e apresentação de artigos.	Compilação e análise das revisões, sugestões e críticas dos artigos.

de IDSs, nesta abordagem, fazem uso extensivo de esforços de padronização e estão fundamentadas em uma infra-estrutura de serviços e suportes. A adoção destes padrões torna possível a interoperabilidade e a comunicação entre elementos de uma composição e, mesmo, entre IDSs completos. Os IDSs materializados a partir da infra-estrutura proposta seguem a arquitetura orientada a serviços suportada pela tecnologia de *Web Services* [W3C 2004], com o amplo uso de textos XML [Bray et al. 2004].

1.4.2.1. Definição dos Objetivos

Tomando como base os requisitos do projeto de pesquisa, foram identificados e descritos cinco objetivos iniciais:

O1: **Detecção de Intrusão Distribuída**
O2: **Uso de Elementos Heterogêneos**
O3: **Composição Dinâmica de IDSs**
O4: **Adoção de Padrões de Interoperabilidade**
O5: **Segurança dos Elementos e da Composição**

No restante do texto, tais objetivos serão referenciados com a ordem e numeração apresentada acima (O1, O2, O3 e O4). A análise do Objetivo 5 (Segurança) é diluída entre os demais objetivos.

A determinação dos ambientes de desenvolvimento e execução do projeto tem por objetivo identificar os riscos desses ambientes que possam afetar os objetivos da pesquisa. No estudo de caso, por se tratar de um projeto envolvendo redes de larga escala, são considerados os ambientes interno e externo.

1.4.2.2. Definição dos Critérios Básicos

São definidas abaixo, as conseqüências da exploração de determinada ameaça à segurança, que possam afetar os objetivos do projeto. Essas conseqüências serão utilizadas para a identificação e a análise dos riscos de segurança do projeto.

- **Confidencialidade** - Informações críticas são reveladas a usuários não autorizados

- **Integridade** - Informações críticas são alteradas ou eliminadas por usuários não autorizados
- **Disponibilidade** - Elementos de software ou hardware têm sua performance reduzida ou seu funcionamento interrompido.

Podemos resumir o processo de identificação dos possíveis fatores de riscos, ao conjunto de respostas a três questões: qual é a **ameaça** (exploração de vulnerabilidades); **o que pode ocorrer** (conseqüências); e **como pode ocorrer** (ataque).

Para o cálculo dos riscos, nesse projeto adotamos a metodologia *Common Vulnerability Scoring System* (CVSS)[12], usada pelo NIST para a classificação de vulnerabilidades no *National Vulnerability Database* (NVD)[13]. A base de dados de vulnerabilidades NVD é integrada *ao Common Vulnerabilities and Exposures* (CVE)[14] [Mell and Grance 2002].

Para a análise de riscos de segurança do projeto, foi adotado apenas o grupo base de critérios de caracterização de vulnerabilidades, já que não estão sendo tratadas vulnerabilidades em softwares específicos.

Serão aceitos como riscos residuais os riscos Baixos. Os riscos Médios, cujos controles para sua redução sejam Altos, também poderão ser aceitos.

1.4.3. Identificação de Riscos

Para identificar as vulnerabilidades associadas ao projeto foi efetuada uma ampla revisão bibliográfica sobre o assunto. As revisões obtidas e a apresentação pública do projeto em congressos científicos auxiliaram na identificação e revisão dos riscos. Usando também a literatura relacionada aos objetivos foi possível identificar possíveis ameaças, o que pode ocorrer (conseqüências), como podem acontecer e quais os possíveis tratamentos.

A seguir, os riscos são separados de acordo com os objetivos. Cabe ressaltar que os controles identificados sugerem os possíveis métodos de tratamento dos riscos e não uma solução ou tecnologia específica.

1.4.3.1. Sistemas de Detecção de Intrusão Distribuídos

Na primeira identificação representada na Tabela 1.2, foram consideradas as ameaças associados aos sistemas de detecção de intrusão distribuídos. As ameaças e vulnerabilidades a tais IDSs são conhecidas na literatura, facilitando a determinação dos riscos e possíveis tratamentos. Nesta identificação, destacamos os trabalhos [Lindqvist and Jonsson 1998], [Ptacek and Newsham 1998], [Mell et al. 2000], [Dacier 2002], [Yegneswaran et al. 2004] e [Yu and Frincke 2004].

[12] http://www.first.org/cvss/
[13] http://nvd.nist.gov/
[14] http://cve.mitre.org/

Tabela 1.2. Registro de riscos: IDSs distribuídos

Ameaça	O que pode ocorrer	Como pode ocorrer	Possíveis Controles	Referências
Negação de Serviço	Afeta a disponibilidade do sistema	Desativação de Elementos por ataques diretos, explorando vulnerabilidades	Uso de mecanismos automáticos para detecção de falhas de funcionamento e Reativação automática dos elementos	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Yu e Frincke, 2004]
			Replicação de elementos	
			FIltragem de tráfego	
			Seleção dinâmica de novos elementos	
		Elementos maliciosos enviam grande quantidade de dados falsos	Controle do fluxo e filtragem da quantidade de mensagens que excedam determinado limite	
Mascaramento	Afeta a integridade e privacidade do sistema	Um elemento malicioso pode se passar por um elemento verdadeiro	Autenticação mútua dos elementos	[Yegneswaran et al. 2004]
Ofuscação	Afeta o desempenho do sistema	Elemento malicioso envia grande quantidade de dados falsos para ofuscar o processo de detecção	Controle do fluxo e filtragem da quantidade de mensagens que excedam determinado limite	[Yegneswaran et al. 2004]
		Elemento malicioso envia pequena quantidade de dados falsos para ofuscar o processo de detecção	Mecanismos de correlação de dados eficientes	
		Tentativa de localização (*scanning*) furtiva ou coordenada dos elementos	Controle de acesso nos mecanismos de registro e pesquisa para localização dos elementos	
			Uso do maior número possível de elementos a fim de detectar tentativas de *scanning*	
Ataque de Inserção	Afeta o desempenho do sistema	O IDS aceita pacotes que são rejeitados pelo sistema alvo. Atacante envia pacotes diretamente ao sensor a fim de iludi-lo.	Uso de sensores baseados em aplicação	[Ptacek and Newsham 1998] [Yu e Frincke, 2004]
			Uso de diversidade de sensores	
Ataque de Evasão	Afeta o desempenho do sistema	O sistema alvo aceita pacotes que o IDS rejeita. Atacante envia pacotes truncados ou com uma ordem trocada para iludir o sensor	Uso de sensores baseados em aplicação	[Ptacek and Newsham 1998] [Yu e Frincke, 2004]
			Uso de diversidade de sensores	
Espionagem	Afeta a confidencialidade do sistema	Atacantes interceptam as mensagens de alerta trocadas entre os elementos de IDS	Uso de canais de comunicação exclusivos	[Mell et al 2000] [Dacier 2002]
			Uso de criptografia	
		Elementos comprometidos são usados para coletar e enviar informações sigilosas	Controle de transmissão	[Lindqvist and Jonsson 1998]
Filtragem de Alertas	Afeta o desempenho, a integridade e a confidencialidade do sistema	Atacantes interceptam mensagens com alertas sobre suas atividades, descartando-as, redirecionando-as ou alterando-as seletivamente	Associação de criptografia e assinatura de mensagens	[Dacier 2002]
Interrupção ou desvio de conexão (*hijacking*)	Afeta o desempenho, a integridade e a confidencialidade do sistema	Atacantes interceptam ou desviam uma conexão entre elementos de IDS	Uso de canais seguros, com criptografia e controle de seção	[Dacier 2002]
Comprometimento de Elementos de IDS	Afeta o desempenho, a integridade e a confidencialidade do sistema	Atacantes alteram o código ou a configuração do elemento	Replicação de elementos em diversas plataformas e comparação de alertas	[Dacier 2002] [Yu e Frincke, 2004]

