UNIVERSIDADE ESTADUAL PAULISTA
"Júlio de Mesquita Filho"
Pós-Graduação em Ciência da Computação

Dioraci Corrêa Junior

Um modelo de assinatura de risco voltada para segurança da informação

UNESP
2009

Dioraci Corrêa Junior

Dissertação sobre Análise de Risco: Um modelo de assinatura de risco voltada para segurança da informação

Orientador: Prof. Dr. Adriano Mauro Cansian

Dissertação de Mestrado elaborada junto ao Programa de Pós-Graduação em Ciência da Computação – Área de Concentração em Sistemas de Computação, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

UNESP
2009

Dioraci Corrêa Junior

Um modelo de assinatura de risco voltada para segurança da informação.

Dissertação apresentada para obtenção do título de Mestre em Ciência da Computação, área de Sistemas de Computação junto ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

BANCA EXAMINADORA

Prof. Dr. Adriano Mauro Cansian
Professor Assistente Doutor
UNESP – São José do Rio Preto
Orientador

Profª. Drª. Luciana Andréia Fondazzi Martimiano
Professor Doutor
UEM – Universidade Estadual de Maringá

Prof. Dr. José Márcio Machado
Professor Assistente Doutor
UNESP – São José do Rio Preto

São José do Rio Preto, julho de 2009.

Agradecimentos

Primeiramente a Deus pela oportunidade concedida de desenvolver este trabalho.

A minha esposa Carine pela compreensão e paciência. Obrigado loira.

Aos meus pais, Dioraci e Ana Maria, por terem sempre me ensinado os valores corretos dessa vida e pelo suporte e apoio nas etapas difíceis de minha vida.

Ao meu irmão Jorge, pelo apoio e companheirismo. Valeu cara.

Ao grande professor, orientador e amigo Adriano Mauro Cansian, pela grande paciência, pelo suporte e apoio, mostrando sempre o caminho a ser seguido, mesmo nos momentos mais difíceis onde não encontrava uma saída.

A todos os meus amigos do Laboratório ACME!, vocês são demais.

Aos meus amigos e colegas da Diretoria de Gestão de Segurança que me apoiaram neste percurso.

Aos amigos do IBILCE que acompanharam a história de minha vida acadêmica desde o início.

A todos os professores do IBILCE que dividiram seus conhecimentos comigo, com muita paciência para ensinar, mostrando sempre o caminho a ser seguido.

Ao Sr. Steve Jobs, o criador da Apple e do Mac OS X, onde esta dissertação foi escrita.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

A Análise de Risco incorpora a avaliação do risco e seu gerenciamento, isto é, ela combina processos sistemáticos para a identificação do risco e suas consequências, e como lidar ou tratar estes riscos. Esta dissertação apresenta o desenvolvimento de uma Assinatura de Risco, suportada pelo sistema *AISF – ACME! Intrusion Signature Format* [SIL, 2002], voltada estritamente à segurança da informação e adequada de acordo com os padrões das normas ISO/IEC 17799 [ISO, 2005], ISO/IEC 27001 [ISO, 2006] e ISO/IEC 27002 [ISO, 2007]. O desenvolvimento desta assinatura está ligado à frente de pesquisa sobre Análise de Risco em sistemas computacionais e representa algo inédito na literatura, uma padronização para Análise de Risco. Com isso, o processo de armazenamento e análise de informação a respeito da Análise de Risco tornar-se mais simples e padronizado.

Palavras chave:
Análise de Risco, Segurança da Informação, Assinatura, AISF

Abstract

Risk analysis includes a risk assessment and management, that is, it combines systematic procedures for risk identification and its consequences, and how to deal and mitigate these risks. This dissertation presents the Signature Risk development, supported by AISF - ACME! Intrusion Signature Format [SIL, 2002] system, dedicated strictly to information security and appropriate under the standards of ISO/IEC 17799 [ISO, 2005], ISO/IEC 27001 [ISO, 2006] and ISO/IEC 27002 [ISO, 2007]. This signature development is linked with computer systems risk analysis research and represent something unprecedented in literature, a standard for risk analysis. Therefore, the storing and analyzing process of information about risk analysis become more simple and standardized.