Tabela 1.3. Registro de riscos: elementos heterogêneos

Ameaça	O que pode ocorrer	Como pode ocorrer	Possíveis Controles	Referências
Elementos vulneráveis	Atacantes exploram vulnerabilidades conhecidas de um determinado elemento de IDS	Falhas de *design* e implementação	Aplicação de técnicas de tolerância à intrusão, com uso de diversidade de software	[Lindqvist and Jonsson 1998]
			Atualização continua com a aplicação de correções	
Códigos maliciosos são introduzidos no elemento.	Afeta a integridade e confidencialidade	Não realização de processo de validação do software no momento da aquisição	Validação do software, verificando se ele está de acordo com os requisitos de segurança necessários	[Lindqvist and Jonsson 1998] [Han e Zheng, 2000]
		Interceptação e adulteração durante o processo de entrega do software	Autenticação da origem e uso de canais seguros de entrega	
Confiar em elementos não confiáveis	Inclusão de novas Vulnerabilidades	Elemento não foi projetado para funcionar de forma segura	Limitar o uso a processos sem requisitos de segurança	[Lindqvist and Jonsson 1998]
			Confinamento a ambientes que forneçam segurança ao elemento	
Dificuldade de Gerenciamento	Falhas de operação	Falhas de instalação e de configuração	Aplicação de técnicas e protocolos padronizados de gerenciamento. Qualificação de recursos humanos	[Lindqvist and Jonsson 1998]
	Aumento dos custos operacionais	Altos custos para administrar e manter atualizada uma base de software e hardware muito heterogênea		
	Inclusão de novas Vulnerabilidades	Atualizações inseguras		
		Efeitos inesperados		
		Backdoors de gerenciamento		
Dificuldade de Interoperabilidade	Falha de comunicação	Os elementos utilizam protocolos de comunicação ou formatos de mensagens incompatíveis	Estabelecimento de um formato padrão de comunicação	[Bass 2004]
	Inclusão de novas vulnerabilidades	Níveis de segurança diferentes entre os elementos	Políticas de segurança com um nível mínimo de segurança que deverá ser comum a todos os elementos	[Lindqvist and Jonsson 1998]

1.4.3.2. Elementos de Detecção de Intrusão Heterogêneos

O segundo objetivo a ter seus riscos identificados é o uso de elementos heterogêneos de detecção de intrusão ou de comunicação entre diferentes IDSs, conforme ilustrado na Tabela 1.3. Por se tratar de uma área nova de pesquisa, não há estudos específicos sobre tal assunto. Adaptando o modelo de análise de segurança para composições de software proposto em [Han and Zheng 2000], identificamos os riscos associados: à segurança dos componentes, à arquitetura do sistema composto e ao processo de design da arquitetura e da composição.

Como a proposta do projeto prevê o uso de ferramentas previamente existentes, mesmo que de diferentes fabricantes, consideramos, principalmente, os riscos relacionados ao uso de softwares prontos (*commercial off-the-shelf – COTS*) [Lindqvist and Jonsson 1998]. Também foram identificadas ameaças na comunicação entre elementos independentes de detecção de intrusão [Bass 2004].

Tabela 1.4. Registro de riscos: composição dinâmica de IDSs

Ameaça	O que pode ocorrer	Como pode ocorrer	Possíveis Controles	Referências
Dificuldade de localização e escolha dos elementos	Falha no processo de descoberta dos componentes	Incompatibilidade nas descrições dos componentes	Uso de linguagens e ferramentas de descrição padronizadas	[Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]
		Falhas na caracterização das interfaces		
		Descrições imprecisas dos componentes	Uso de taxonomias, ontologia e semântica para caracterização dos componentes	
Elementos indisponíveis	Indisponibilidade no momento da criação ou reconfiguração da composição	Falha nos mecanismos de busca	Mecanismos de busca distribuída e replicação de informações	
		Falha nos componentes	Redundância, mecanismos de detecção de falhas e mecanismos de reativação automática	
Redução da confiabilidade da composição	Afeta a integridade, a confidencialidade e a disponibilidade do sistema	Novo elemento altera as características de segurança da composição	Definir os requisitos de segurança da composição e avaliar os requisitos de segurança do elemento antes de incluí-lo na composição	[Charfi e Mezini, 2005] [Feiertag et al., 2000a, 2000b] [Frincke, 2000]
Exposição de informações confidenciais	Afeta a confidencialidade do sistema	Informações confidenciais são repassadas a novos elementos que não possuem autorização para recebê-las	Definir mecanismos que permitam filtrar e retransmitir informações que estejam de acordo com a política de segurança da composição e dos seus elementos	[Feiertag et al., 2000a, 2000b] [Frincke, 2000]
Negação de Serviço	Afeta a disponibilidade do sistema	Um elemento provedor de serviço aceita mais requisições de serviço do que é capaz de atender	Controlar e limitar o número de requisições	[Feiertag et al., 2000b]
		Um elemento cliente de serviço recebe mais mensagens do que é capaz de processar	Controlar o número de mensagens recebidas e renegociar com os elementos provedores de serviço	

1.4.3.3. Composição Dinâmica de IDSs

A maioria das ameaças pertinentes à composição dinâmica estão relacionadas à composição de serviços [Esfandiari and Tosic 2004][Esfandiari and Tosic 2005] [Wang et al. 2004] [Charfi and Mezini 2005]. Os trabalhos [Feiertag et al. 2000] e [Frincke 2000] auxiliam na identificação dos requisitos de IDSs dinâmicos e das etapas de composição. Novas questões são identificadas a partir destas informações: a disponibilização de elementos de IDSs; a localização desses elementos; a escolha dos elementos; e a reconfiguração da composição. Cada uma dessas questões possui problemas e riscos específicos que foram agrupados na Tabela 1.4.

1.4.3.4. Padrões de Interoperabilidade

O quarto escopo a ser analisado é bastante amplo, pois são combinados o uso de padrões de interoperabilidade com a aplicação da linguagem XML e o uso de *Web Services*. Cada uma dessas questões merece uma análise separada.

Tabela 1.5. Registro de riscos: adoção de padrões

Ameaça	O que pode ocorrer	Como pode ocorrer	Possíveis Controles	Referências
Dificuldade de interoperabilidade	O sistema não consegue integrar com novos elementos de IDS ou de fabricantes distintos	A especificação usada não se torna um padrão	Não adotar especificações muito incipientes	[Parastatidis and Webber 2004]
		Os padrões adotados não são compatíveis entre si.	Adotar padrões que reconhecidamente sejam compatíveis, como os relacionados no WS-Interoperability Profile	
		Alto custo de integração dos padrões		
		Os padrões dependem da tecnologia adotada ou são disponibilizados por um único fabricante	Adotar padrões que sejam independentes de tecnologia	
		O padrão adotado no projeto pode não ser adotado pelo mercado	Usar somente padrões de organizações conhecidas e associadas mercado, como o IETF, OASIS e W3C	
Dificuldade de Implementação	A composição não pode ser implementada em determinados ambientes	Componentes, ferramentas e implementações dos padrões não são completamente compatíveis com a especificação original	Evitar o uso de ferramentas e implementações que disponibilizem recursos não compatíveis com o padrão original	
			Utilizar padrões que possuam a maior variedade de implementações possíveis	
			Dar preferência a implementações e ferramentas amplamente utilizadas no mercado	
	Atrasos na implementação	Falta de pessoal qualificado	Qualificação de pessoal	
			Adotar padrões que já possuam ferramentas no mercado e boa documentação	

Como pretendemos adotar padrões de interoperabilidade emergentes, a análise de [Parastatidis and Webber 2004] é bastante esclarecedora. Nela, os riscos associados à adoção de padrões emergentes, principalmente aqueles relacionados aos padrões de Web Services, são identificados e são sugeridas algumas contramedidas. A Tabela 1.5 apresenta tais riscos.

Os riscos da aplicação da linguagem XML em conjunto com a tecnologia de web service são analisados em [Demchenko et al. 2005] e [Yu et al. 2005] e estão representados na Tabela 1.6.