Key words:
Risk Analysis, Information Security, Signature, AISF

1. Objetivos e proposta

1.1. Introdução

A operação de sistemas computacionais deveria levar a alguns questionamentos relevantes relativos à segurança da informação. Dentre os mais importantes, podemos destacar questionamentos sobre quão seguro é o sistema e quão seguro ele precisaria ser. Ao responder estes questionamentos, um analista deve ser capaz de responder sobre quanto pode ser melhorada a segurança nosso sistema, a fim de avaliar a eficácia dos dispositivos de segurança.

Os analistas procuram respostas a estes questionamentos e a outros que forneçam medidas de quão eficientes são os esforços em segurança, de modo a reduzir os riscos ao qual o sistema está exposto, ou qual a redução nos riscos que deve ser esperada com a adição de novos mecanismos e controles de segurança. Normalmente isso significa estimar valores passados e projetar valores futuros de cada uma das métricas dos riscos à segurança, tais como frequência de incidentes de segurança ou custos anuais destes incidentes. Para tomar decisões de segurança é necessário utilizar estas métricas para decidir quais escolhas devem ser realizadas, a fim de que estas influenciem efetivamente nas estratégias de segurança e na redução dos riscos.

Pensar em uma metodologia geral e padronizada para modelar riscos de segurança tem se mostrado algo ilusório, pois a segurança de um sistema é afetada não apenas por ações, mas também por escolhas estratégicas dos atacantes, dentre outros fatores e variáveis. Assim, a metodologia deve ser adaptativa a ponto de considerar estes conceitos.

1.2. Identificação do Problema e Justificativa

Nesta seção são expostos os fatos e os conceitos preliminares que levaram à decisão de desenvolver esta linha de pesquisa e que resultaram neste trabalho.

1.2.1. Definições sobre segurança da informação [ISO, 2007]

A informação é um ativo[1] como qualquer outro. Atualmente, em alguns casos, a informação é o ativo mais importante da organização, sendo essencial para os negócios. Consequentemente, assim como os demais ativos, necessita ser protegida de forma adequada, especialmente no ambiente dos negócios, cada vez mais interconectados. Com este aumento da interconectividade, a informação passa a estar a cada dia mais exposta a uma grande variedade de ameaças e vulnerabilidades.

A informação pode se apresentar de diversas formas, impressa ou escrita, transmitida pelo correio ou através de meios eletrônicos, armazenada fisicamente ou eletronicamente, apresentada em filmes ou falada em conversas, ou seja, de forma verbal. Independente do meio ao qual a informação está sendo transmitida ou compartilhada ou de qual forma está sendo armazenada ou apresentada, é recomendado que esta seja sempre adequadamente protegida.

Segundo a norma ISO/IEC 17799, "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" [ISO, 2007].

Para se garantir segurança da informação é necessário a implementação de um conjunto de controles[2] adequados. Dentre estes controles podemos incluir processos, políticas, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Tais controles necessitam serem estabelecidos, implementados, monitorados, analisados criticamente e melhorados, caso necessário, a fim de assegurar que os objetivos do negócio e de segurança da organização sejam atendidos em sua completude.

[1] "Qualquer coisa que tenha valor para a organização" [ISO, 2006]
[2] formas de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal [ISO,2006]

1.2.2. A necessidade da segurança da informação [ISO, 2007]

Conforme já mencionado, a informação e seus processos de suporte, sistemas computacionais e redes de computadores são ativos importantes para os negócios da instituição. Algumas atividades, como, definir, alcançar, manter e melhorar a segurança da informação podem ser essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.