1.4.3.5. Agrupamento dos Riscos

Os riscos similares levantados foram agrupados e os riscos de menor impacto foram excluídos. Após analisar os resultados da fase anterior do processo de gestão de riscos,

Tabela 1.6. Registro de riscos: uso de XML

Ameaça	O que pode ocorrer	Como pode ocorrer	Possíveis Controles	Referências
Sondagem às interfaces dos Web Services	Afeta a confidencialidade do sistema	Atacante identifica interfaces, operações e parâmetros dos serviços que são publicados indevidamente em documentos WSDL ou não estão publicados	Uso de ferramentas de análise de vulnerabilidades para validar os documentos WSDL e as interfaces dos serviços	[Demchenko et al 2005] [Yu et al., 2005]
			Controle de acesso aos documentos WSDL e aos serviços.	
Ataque ao analisador gramatical XML	Afeta a confidencialidade, integridade e disponibilidade do sistema	O analisador gramatical XML é iludido para subjugar a capacidade de processamento ou executar códigos móveis maliciosos	Autenticação, assinatura de mensagens, controle de acesso e análise de conteúdo.	
Conteúdo XML malicioso	Afeta a confidencialidade, integridade e disponibilidade do sistema	Textos XML contém códigos maliciosos que exploram vulnerabilidades ou são executados pelas aplicações		
Ataques por referências externas	Afeta a confidencialidade, integridade e disponibilidade do sistema	Documentos XML contêm ponteiros maliciosos para referências externas que são chamadas ou executadas indevidamente		
Ataques aos protocolos SOAP/XML	Afeta a disponibilidade do sistema (negação de serviço)	Um atacante tenta sobrecarregar o sistema com mensagens SOAP (SOAP *Flooding*)	Autenticação e controle de acesso	
	Afeta a confidencialidade, integridade e disponibilidade do sistema	Mensagens são interceptadas e retransmitidas como se fossem mensagens legítimas (*Replay*)	Uso de *timestamps* nas mensagens e *cache* nos serviços.	
	Afeta a confidencialidade do sistema	Atacantes interceptam mensagens XML (Espionagem)	Uso de Criptografia (*WS-Security*)	
	Afeta a confidencialidade, integridade do sistema	Atacantes interceptam e alteram o conteúdo das mensagens (*Man-in-the-middle*)	Associação de Criptografia e Assinatura de mensagens (*WS-Security*)	
Interferência nas credenciais de segurança XML	Afeta a confidencialidade do sistema	Um atacante pode roubar ou alterar as credenciais dos clientes e serviços	Uso de criptografia na comunicação e de chaves "fortes" nas credenciais. Proteção de credenciais.	
Interferência nas negociações de chaves e seções	Afeta a confidencialidade, integridade e disponibilidade do sistema	Falhas de implementação de segurança, geração de chaves pobres e uso de algoritmos criptográficos fracos ou customizados.	Uso de padrões criptográficos robustos com chaves "fortes".	

verificamos a necessidade de dividi-los em duas categorias: **riscos de segurança** e **riscos operacionais**. Os riscos de segurança referem-se às vulnerabilidades que podem ser exploradas para afetar os requisitos de confidencialidade, integridade e disponibilidade de um sistema de detecção de intrusão de larga escala. Os riscos operacionais não são provocados por vulnerabilidades, mas envolvem decisões que podem afetar o resultado final do projeto de pesquisa.

Alguns eventos, apesar de serem idênticos, são explorados de forma diferente e, portanto, são analisados separadamente. Cada risco recebe uma identificação única que será usada para referenciá-lo nas etapas subseqüentes do processo de gestão de riscos.

Tabela 1.7. Riscos de segurança combinados

Risco	Ameaça	Conseqüências	Como pode ocorrer
RS1.1	Espionagem	Confidencialidade	Atacantes interceptam as mensagens de alerta trocadas entre os elementos de IDS
RS1.2	Espionagem	Confidencialidade	Elementos comprometidos são usados para coletar e enviar informações sigilosas
RS1.3	Negação de Serviço	Disponibilidade	Desativação de Elementos por ataques diretos, explorando vulnerabilidades
RS1.4	Negação de Serviço	Disponibilidade	Elementos maliciosos enviam grande quantidade de dados falsos
RS1.5	Mascaramento	Integridade e Confidencialidade	Um elemento malicioso pode se passar por um elemento verdadeiro
RS1.6	Ataque de Evasão	Disponibilidade	O sistema alvo aceita pacotes que o IDS rejeita. Atacante envia pacotes truncados ou com uma ordem trocada para iludir o sensor
RS1.7	Ataque de Inserção	Disponibilidade	O IDS aceita pacotes que são rejeitados pelo sistema alvo. Atacante envia pacotes diretamente ao sensor a fim de iludi-lo.
RS1.8	Ofuscação	Disponibilidade	Elemento malicioso envia grande quantidade de dados falsos para ofuscar o processo de detecção
RS1.9	Ofuscação	Disponibilidade	Elemento malicioso envia pequena quantidade dados falsos para ofuscar o processo de detecção
RS1.10	Ofuscação	Disponibilidade	Tentativa de localização (*scanning*) furtiva ou coordenada dos elementos
RS1.11	Filtragem de Alertas	Disponibilidade, Integridade e Confidencialidade	Atacantes interceptam mensagens com alertas sobre suas atividades, descartando-as, redirecionando-as ou alterando-as seletivamente
RS1.12	Comprometimento de Elementos de IDS	Disponibilidade, Integridade e Confidencialidade	Atacantes alteram o código ou a configuração do elemento
RS1.13	Interrupção ou desvio de conexão (*hijacking*)	Disponibilidade, Integridade e Confidencialidade	Atacantes interceptam ou desviam uma conexão entre elementos de IDS
RS2.1	Uso de Elementos vulneráveis	Disponibilidade, Integridade e Confidencialidade	Falhas de *design* e implementaçã. Atacantes exploram vulnerabilidades conhecidas de um determinado elemento de IDS
RS2.2	Uso de elementos contendo código malicioso	Disponibilidade, Integridade e Confidencialidade	Não realização de processo de validação do software no momento da aquisição ou de entrega do software
RS2.3	Confiar em elementos não confiáveis	Disponibilidade, Integridade e Confidencialidade	Inclusão de novas Vulnerabilidades. Elemento não foi projetado para funcionar de forma segura
RS2.4	Dificuldade de Gerenciamento	Disponibilidade, Integridade e Confidencialidade	Inclusão de novas Vulnerabilidades. Atualizações inseguras.
RS2.5	Dificuldade de Gerenciamento	Disponibilidade, Integridade e Confidencialidade	Inclusão de novas Vulnerabilidades. Efeitos inesperados
RS2.6	Dificuldade de Gerenciamento	Disponibilidade, Integridade e Confidencialidade	*Inclusão de novas Vulnerabilidades. Backdoors* de gerenciamento
RS2.7	Dificuldade de Interoperabilidade	Disponibilidade, Integridade e Confidencialidade	Inclusão de novas vulnerabilidades. Níveis de segurança diferentes entre os elementos
RS3.1	Exposição de informações confidenciais	Confidencialidade	Informações confidenciais são repassadas a novos elementos que não possuem autorização para recebê-las
RS3.2	Negação de Serviço	Disponibilidade	Um elemento provedor de serviço aceita mais requisições de serviço do que é capaz de atender
RS3.3	Negação de Serviço	Disponibilidade	Um elemento cliente de serviço recebe mais mensagens do que é capaz de processar
RS3.4	Redução da confiabilidade da composição	Disponibilidade, Integridade e Confidencialidade	Novo elemento altera as características de segurança da composição
RS3.5	Elementos indisponíveis	Afeta a integridade e a disponibilidade do sistema	Falha nos mecanismos de busca
RS3.6	Elementos indisponíveis	Afeta a integridade e a disponibilidade do sistema	Falha nos componentes
RS4.1	Sondagem às interfaces dos Web Services	Confidencialidade	Atacante identifica interfaces, operações e parâmetros dos serviços que são publicados indevidamente em documentos WSDL ou não estão publicados
RS4.2	Ataque ao analisador gramatical XML	Disponibilidade, Integridade e Confidencialidade	O analisador gramatical XML é iludido para subjugar a capacidade de processamento ou executar códigos móveis maliciosos
RS4.3	Conteúdo XML malicioso	Disponibilidade, Integridade e Confidencialidade	Textos XML contém códigos maliciosos que exploram vulnerabilidades ou são executados pelas aplicações
RS4.4	Ataques por referências externas	Disponibilidade, Integridade e Confidencialidade	Documentos XML contêm ponteiros maliciosos para referências externas que são chamadas ou executadas indevidamente
RS4.5	Ataques aos protocolos SOAP/XML	Disponibilidade	Um atacante tenta sobrecarregar o sistema com mensagens SOAP (SOAP *Flooding*)
RS4.6	Ataques aos protocolos SOAP/XML	Disponibilidade, Integridade e Confidencialidade	Mensagens são interceptadas e retransmitidas como se fossem mensagens legítimas (*Replay)*
RS4.7	Ataques aos protocolos SOAP/XML	Confidencialidade	Atacantes interceptam mensagens XML (Espionagem)
RS4.8	Ataques aos protocolos SOAP/XML	Confidencialidade e Integridade	Atacantes interceptam e alteram o conteúdo das mensagens (*Man-in-the-middle*)
RS4.9	Interferência nas credenciais de segurança XML	Confidencialidade	Um atacante pode roubar ou alterar as credenciais dos clientes e serviços
RS4.10	Interferência nas negociações de chaves e seções	Disponibilidade, Integridade e Confidencialidade	Falhas de implementação de segurança, geração de chaves pobres e uso de algoritmos criptográficos fracos ou customizados.