Tanto as organizações, quanto seus sistemas de informação e redes de computadores estão expostos a diversos tipos de ameaças à segurança da informação. Estas podem ser lógicas ou físicas, incluindo desde fraudes eletrônicas, espionagem, sabotagem, vandalismo, até incêndio, inundação ou outras causas naturais. Caso o sistema esteja vulnerável a estas ameaças, a instituição poderá sofrer danos e prejuízos elevados. Atualmente, danos causados por códigos maliciosos, *hackers,* ataques de negativa de serviço (*Denial-of-Service* - *DoS*) fraudes eletrônicas estão se tornando cada vez mais comuns, mais ambiciosos e muito mais sofisticados.

A segurança da informação é essencial para o mundo dos negócios, tanto no setor público como no setor privado. A segurança da informação tem como uma das funções viabilizar os negócios e evitar ou reduzir os riscos relevantes a estes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar todos os fatores envolvidos.

Muitos sistemas de informação não foram concebidos e projetados visando a segurança da informação, logo, para estes sistemas o nível de segurança que pode ser alcançado por meios técnicos é limitado e deve ser suprido por uma gestão com procedimentos apropriados. Para isso, torna-se necessário a identificação de controles a serem implementados a fim de se prover melhorias na segurança destes sistemas, o que requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão de segurança da informação requer pelo menos a participação de todos os membros da organização.

1.2.3. Relação entre Segurança da Informação e Análise de Risco

No passado, segurança consistia em limitar o acesso a funcionários autorizados e a segurança física dos terminais de acesso ao sistema. Assim, segurança eletrônica era, simplesmente, o isolamento dos sistemas de qualquer acesso externo. Infelizmente, muitos sistemas computacionais hoje utilizados, ainda confiam na premissa de manter a segurança isolando o sistema corporativo e as redes internas da Internet. Claramente, esta abordagem não é eficaz, pois tanto as redes corporativas quanto a Internet são atualmente utilizadas para o fluxo de informações de uma forma conjunta, interligando todos os setores e localidades da instituição detentora do sistema.

Tem sido extensamente discutido que a realização de atividades pessoais e profissionais através da Internet tornou-se parte integrante da rotina diária da sociedade atual. Também é bem sabido que cada vez mais atividades, tais como transações bancárias, comércio eletrônico, operações confidenciais ou mesmo controle de processos críticos, ocorrem diuturnamente por intermédio de redes de computadores e sistemas computacionais.

A proliferação dos computadores e das redes com um custo mais acessível ampliou o problema da segurança nestes sistemas. A disponibilidade de conexão a todo momento, com taxas de transmissão cada vez mais elevadas, tem contribuído para o crescimento do número de problemas de segurança, principalmente *worms* [LUR, 2004], ataques de negativa de serviço (*Denial-of-Service - DoS*) [MVF, 2001] e fraudes eletrônicas. Existe também uma ampla gama de *softwares*, bastante utilizados atualmente, com a premissa de redução de custo e minimização da complexidade de manutenção. No entanto, estes *softwares* são escritos priorizando-se a funcionalidade e performance em detrimento da segurança.

Dessa forma, um número cada vez maior de incidentes é reportado aos centros de resposta à incidentes de segurança, tais como o CERT/CC [CER, 2008] e o CERT.BR [CBR, 2008]. Trabalhos recentes destas instituições apontam que, dentre os incidentes reportados, 54% são fraudes, 25% são ataques de prospecção (denominados genericamente de *scan*) e 16% são ataques de *worms*. Tais ataques

podem causar grandes danos e prejuízos às redes e sistemas de diversas organizações, comprometendo operações críticas e a continuidade dos negócios.

Portanto, o funcionamento correto de toda esta infraestrutura de conexão, a todo momento, tornou-se de fundamental importância para nossa sociedade[3]. Mas, para que isso ocorra, falhas de segurança devem ser eliminadas ou reduzidas, quando for o caso. Isto faz com que técnicas especiais de segurança sejam indispensáveis nos sistemas computacionais e nas redes de computadores atuais. Desta forma, os desenvolvimentos atuais buscam identificar quais destas técnicas especiais de segurança devem ser empregadas para tornar o sistema mais seguro, com relação às ameaças ao qual está exposto. Desta forma, faz-se necessário o desenvolvimento e o aprimoramento de técnicas para análise e classificação dos riscos inerentes a estes sistemas, a fim de evitar ou minimizar danos e prejuízos.

O conceito de análise de risco, na sua forma genérica, é atualmente empregado em diversas áreas, como por exemplo: medicina, economia, mercado financeiro, segurança interna e operações militares. Na maioria dos casos, a análise é feita de forma quantitativa, baseada apenas em números e fatos que já aconteceram. No entanto, torna-se muito difícil priorizar as vulnerabilidades de segurança de sistemas computacionais, de uma maneira eficiente, considerando apenas uma análise quantitativa, devido à enorme quantidade de métricas efetivas e dados históricos. Além disso, há uma complexidade e natureza sensível que envolve os assuntos relacionados à segurança. Essas dificuldades podem resultar em uma alocação insuficiente de recursos de segurança, ou numa análise sub ou superestimada.

Esta análise e controle dos riscos são muito importantes para a continuidade dos negócios nas empresas e instituições. Quando realizada de uma forma correta e bem elaborada, considerando não apenas dados quantitativos mas também o contexto envolvido, pode evitar muitos prejuízos e gastos desnecessários.

[3] Exemplo: Pane em provedor de internet em julho de 2008 deixou usuários e várias instituições públicas e privadas do estado de São Paulo totalmente paradas e causou um prejuízo da ordem de milhões de reais.

Além destes fatos, segurança adicional quase sempre envolve custos adicionais, custos estes que não geram retorno diretamente ao investidor ou à instituição detentora do sistema, o que sempre deve ser justificado em termos financeiros. Uma análise de risco bem elaborada irá gerar direta e automaticamente tal justificativa para recomendações de segurança, pois mostrará de forma clara o custo com um eventual incidente e o investimento para evitar que este ocorra.

Quando do processo de listagem das considerações de segurança, alguns quesitos devem ser considerados, dentre os quais se destacam:

- Tipos de risco associados aos sistemas analisados;
- Mecanismos de segurança necessários para prover proteção satisfatória;
- Nível de segurança desejado ou requerido provido pelos mecanismos;
- Risco residual.

As análises destes quesitos auxiliam na identificação e entendimento dos riscos, na seleção dos mecanismos de segurança apropriados e na redução dos riscos ao sistema, identificando e mitigando vulnerabilidades.

Explorando vulnerabilidades ou falhas nos sistemas computacionais, diversos tipos de ataques podem ser desencadeados, desde simples tentativas de prospecção até ataques sofisticados para ganho de acesso privilegiado ao sistema. A natureza destes ataques está ligada a diversos fatores, tais como arquitetura do sistema, conectividade com o mundo exterior, atos de engenharia social – fortemente ligados ao fator humano, dentre outros.

1.2.4. Contextualizando o problema

Em grandes redes institucionais o trabalho de monitorar inúmeras redes e máquinas com propósitos de segurança pode ser dispendioso, pois seria necessário o monitoramento individual de cada máquina, caso a rede não tenha sido projetada e montada de uma forma que vise a segurança do conjunto, deixando lacunas

vulneráveis que possam comprometer a segurança deste conjunto. O mesmo acontece em nível de *software*. Se um *software* instalado ou desenvolvido pela instituição não prover um nível de segurança mínimo – livre de falhas ou *bugs* que possam gerar vulnerabilidades ao sistema como um todo – estes poderão comprometer a segurança do sistema.

Para evitar que esta situação ocorra surge a idéia de construir uma metodologia de Análise de Risco Computacional voltada para a Segurança da informação, baseada nas normas publicadas pela ISO - *International Organization for Standardization* e pela IEC - *International Electrotechnical Commission*: ISO 17799 [ISO, 2005] e suas atualizações ISO 27001 [ISO, 2006] e ISO 27002 [ISO, 2007]. Como já citado, atualmente existem muitas metodologias de Análise de Risco, focando diferentes tipos de riscos ou diferentes áreas de conhecimento: projetos em TI, desenvolvimento de software, medicina, dentre outras. No entanto, nenhum modelo específico é voltado estritamente para a segurança da informação em ambientes computacionais.