A Tabela 1.7 apresenta os riscos de segurança combinados. A Tabela 1.8 apresenta os riscos operacionais combinados.

Tabela 1.8. Riscos operacionais combinados

Item	Ameaça	Conseqüências	Como pode ocorrer
RO2.1	Aumento dos custos operaci onais	Dificuldade de Gerenciamento	Altos custos para administrar e manter atualizada uma base de software e hardware muito heterogênea
RO2.2	Falha de comunicação	Dificuldade de Interoperabilidade	Os elementos utilizam protocolos de comunicação ou formatos de mensagens incompatíveis
RO3.1	Falha no processo de desc oberta dos componentes	Dificuldade de localiz ação e escolha dos el ementos	Incompatibilidade nas descrições dos componen tes e falhas na caracterização das interfaces
RO3.2	Falha no processo de desc oberta dos componentes	Dificuldade de localiz ação e escolha dos el ementos	Descrições imprecisas dos componentes
RO4.1	O sistema não consegue integrar com novos elementos de IDS ou de fabricantes distintos	Dificuldade de interoperabilidade	A especificação usada não se torna um padrão
RO4.2	O sistema não consegue integrar com novos elementos de IDS ou de fabricantes distintos	Dificuldade de interoperabilidade	Os padrões adotados n ão são compat íveis entre si ou o custo de integração é muito alto.
RO4.3	O sistema não consegue integrar com novos elementos de IDS ou de fabricantes distintos	Dificuldade de interoperabilidade	Os padrões dependem da tecnologia adotada ou são disponibiliz ados por um único fabricante
RO4.4	O sistema não consegue integrar com novos elementos de IDS ou de fabricantes distintos	Dificuldade de interoperabilidade	O padrão adotado no projeto pode não ser adotado pelo mercado
RO4.5	A composição não pode ser implementada em determin ados ambientes	Dificuldade de Implementação	Componentes, ferramentas e impleme ntações dos padrões não são complet amente compatíveis com a especificação original
RO4.6	Atrasos na implementação	Dificuldade de Implementação	Falta de pes soal qualificado

1.4.3.6. Agrupamento dos Controles

As técnicas, mecanismos e ferramentas de controle são agrupadas para simplificar o processo de definição de custos e tratamento dos riscos. A Tabela 1.9 apresenta os controles de segurança, suas referências e os custos. Os custos foram atribuídos de acordo com a disponibilidade de ferramentas, a necessidade de pessoal especializado, a documentação, a multiplicação de recursos e a facilidade de implementação dos controles. Os controles de baixo custo são aqueles amplamente difundidos, que possuem boa documentação e são de fácil implementação. Os controles de custo médio são pouco difundidos, possuem algumas ferramentas, são de implementação mais complicada ou envolvem redundância de recursos. Já os controles de alto custo são em geral incipientes, necessitam de pessoal especializado, são de difícil implementação ou necessitam de muito mais recursos para serem efetivados.

A Tabela 1.10 apresenta os controles relacionados aos riscos operacionais, junto com seus respectivos custos. Os custos dos controles operacionais dependem do esforço necessário para implementá-los. São considerados de baixo custo os controles operacionais que usam pouca mão-de-obra ou podem ser executados em pouco tempo. Os controles de custo médio necessitam de mão-de-obra especializada ou da aplicação de técnicas de gerenciamento. Os controles de alto custo envolvem o uso de métodos ou tecnologias incipientes ou de difícil implementação.

Tabela 1.9. Classificação de controles de segurança e seus custos

Item	Controle	Referências	Custo
CS1	Autenticação	[Yegneswaran et al. 2004] [Demchenko et al 2005] [Yu et al., 2005] [Lindqvist and Jonsson 1998] [Han e Zheng, 2000]	BAIXO
CS2	Assinatura	[Demchenko et al 2005] [Yu et al., 2005] [Dacier 2002]	BAIXO
CS3	Controle de Acesso	[Demchenko et al 2005] [Yu et al., 2005] [Yegneswaran et al. 2004]	BAIXO
CS4	Controle de fluxo	[Lindqvist and Jonsson 1998] [Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Feiertag et al., 2000b] [Frincke, 2000]	BAIXO
CS5	Criptografia	[Mell et al 2000] [Dacier 2002] [Demchenko et al 2005] [Yu et al., 2005]	BAIXO
CS6	Detecção de falhas	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Demchenko et al 2005] [Yu et al., 2005] [Feiertag et al., 2000a, 2000 b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	BAIXO
CS7	Filtragem de Tráfego	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Feiertag et al., 2000a, 2000b]	BAIXO
CS8	Reativação automática	[Yegneswaran et al. 2004] [Ptacek an d Newsham 1998] [Dacier 2002] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	BAIXO
CS9	Sensores baseados em aplic ação	[Ptacek and Newsham 1998]	BAIXO
CS10	*Timestamps* e *cache*	[Demchenko et al 2005] [Yu et al., 2005]	BAIXO
CS11	Análise de Conteúdo	[Demchenko et al 2005] [Yu et al., 2005]	MÉDIO
CS12	Correlação de dados	[Yegneswaran et al. 2004] [Dacier 2002]	MÉDIO
CS13	Distribuição de sistemas	[Yegneswaran et al. 2004] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tos ic, 2004, 2005] [Wang et al., 2004]	MÉDIO
CS14	Diversidade	[Ptacek and Newsham 1998]	MÉDIO
CS15	Política de Segurança	[Lindqvist and Jonsson 1998] [Feiertag et al., 2000a, 2000b]	MÉDIO
CS16	Replicação	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002] [Dacier 2002] [Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	MÉDIO
CS17	Seleção dinâmica	[Yegneswaran et al. 2004] [Ptacek and Newsham 1998] [Dacier 2002]	MÉDIO
CS18	Gerenciamento	[Lindqvist and Jonsso n 1998] [Han e Zheng, 2000] [Charfi e Mezini, 2005] [Feiertag et al., 2000a, 2000b] [Demchenko et al 2005] [Yu et al., 2005] [Frincke, 2000]	MÉDIO
CS19	Uso de recursos exclusivos	[Mell et al 2000] [Dacier 2002]	ALTO

Tabela 1.10. Classificação de controles operacionais e seus custos

Item	Controle	Referências	Custos
CO1	Avaliação dos padrões	[Parastatidis and Webber 2004]	BAIXO
CO2	Caracterização padronizada	[Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	ALTO
CO3	Comunicação padronizada	[Bass 2 004]	MÉDIO
CO4	Descrição padronizada	[Feiertag et al., 2000a, 2000b] [Esfandiari e Tosic, 2004, 2005] [Wang et al., 2004]	MÉDIO
CO5	Disponibilidade de ferramentas	[Parastatidis and Webber 2004]	MÉDIO
CO6	Documentação	[Parastatidis and Webber 2004]	BAIXO
CO7	Gerenciamento padronizado	[Lindqvist and Jonsson 1998]	BAIXO
CO8	Independência de Tecnologia	[Parastatidis and Webber 2004]	BAIXO
CO9	Qualificação de recursos humanos	[Lindqvist and Jonsson 1998] [Parastatidis and Webber 2004]	MÉDIO

1.4.4. Estimativa de Riscos

Após combinar os riscos de segurança identificados anteriormente, aplicamos os critérios de análise definidos na seção 1.4.2 para construir a Tabela 1.11. A tabela apresenta os riscos, as conseqüências e o impacto da exploração do risco. A tabela também contém o escore de risco de cada um dos itens relacionados à segurança. Esse escore foi obtido com a aplicação da metodologia CVSS, descrita na seção 1.3.1. Assumimos nesta análise que

não há controles implementados, pois os mesmos serão propostos nas próximas etapas do processo de gestão de riscos.

Tabela 1.11. Níveis de risco de segurança e a avaliação dos riscos

Risco	Acesso	Comp. Ac.	Autenticação	Imp. Conf.	Imp. Integr.	Imp. Disp.	Escore	Avaliação
1.1	REMOTO	BAIXA	DESNECESSÁRIA	COMPLETA	NENHUMA	NENHUMA	**7,8**	**ALTO**
1.2	LOCAL	ALTA	ÚNICA	COMPLETA	NENHUMA	NENHUMA	**3,8**	**BAIXO**
1.3	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	PARCIAL	COMPLETA	**8,5**	**ALTO**
1.4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	COMPLETA	**7,8**	**ALTO**
1.5	LOCAL	ALTA	ÚNICA	COMPLETA	PARCIAL	NENHUMA	**4,5**	**MÉDIO**
1.6	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	**5,0**	**MÉDIO**
1.7	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	**5,0**	**MÉDIO**
1.8	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	**5,0**	**MÉDIO**
1.9	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	**5,0**	**MÉDIO**
1.10	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	**5,0**	**MÉDIO**
1.11	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	PARCIAL	**7,3**	**ALTO**
1.12	LOCAL	ALTA	ÚNICA	COMPLETA	COMPLETA	COMPLETA	**6,0**	**MÉDIO**
1.13	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.1	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.2	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.3	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.4	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.5	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.6	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
2.7	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
3.1	REMOTO	ALTA	ÚNICA	COMPLETA	NENHUMA	NENHUMA	**4,9**	**MÉDIO**
3.2	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	COMPLETA	**7,8**	**ALTO**
3.3	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	COMPLETA	**7,8**	**ALTO**
3.4	REMOTO	ALTA	ÚNICA	COMPLETA	COMPLETA	COMPLETA	**7,1**	**ALTO**
3.5	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	PARCIAL	COMPLETA	**8,5**	**ALTO**
3.6	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	PARCIAL	COMPLETA	**8,5**	**ALTO**
4.1	REMOTO	ALTA	DESNECESSÁRIA	PARCIAL	NENHUMA	NENHUMA	**2,6**	**BAIXO**
4.2	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
4.3	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
4.4	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
4.5	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	COMPLETA	**7,8**	**ALTO**
4.6	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
4.7	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	NENHUMA	NENHUMA	**5,4**	**MÉDIO**
4.8	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	NENHUMA	**7,1**	**ALTO**
4.9	REMOTO	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	**7,6**	**ALTO**
4.10	REMOTO	ALTA	ÚNICA	COMPLETA	COMPLETA	COMPLETA	**7,1**	**ALTO**

Para exemplificar o cálculo do escore e a definição do nível de risco, tomemos como exemplo o risco RS1.1 (Espionagem - atacantes interceptam as mensagens de alerta trocadas entre os elementos de IDS). Para explorar a vulnerabilidade, o atacante pode estar remotamente (AV = 1), a complexidade de acesso é baixa (AC = 0,71) e é desnecessária a autenticação no sistema alvo (AU = 0,704). Como conseqüência da exploração da vulnerabilidade, há uma quebra completa da confidencialidade (CI = 0,660), mas não são afetadas a integridade e a disponibilidade do sistema (II = AI = 0). Concluída a análise, é aplicada a fórmula apresentada na seção 1.3.1 para a obtenção do escore:

$$\textbf{Impacto} = 10{,}41 * (1 - (1 - 0{,}66) * (1 - 0) * (1 - 0)) = 6{,}9$$

$$\textbf{Complexidade} = 20 * 0{,}71 * 0{,}704 * 1 = 10$$

$$\textbf{Risco Básico} = (0{,}6 * 6{,}9 + 0{,}4 * 10 - 1{,}5) * 1{,}176 = 7{,}8$$

Após ser calculado o escore, é atribuído o nível de risco de acordo com a classificação do NIST, na qual o escore com valor "7,8" é considerado como nível de risco Alto. Essa operação de cálculo é repetida para todos os riscos listados, formando a Tabela 1.11.

1.4.5. Avaliação de Riscos

Parte do trabalho de avaliação dos riscos de segurança foi adiantado ao se confeccionar a Tabela 1.11, tomando como base os dados obtidos na análise de riscos. A partir da observação da Tabela 1.11, foi construído o gráfico da Figura 1.10, no qual verifica-se uma maior quantidade de vulnerabilidades com alto risco de segurança, representando 39% do total, enquanto as de baixo e médio risco representam respectivamente 28% e 33% do total. Isso demonstra a necessidade de um tratamento de riscos para reduzir a quantidade de vulnerabilidades de médio e alto risco a um nível mínimo aceitável, de acordo com os recursos disponíveis. Sendo assim, é dada prioridade ao tratamento das vulnerabilidades de médio e alto risco.

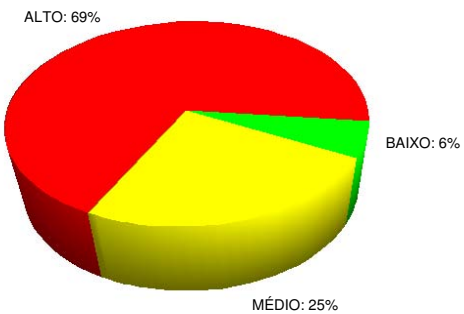

Figura 1.10. Distribuição dos níveis de risco iniciais

Os riscos operacionais relacionados ao uso de elementos heterogêneos estão associados a dificuldades de interoperabilidade e gerenciamento, que podem ser tratados com a adoção de padrões (Objetivo 3 – O3). Os riscos operacionais da composição dinâmica estão ligados a problemas de descrição e caracterização de componentes e serviços. Esses tipos de risco necessitam para seu tratamento de áreas de pesquisa incipientes que envolvem o uso de taxonomias, ontologia e semântica.

1.4.6. Tratamento do Risco

As opções de tratamentos foram identificadas na literatura e agrupadas na Tabela 1.9 (segurança) e na Tabela 1.10 (operacional), junto com os custos envolvidos. Para algumas vulnerabilidades é necessário associar diversos tratamentos.

As tabelas de identificação dos riscos de segurança (ver seção 6.5) e as tabelas com os controles para cada vulnerabilidade foram combinadas para uma nova análise de riscos, conforme ilustrado na Tabela 1.12.