Na maioria destes casos, com modelos quantitativos, baseada em números e fatos que já ocorreram. Na área de segurança da informação em sistemas computacionais, essa abordagem torna-se complexa devido à enorme quantidade de dados, grande número de métricas a serem consideradas e o conjunto de dados históricos é muito extenso. Dessa forma, uma metodologia que trate estes dados de forma qualitativa faz-se necessária, a fim de se padronizar o processo de análise de risco voltado para segurança da informação.

A próxima seção apresenta os objetivos deste trabalho, e como o trabalho desenvolvido foi estruturado.

1.3. Objetivos

O principal objetivo deste trabalho é desenvolver uma Assinatura de Risco baseada no conceito de árvores de ataque e no modelo *The Australian/New Zeland*

standard. Esta assinatura é utilizada como peça fundamental de uma metodologia de Análise de Risco voltada para a segurança da informação que atenda as normas ISO 17799 [ISO, 2005], ISO 27001 [ISO, 2006] e ISO 27002 [ISO, 2007] além de ser compatível com o modelo de gerenciamento de assinaturas AISF - *ACME! Intrusion Signature Format* [SIL, 2002].

Desta forma, pretende-se estudar os riscos inerentes a um sistema, desenvolvendo uma assinatura de risco, um trabalho pioneiro que procura criar o conceito de assinatura de risco que será a base dentro de uma metodologia de análise de risco. A assinatura cataloga e classifica tais riscos, coletando as informações necessárias para a realização de uma análise completa a respeito da probabilidade desses riscos se tornarem um incidente, qual o impacto – prejuízo – que o incidente causaria no sistema e na sua organização detentora.

Além desta análise, a assinatura indica quais são as contramedidas ou controles a serem implementados, de acordo com a ISO 27001 [ISO, 2006], para evitar que estes ocorram e, por fim, quanto custariam estes controles em relação ao custo de uma ocorrência.

Como resultado espera-se uma Assinatura de Risco compatível com o modelo AISF [SIL, 2002], que poderá ser utilizada como base para a implementação de controles de segurança aos ativos de uma organização – conforme dispostos na norma ISO 27001 [ISO, 2006] e ISO 27002 [ISO, 2007] e que, quando colocada em prática, funcione como uma ferramenta que possibilite descrever com detalhes as falhas e vulnerabilidades de sistemas computacionais, fornecendo um parecer completo, direto e objetivo da análise dos riscos de um sistema, voltado para a segurança, baseado em dados concretos obtidos através de uma análise minuciosa do sistema cliente. Outro resultado esperado é que a Assinatura possa ser usada para servir como base de uma ferramenta de certificação de adequação à norma ISO 27001 [ISO, 2006].

Nas próximas seções, são mostrados o escopo do trabalho e sua organização.

1.4. Escopo do Trabalho

Esta seção apresenta o escopo deste trabalho, conforme mostrado na figura 1.1.

Este trabalho adota como base as normas ISO 17799 [ISO, 2005] e ISO 27002 [ISO, 2007]. Estas normas contém 11 cláusulas de controle de segurança da informação, que resultam em um total de 39 categorias principais de segurança da informação a serem implementadas para melhoria da segurança em um sistema computacional. Além destas 11 cláusulas de controle de segurança, as normas ISO possuem uma cláusula introdutória específica sobre Análise de Risco, abordando alguns conceitos sobre a Análise, a Avaliação e o Tratamento de Riscos.

Partindo desta cláusula introdutória sobre Análise de Risco das Normas ISO supracitadas, a pesquisa foi focada para os modelos conhecidos de Análise de Risco, a fim de localizar um modelo que se adaptasse a necessidade deste projeto – um modelo de Análise de Risco que possa ser voltado para a segurança da informação – a fim de pautar a metodologia que será desenvolvida no projeto. Dentre vários modelos pesquisados, o modelo *The Australian/New Zeland standard* [ASN, 1999], que será visto mais adiante, foi o que mais se adaptou a essa exigência.