Os tratamentos identificados para os riscos operacionais O2 e O3 foram considerados como boas práticas de desenvolvimento, para a seleção dos padrões utilizados

Tabela 1.12. Análise dos riscos de segurança tratados

Risco	Controles	Acesso	Comp. Ac.	Autenticação	Imp. Conf.	Imp. Integr.	Imp. Disp.	Escore	Avaliação
1.1	C19	LOCAL	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
1.1	C5	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
1.2	C4	LOCAL	ALTA	ÚNICA	PARCIAL	NENHUMA	NENHUMA	1,0	BAIXO
1.3	C6 + C8	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.3	C16	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.3	C7	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.3	C17	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.4	C4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.5	C1	LOCAL	ALTA	ÚNICA	COMPLETA	PARCIAL	NENHUMA	4,5	MÉDIO
1.6	C9	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.6	C14	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.7	C9	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.7	C14	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.8	C4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
1.9	C12	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.10	C3	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	PARCIAL	2,1	BAIXO
1.10	C13	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
1.11	C2 + C5	REMOTO	ALTA	ÚNICA	PARCIAL	NENHUMA	NENHUMA	2,1	BAIXO
1.12	C16	LOCAL	ALTA	ÚNICA	PARCIAL	NENHUMA	PARCIAL	2,4	BAIXO
1.13	C5	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	PARCIAL	PARCIAL	4,0	MÉDIO
2.1	C6+C13 + C14+C16	REMOTO	ALTA	DESNECESSÁRIA	PARCIAL	NENHUMA	PARCIAL	4,0	MÉDIO
2.1	C18	REMOTO	ALTA	DESNECESSÁRIA	PARCIAL	PARCIAL	PARCIAL	5,1	MÉDIO
2.2	C18	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
2.2	C1	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
2.3	C18	LOCAL	ALTA	DESNECESSÁRIA	PARCIAL	PARCIAL	PARCIAL	3,7	BAIXO
2.3	C19	LOCAL	ALTA	DESNECESSÁRIA	PARCIAL	PARCIAL	PARCIAL	3,7	BAIXO
2.4	C18	LOCAL	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	6,2	MÉDIO
2.5	C18	LOCAL	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	6,2	MÉDIO
2.6	C18	LOCAL	ALTA	DESNECESSÁRIA	COMPLETA	COMPLETA	COMPLETA	6,2	MÉDIO
2.7	C15 + C3	REMOTO	ALTA	UNICA	NENHUMA	PARCIAL	PARCIAL	3,6	BAIXO
3.1	C7 + C15	REMOTO	ALTA	ÚNICA	PARCIAL	NENHUMA	NENHUMA	2,1	BAIXO
3.2	C3 + C4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
3.3	C4	REMOTO	BAIXA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	5,0	MÉDIO
3.4	C18	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	PARCIAL	2,1	BAIXO
3.5	C13 + C16	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
3.6	C6+C8+C16	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
4.1	C18	REMOTO	ALTA	DESNECESSÁRIA	PARCIAL	NENHUMA	NENHUMA	2,6	BAIXO
4.1	C3	REMOTO	ALTA	ÚNICA	PARCIAL	NENHUMA	NENHUMA	2,1	BAIXO
4.2	C1 + C2 + C3 + C11	REMOTO	ALTA	MÚLTIPLAS	COMPLETA	COMPLETA	COMPLETA	6,8	MÉDIO
4.3	C1 + C2 + C3 + C11	REMOTO	ALTA	MÚLTIPLAS	COMPLETA	COMPLETA	COMPLETA	6,8	MÉDIO
4.4	C1 + C2 + C3 + C11	REMOTO	ALTA	MÚLTIPLAS	COMPLETA	COMPLETA	COMPLETA	6,8	MÉDIO
4.5	C1 + C3	REMOTO	BAIXA	MÚLTIPLAS	NENHUMA	NENHUMA	PARCIAL	3,3	BAIXO
4.6	C10	REMOTO	ALTA	DESNECESSÁRIA	NENHUMA	NENHUMA	PARCIAL	2,6	BAIXO
4.6	C2 + C5	REMOTO	ALTA	MÚLTIPLAS	NENHUMA	NENHUMA	PARCIAL	1,7	BAIXO
4.7	C5	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
4.8	C2 + C5	REMOTO	ALTA	MÚLTIPLAS	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
4.9	C5 + C18	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO
4.10	C5 + C18	REMOTO	ALTA	ÚNICA	NENHUMA	NENHUMA	NENHUMA	0,0	BAIXO

no projeto. Tais controles foram adotados, por exemplo, na escolha de padrões de organizações conhecidas, como o IETF, W3C e OASIS. Também foram úteis na escolha de ferramentas de desenvolvimento que são bem documentadas e conhecidas. O controle para a caracterização padronizada (CO2) foi implementado com a aplicação de uma taxonomia de elementos de detecção de intrusão. Já o controle para o uso de linguagens de descrição padrão foi efetivado com a adoção de XML e da especificação BPEL4WS.

Para mensurar os custos desses tratamentos combinados, será adotado o custo do tratamento mais oneroso, independentemente da quantidade de tratamentos associados.

Tabela 1.13. Avaliação e seleção dos tratamentos de segurança

Risco	Controles	Escore Original	Escore Tratado	Nível de Risco Original	Nível de Risco Tratado	Custo	Aplicação
1.1	C19	7,8	0,0	ALTO	BAIXO	ALTO	Não
1.1	C5	7,8	0,0	ALTO	BAIXO	BAIXO	**Sim**
1.2	C4	3,8	1,0	BAIXO	BAIXO	BAIXO	**Sim**
1.3	C6 + C8	8,5	5,0	ALTO	MÉDIO	BAIXO	**Sim**
1.3	C16	8,5	5,0	ALTO	MÉDIO	MÉDIO	Não
1.3	C7	8,5	5,0	ALTO	MÉDIO	BAIXO	**Sim**
1.3	C17	8,5	5,0	ALTO	MÉDIO	MÉDIO	Não
1.4	C4	7,8	5,0	ALTO	MÉDIO	BAIXO	**Sim**
1.5	C1	4,5	4,5	MÉDIO	MÉDIO	BAIXO	**Sim**
1.6	C9	5	2,6	MÉDIO	BAIXO	BAIXO	**Sim**
1.6	C14	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.7	C9	5	2,6	MÉDIO	BAIXO	BAIXO	**Sim**
1.7	C14	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.8	C4	5	5,0	MÉDIO	MÉDIO	BAIXO	**Sim**
1.9	C12	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.10	C3	5	2,1	MÉDIO	BAIXO	BAIXO	**Sim**
1.10	C13	5	2,6	MÉDIO	BAIXO	MÉDIO	Não
1.11	C2 + C5	7,3	2,1	ALTO	BAIXO	BAIXO	**Sim**
1.12	C16	6	2,4	MÉDIO	BAIXO	MÉDIO	**Sim**
1.13	C5	7,6	4,0	ALTO	MÉDIO	BAIXO	**Sim**
2.1	C6+C13 + C14+C16	7,6	4,0	ALTO	MÉDIO	MÉDIO	**Sim**
2.1	C18	7,6	5,1	ALTO	MÉDIO	MÉDIO	Não
2.2	C18	7,6	0,0	ALTO	BAIXO	MÉDIO	Não
2.2	C1	7,6	0,0	ALTO	BAIXO	BAIXO	**Sim**
2.3	C18	7,6	3,7	ALTO	BAIXO	MÉDIO	**Sim**
2.3	C19	7,6	3,7	ALTO	BAIXO	ALTO	Não
2.4	C18	7,6	6,2	ALTO	MÉDIO	MÉDIO	**Sim**
2.5	C18	7,6	6,2	ALTO	MÉDIO	MÉDIO	**Sim**
2.6	C18	7,6	6,2	ALTO	MÉDIO	MÉDIO	**Sim**
2.7	C15 + C3	7,6	3,6	ALTO	BAIXO	MÉDIO	**Sim**
3.1	C7 + C15	4,9	2,1	MÉDIO	BAIXO	MÉDIO	**Sim**
3.2	C3 + C4	7,8	5,0	ALTO	MÉDIO	BAIXO	**Sim**
3.3	C4	7,8	5,0	ALTO	MÉDIO	BAIXO	**Sim**
3.4	C18	7,1	2,1	ALTO	BAIXO	MÉDIO	**Sim**
3.5	C13 + C16	8,5	2,6	ALTO	BAIXO	MÉDIO	**Sim**
3.6	C6+C8+C16	8,5	2,6	ALTO	BAIXO	MÉDIO	**Sim**
4.1	C18	2,6	2,6	BAIXO	BAIXO	MÉDIO	Não
4.1	C3	2,6	2,1	BAIXO	BAIXO	BAIXO	**Sim**
4.2	C1 + C2 + C3 + C11	7,6	6,8	ALTO	MÉDIO	BAIXO	**Sim**
4.3	C1 + C2 + C3 + C11	7,6	6,8	ALTO	MÉDIO	BAIXO	**Sim**
4.4	C1 + C2 + C3 + C11	7,6	6,8	ALTO	MÉDIO	BAIXO	**Sim**
4.5	C1 + C3	7,8	3,3	ALTO	BAIXO	BAIXO	**Sim**
4.6	C10	7,6	2,6	ALTO	BAIXO	BAIXO	Não
4.6	C2 + C5	7,6	1,7	ALTO	BAIXO	BAIXO	**Sim**
4.7	C5	5,4	0,0	MÉDIO	BAIXO	BAIXO	**Sim**
4.8	C2 + C5	7,1	0,0	ALTO	BAIXO	BAIXO	**Sim**
4.9	C5 + C18	7,6	0,0	ALTO	BAIXO	MÉDIO	**Sim**
4.10	C5 + C18	7,1	0,0	ALTO	BAIXO	MÉDIO	**Sim**