Tendo como base o modelo supracitado, esta dissertação visa atuar dentro dos conceitos de Identificação e Avaliação dos Riscos do referido modelo.

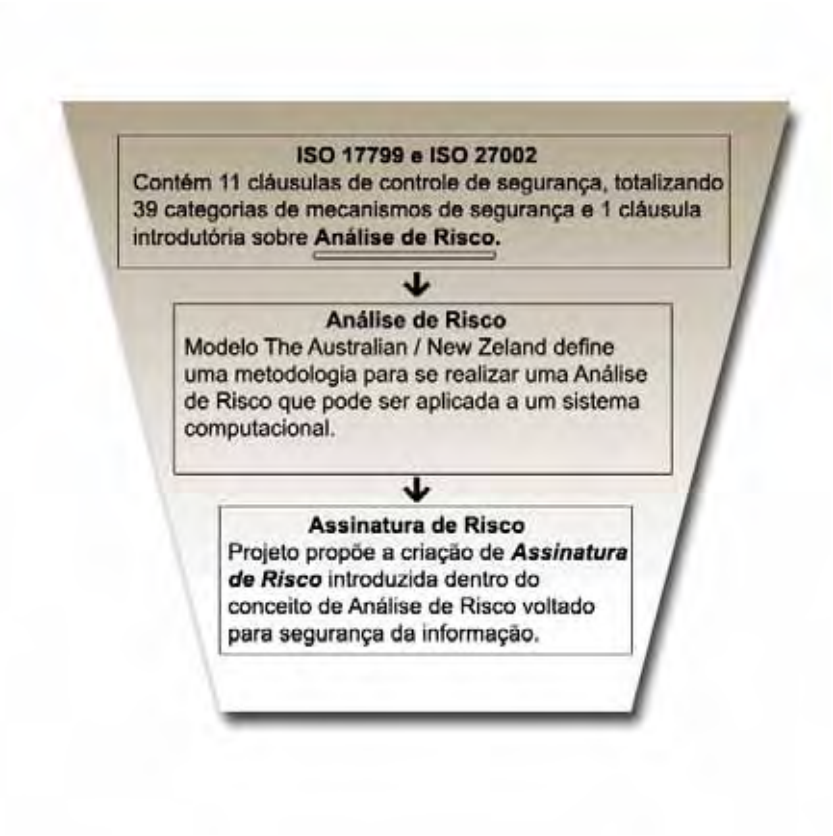

Figura 1.1: Escopo do Trabalho

1.5. Organização do trabalho

Esta dissertação está dividida em capítulos, a saber:

- **Capítulo 1 – Objetivos e Proposta**.

- **Capítulo 2 – Fundamentação**, incluindo revisão de estudos e contribuições da literatura disponível sobre o tema.

- **Capítulo 3 – Desenvolvimento**, contém os aspecto metodológicos envolvidos no tipo de pesquisa utilizada neste estudo, o desenvolvimento da assinatura, adequação às normas ISO e ao modelo AISF.

- **Capítulo 4 – Resultados e Análises,** mostra a aplicação da assinatura em uma análise de risco para um *Web Server*.

- **Capítulo 5 – Conclusões e trabalhos futuros,** mostra as conclusões do trabalho e quais são os trabalhos futuros deste projeto.

- **Referências e Bibliografia**

2. Fundamentação

Este capítulo tem como objetivo apresentar os conceitos básicos necessários para a compreensão deste trabalho.

2.1. Conceitos

Segurança em sistemas computacionais e em redes pode ser definida como a ausência de acesso não autorizado e de manipulação do estado do sistema. O estado do sistema refere-se a qualquer dos seguintes estados: computação, comunicação, armazenamento da informação, interconexão e condição física [AVI, 2004]. Os atributos de segurança são: confidencialidade, integridade, e disponibilidade [NIC, 2004].

Confidencialidade: é a propriedade da indisponibilidade ou não divulgação da informação a indivíduos, processos ou entidades não autorizados [ISO, 2007]. A informação pode ser obtida de forma não lícita através de interceptação, ataques passivos (monitoramento da transmissão), captura de dados de uma rede e cópia de arquivos e programas. Um ataque pode causar uma violação de confidencialidade se este permitir ao atacante acessar dados sem autorização do proprietário da informação [NIC, 2004].