Comparando os níveis de risco originais, os níveis de risco tratados e os custos de tratamento, identificamos quais tratamentos são mais eficientes e quais deverão ser implementados. A Tabela 1.13 apresenta essa comparação e os tratamentos selecionados. Foram 36 tratamentos selecionados e 12 tratamentos rejeitados. Apenas em um caso, no item RS1.3, foram combinadas as alternativas de tratamento, devido ao baixo custo de ambas.

1.4.7. Aceitação do Risco

Após a seleção dos tratamentos, verificamos a eliminação das vulnerabilidades de alto risco e a redução significativa dos riscos médios, conforme pode ser observado no gráfico da Figura 1.11.

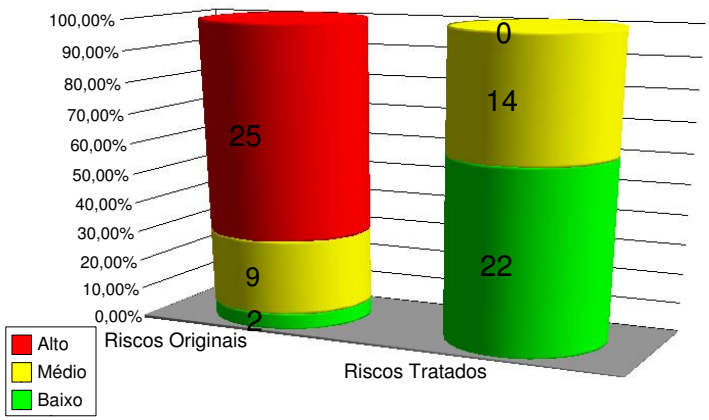

Figura 1.11. Comparativo dos níveis de risco de segurança, antes e após o tratamento

1.4.8. Monitoramento e Análise Crítica de Riscos

Nos projetos científicos, as revisões da gestão de riscos podem ser motivadas pela inclusão de novos elementos ao projeto, como, por exemplo, mudanças de paradigmas, novas bibliografias ou revisões de trabalhos submetidos para publicação. O processo de Comunicação do Risco é de extrema importância na revisão de projetos científicos.

Um método de revisão é o refinamento contínuo da análise. Parte-se de um escopo mais global, no qual os novos elementos do projeto são identificados. Depois, tais elementos são analisados separadamente para verificar se novos riscos foram descobertos e se novos tratamentos são necessários.

Outra questão diz respeito a ajustes do processo de gestão de riscos de segurança, em decorrência de mudanças metodológicas, como o lançamento de uma nova norma ou a alteração de versão do CVSS, por exemplo. A primeira análise realizada neste projeto foi elaborada usando exclusivamente a norma AS/NZ4360 e a versão 1,0 do CVSS. A

presente análise reviu estes procedimentos e elaborou novos resultados de acordo com os novos critérios.

1.4.9. Considerações sobre o Estudo de Caso

Com a metodologia aplicada, foi possível acompanhar o desenvolvimento das soluções propostas e implementadas no projeto de pesquisa e trabalhar os riscos envolvidos, melhorando significativamente a compreensão dos problemas e suas soluções. Tal acompanhamento ocasionou melhorias evidentes nos resultados do projeto.

Durante o processo foi preciso revisar e agrupar várias referências científicas dentro do escopo de cada objetivo. Como conseqüência, além da metodologia de gestão de riscos aplicada a cada área do escopo do projeto, temos como contribuições adicionais:

1. Identificação de riscos nas composições de IDSs;
2. Análise e avaliação dos riscos de segurança;
3. Tratamentos para riscos operacionais discutidos na literatura científica;
4. Identificação de riscos e tratamentos associados a IDSs distribuídos;
5. Identificação de riscos e tratamentos associados ao uso de COTS; e
6. Identificação de riscos e tratamentos associados à composição dinâmica de IDSs.

A gestão de riscos também pode ser aplicada em outras etapas do projeto, como na avaliação dos produtos utilizados no desenvolvimento do protótipo.

1.5. Conclusões

Esse curso apresentou a disciplina de gestão de riscos de segurança, tratando, principalmente, dos principais padrões relacionados ao assunto. Para ilustrar o tema, foi detalhado um estudo de caso, no qual uma metodologia de Gestão de Riscos foi aplicada no acompanhamento de um projeto científico.

Com a utilização da metodologia de gestão de riscos, espera-se a identificação e o tratamento da maioria das vulnerabilidades conhecidas e pertinentes às soluções adotadas em um projeto de Tecnologia da Informações. Isso sem dúvida auxilia no entendimento dos problemas de segurança que seriam enfrentados, tendo como conseqüência a melhoria do projeto como um todo. Infelizmente, não é possível garantir que o projeto seja totalmente seguro. Contudo, podemos afirmar que, com a realização de boas práticas de gestão de risco, são tomadas todas as medidas preventivas necessárias à atenuação do impacto negativo que possíveis vulnerabilidades infringiriam ao projeto.

Esperamos com esse curso ter contribuído para um melhor entendimento destas metodologias de gestão de riscos e a difusão das idéias da necessidade da avaliação via estes testes padronizados dos sistemas de segurança.

Referências

[ABNT 2006a] ABNT (2006a). Código de Prática para a Gestão da Segurança da Informação. ABNT NBR ISO/IEC 27002:2005.

[ABNT 2006b] ABNT (2006b). Sistemas de Gestão de Segurança da Informação - Requisitos. ABNT NBR ISO/IEC 27001:2006.

[ABNT 2008] ABNT (2008). Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. ABNT NBR ISO/IEC 27005:2008.

[AS/NZS 2004a] AS/NZS (2004a). *Risk Management - AS/NZS4360:2004*. Australian/New Zealand Standard, third edition.

[AS/NZS 2004b] AS/NZS (2004b). *Risk Management Guidelines Companion to AS/NZS 4360:2004 - HB 436:2004*. Australian/New Zealand Standard, third edition.

[Athanasiades et al. 2003] Athanasiades, N., Abler, R., Levine, J., Owen, H., and Riley, G. (2003). Intrusion detection testing and benchmarking methodologies. In *IEEE-IWIA '03: Proceedings of the First IEEE International Workshop on Information Assurance (IWIA'03)*, page 63, Washington, DC, USA. IEEE Computer Society.

[Barker and Lee 2004] Barker, W. C. and Lee, A. (2004). Information security - volume ii: Appendices to guide for mapping types of information and information systems to security categories. NIST Special Publication 800-60.

[Bass 2004] Bass, T. (2004). Service-oriented horizontal fusion in distributed coordination-based systems. In *IEEE MILCOM 2004*, volume 2, pages 615– 621, Monterey, CA, USA.

[Bishop 2003] Bishop, M. (2003). *Computer Security: Art and Science*. Addison Wesley, Bonston, MA.

[Blakley et al. 2001] Blakley, B., McDermott, E., and Geer, D. (2001). Information security is information risk management. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 97–104, New York, NY, USA. ACM Press.