Integridade: é a ausência (não ocorrência) de alterações impróprias nos dados ou no sistema garantindo a exatidão e completeza dos ativos [ISO, 2007]. Um ataque causa uma violação de integridade se permite, de forma não autorizada, ao atacante realizar modificações, alteração de valores em arquivos ou de programas para que estes se comportem de uma forma diferente da original ou modificações de conteúdo de mensagens [NIC, 2004].

Disponibilidade: é definida como a prontidão para o serviço correto, ou a qualidade de a informação ou sistema estar acessível e utilizável toda vez que for requisitado por um individuo, entidade ou processo autorizado [ISO, 2007]. Um ataque causa uma violação da disponibilidade se este impedir que as referidas

entidades autorizadas acessem um recurso de sistema ou dados da instituição quando, onde, e na forma que estas necessitarem. A disponibilidade de um sistema pode ser perdida por interrupções, ataques de negativa de serviço (*Denial of Service – DoS*), ataques do homem do meio (*Man In The Middle – MITM*), falhas no sistema ou em sua infraestrutura, etc. [NIC, 2004].

A norma ISO/IEC 13335 [ISO, 1996] define risco como sendo o potencial com que uma ameaça explorará as vulnerabilidades de um ativo ou de um grupo dos ativos causando perdas ou os danos aos ativos. Risco é uma função da consequência (ou impacto) de um evento não desejado e da probabilidade deste evento ocorrer. Segundo a norma ISO 27002, vulnerabilidade é uma "fraqueza de um ativo ou de um grupo de ativos que pode ser explorada por uma ameaça" [ISO, 2007]. A norma ISO/IEC 15408 define Ameaça como a "causa potencial de um incidente não desejado, que pode resultar em danos para um sistema ou organização" [ISO2, 2005]. A ameaça não pode ser eliminada, apenas antecipada. Mas mecanismos de segurança podem ser adicionados ao sistema para minimizar seus impactos. Ameaças simples ou múltiplas podem explorar vulnerabilidades simples ou múltiplas.

As ameaças são colocadas por um agente de ameaça ou atacante. Diferentes tipos de agentes de ameaça, ou seja, atacantes, têm diferentes atributos e interagem de forma diferente com os ativos e com os controles de segurança. Controles de segurança podem ser administrativos, técnicos ou contramedidas físicas que podem proteger contra uma ameaça, reduzir uma vulnerabilidade, limitar o impacto de um incidente não desejado, detectar estes incidentes e facilitar a recuperação após um incidente [COH, 1998].

A Análise de Risco (*Risk Assessment* ou *RA*) [ISO, 2006] é o processo pelo qual são analisados os relacionamentos entre os riscos, e são estimados os riscos que podem levar ao comprometimento de um ativo. Comprometimento inclui acesso ou divulgação não autorizado, destruição, remoção, modificação, ou interrupção [ROS, 2005].

A Gestão do Risco (*Risk Management* ou *RM*) [ISO, 2006] é o processo de análise de situações, implementando decisões requeridas para controlar o risco e

conseguir algum resultado desejado. Gerenciamento de Risco envolve planejamento, organização, acompanhamento e controle dos recursos e atividades em andamento, a fim de minimizar os efeitos operacionais e financeiros adversos, oriundos de perdas acidentais, sobre a organização [AND, 2001]. A norma ISO 27001 ilustra de forma prática como iniciar a implementação de um Sistema de Gerenciamento de Risco, baseado em um ciclo conhecido pela denominação "*PDCA*" que significa "*Plain, Do, Check, Act*", ou seja, Planejar, Fazer, Verificar, Agir.