[Brandão 2007] Brandão, J. E. M. S. (2007). *COMPOSIÇÕES DE IDSs: VIABILIZANDO O MONITORAMENTO DE SEGURANÇA EM AMBIENTES DE LARGA ESCALA*. PhD thesis, Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina.

[Brandão et al. 2006a] Brandão, J. E. M. S., Fraga, J. S., and Mafra, P. M. (2006a). A New Approach for IDS Composition. In *Proceedings of ICC 2006: IEEE International Conference on Communications*, Istanbul, Turkey.

[Brandão et al. 2006b] Brandão, J. E. M. S., Fraga, J. S., Mafra, P. M., and Obelheiro, R. R. (2006b). A WS-Based Infrastructure for Integrating Intrusion Detection Systems in Large-Scale Environments. In *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE*, volume 4275 of *Lecture Notes in Computer Science*, pages 462–479, Montpellier, France. Springer Berlin / Heidelberg.

[Bray et al. 2004] Bray, T., Paoli, J., and Sperberg-McQueen, C. M. (2004). Extensible Markup Language (XML) 1.0 (third edition)". W3C Recommendation.

[BSi 1999] BSi (1999). Information Security Management, Part 1: Code of Practice for Information Security Management. BS 7799-1:1999.

[BSi 2002] BSi (2002). Information Security Management, Part 2: Specification with guidance for use. BS 7799-2:2002.

[BS/ISO 2005] BS/ISO (2005). BS/ISO17799 Information technology – Code of practice for information security managementt. BS/ISO 17799:2005.

[Charfi and Mezini 2005] Charfi, A. and Mezini, M. (2005). Using aspects for security engineering of web service compositions. In *ICWS '05: Proceedings of the IEEE International Conference on Web Services (ICWS'05)*, pages 59–66, Washington, DC, USA. IEEE Computer Society.

[Dacier 2002] Dacier, M. (2002). Design of an intrusion-tolerant intrusion detection system. maftia project, deliverable 10. Technical report, IBM Zurich Research Laboratory.

[Debar et al. 1998] Debar, H., Dacier, M., Wespi, A., and Lampart, S. (1998). An Experimentation Workbench For Intrusion Detection Systems. Technical report, IBM, IBM Research, Zurich Research Laboratory.

[Demchenko et al. 2005] Demchenko, Y., Gommans, L., de Laat, C., and Oudenaarde, B. (2005). Web services and grid security vulnerabilities and threats analysis and model. In *Proceedings of the "6th IEEE/ACM International Workshop on Grid Computing*, pages 262–267, Seattle, Washington, USA. IEEE Cat. No. 05EX1210C.

[Durst et al. 1999] Durst, R., Champion, T., Witten, B., Miller, E., and Spagnuolo, L. (1999). Testing and evaluating computer intrusion detection systems. *Commun. ACM*, 42(7):53–61.

[Esfandiari and Tosic 2004] Esfandiari, B. and Tosic, V. (2004). Requirements for web service composition management. In *Proc. of the 11th Hewlett-Packard Open View University Association (HP-OVUA) Workshop*, Paris, France. Hewlett-Packard.

[Esfandiari and Tosic 2005] Esfandiari, B. and Tosic, V. (2005). Towards a web service composition management framework. In *ICWS*, pages 419–426. IEEE Computer Society.

[Feiertag et al. 2000] Feiertag, R., Redmond, T., and Rho, S. (2000). A framework for building composable replaceable security services. In *DARPA Information Survivability Conference & Exposition*, volume 2, pages 391–402.

[Frincke 2000] Frincke, D. (2000). Balancing cooperation and risk in intrusion detection. *ACM Trans. Inf. Syst. Secur.*, 3(1):1–29.

[Garfinkel et al. 2003] Garfinkel, S., Spafford, G., and Schwartz, A. (2003). *Practical Unix and Internet security (3rd ed.)*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, third edition.

[Han and Zheng 2000] Han, J. and Zheng, Y. (2000). Security characterisation and integrity assurance for software components and component-based systems. In *International Conference on Software Methods and Tools*, pages 61–66. IEEE Computer Society Press.

[ISO 1989] ISO (1989). Information processing systems - open systems interconnection - basic reference model - part 2: Security architecture. ISO 7498-2.

[ISO 2002] ISO (2002). Risk management - Vocabulary - Guidelines for use in standards. ISO/IEC Guide 73:2002.

[ISO 2007] ISO (2007). Risk management - guidelines on principles and implementation of risk management. ISO/TMB WG on Risk management N 047.

[ISO/IEC 2005a] ISO/IEC (2005a). Common criteria for information technology security evaluation - part 1: Introduction and general model. ISO/IEC 15408:2005.

[ISO/IEC 2005b] ISO/IEC (2005b). Common criteria for information technology security evaluation - part 2: Security functional requirements. ISO/IEC 15408:2005.

[ISO/IEC 2005c] ISO/IEC (2005c). Common criteria for information technology security evaluation - part 3: Security assurance requirements. ISO/IEC 15408:2005.

[Lindqvist and Jonsson 1998] Lindqvist, U. and Jonsson, E. (1998). A map of security risks associated with using cots. *Computer*, 31(6):60–66.

[Lippmann et al. 2000a] Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., and Das, K. (2000a). The 1999 darpa off-line intrusion detection evaluation. *Comput. Networks*, 34(4):579–595.

[Lippmann et al. 2000b] Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., Weber, D., Webster, S. E., Wyschogrod, D., Cunningham, R. K., and Zissman, M. A. (2000b). Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. *discex*, 02:1012.

[McHugh 2000] McHugh, J. (2000). Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. *ACM Trans. Inf. Syst. Secur.*, 3(4):262–294.

[Mell and Grance 2002] Mell, P. and Grance, T. (2002). Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme. NIST Special Publication 800-51.

[Mell et al. 2000] Mell, P., Marks, D., and McLarnon, M. (2000). A denial-of-service resistant intrusion detection architecture. *Comput. Networks*, 34(4):641–658.

[Parastatidis and Webber 2004] Parastatidis, S. and Webber, J. (2004). Assessing the risk and value of adopting emerging and unstable web services specifications. In *SCC '04: Proceedings of the 2004 IEEE International Conference on Services Computing*, pages 65–72, Washington, DC, USA. IEEE Computer Society.

[Ptacek and Newsham 1998] Ptacek, T. H. and Newsham, T. N. (1998). Insertion, evasion, and denial of service: Eluding network intrusion detection. Technical report, Secure Networks,Inc.

[Puketza et al. 1996] Puketza, N. J., Zhang, K., Chung, M., Mukherjee, B., and Olsson, R. A. (1996). A methodology for testing intrusion detection systems. *IEEE Trans. Softw. Eng.*, 22(10):719–729.

[Ross et al. 2005] Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., and Lee, A. (2005). Recommended security controls for federal information systems. NIST Special Publication 800-53.

[Stoneburner et al. 2002] Stoneburner, G., Goguen, A., and Feringa, A. (2002). Risk management guide for information technology systems. NIST Special Publication 800-30.

[Swanson and Guttman 1996] Swanson, M. and Guttman, B. (1996). Generally accepted principles and practices for securing information technology systems. NIST Special Publication 800-14.

[US Department of Homeland Security 2002] US Department of Homeland Security (2002). Federal Information Security Management Act of 2002, H.R. 2458-48. (Public Law 107-347).

[W3C 2004] W3C (2004). Web Services Architecture. W3C Working Group Note 11.

[Wang et al. 2004] Wang, H., Huang, J. Z., Qu, Y., and Xie, J. (2004). Web services: problems and future directions. *Journal of Web Semantics*, 1(3):309–320.

[Yegneswaran et al. 2004] Yegneswaran, V., Barford, P., and Jha, S. (2004). Global intrusion detection in the DOMINO overlay system. In *NDSS*, San Diego, California, USA. The Internet Society.

[Yu and Frincke 2004] Yu, D. and Frincke, D. (2004). Towards survivable intrusion detection system. *hicss*, 09:90299a.

[Yu et al. 2005] Yu, W. D., Supthaweesuk, P., and Aravind, D. (2005). Trustworthy web services based on testing. *sose*, 0:167–177.