Atualmente, muitos mecanismos de segurança vêm sendo sugeridos, comercializados e implementados como contramedidas para diferentes tipos de ameaças contra sistemas computacionais e à segurança da informação. Mas, existem três partes de um sistema computacional que devem ser seguras: (i) comunicação em rede, (ii) base do sistema ou sistema operacional, e (iii) aplicações. Cada um destes componentes do sistema deve ser individualmente analisado e fechado, do ponto de vista de segurança, a fim de se conseguir o nível de segurança desejado [ROS, 2005]. No entanto, para se chegar a esse nível é necessário um embasamento, ou seja, uma metodologia que, dado o sistema e seus componentes, forneça dados acerca de quais mecanismos são viáveis de serem empregados para se alcançar o nível de segurança necessário.

Por se tratar de um assunto relativamente novo, as questões relativas à Análise de Risco frequentemente causam mal entendidos e confusão tanto às pessoas que realizam a análise quanto aos que analisam os resultados, devido a alguns métodos serem um tanto quanto confusos para serem empregados. Existem extensos métodos qualitativos de análise que endereçam todos os riscos de uma forma geral, cobrindo todas as fases do processo de desenvolvimento de um sistema e de sua manutenção. De um modo geral, estes métodos qualitativos de Análise de Risco são eficientes em identificar ameaças e falhas, porém, eles deixam uma grande lacuna no que diz respeito a se mensurar as dependências entre os eventos identificados. É exatamente esta falta de conhecimento destas dependências que este projeto visa atacar, pois nestas lacunas podem estar escondidas falhas de segurança nos sistemas.

Neste capítulo são descritos todos os elementos nos quais o escopo desta dissertação se baseia, começando pela família de normas ISO/IEC 27000, seguido

pelo Modelo *The Australian/New Zeland*, uma introdução sobre árvores de ataque e uma descrição sobre o modelo AISF.

Antes de detalhar as normas e os modelos para gestão de risco, convém citar um termo muito discutido na literatura de TI ultimamente, a Governança em Tecnologia da Informação. A Governança em TI busca englobar e centralizar todas as metodologias necessárias a uma instituição para implantar um sistema de gestão em seu ambiente de tecnologia, visando prover maior eficiência em sua administração.

O termo Governança em TI surgiu da derivação do termo Governança Corporativa, que consiste em criar e descrever um processo de tomada de decisão. A Governança em TI busca um paralelo entre a tecnologia e administração, buscando subsidiar a área administrativa a fim de prover maior agilidade e certeza no processo de tomada de decisão.

Em paralelo à área de Governança de TI surge a área de *security governance* (Governança em Segurança) que busca complementar a Governança em TI. Enquanto a TI busca subsidiar e fornecer informações à Corporativa, a Governança em Segurança busca a qualidade na segurança em relação a estas informações, ou seja, garantia de confiabilidade, integridade e disponibilidade destas, características importantes a fim de resguardar não só a informação, mas também a imagem da corporação.

2.2. *Sarbanes-Oxley – SOX* [MEL, 2008]

A lei *Sarbanes-Oxley* [MEL, 2008] surgiu nos Estados Unidos, em 2002, motivada por escândalos financeiros coorporativos (dentre eles o da *Enron*, que acabou por afetar drasticamente a empresa de auditoria *Arthur Andersen*). A lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da governança adequada das empresas, pois tal governança não seguia nenhuma normatização nem havia na época legislação que a regulamentasse.

Surgiu inicialmente como um ato de legislação federal, o *The U.S. Public Accounting Reform and Investor Protection* que mais tarde, acabou sendo batizado como a lei *Sarbanes-Oxley* ou *SOX* em homenagem a seus relatores, senador *Paul Sarbanes* e o deputado *Michael Oxley*. A base dessa lei dispõe sobre o esforço para melhoria do gerenciamento corporativo e da qualidade da auditoria, itens estes que pertencem à Governança Corporativa citada anteriormente. A lei criou e definiu vários parâmetros para um melhor controle das companhias de capital aberto e suas subsidiárias que possuem ações negociadas nas bolsas de Nova Iorque e *Nasdaq*.

A partir de sua publicação, o que antes era apenas uma simples recomendação sem valia perante a lei americana, passou a ser uma obrigação legal, definindo deveres e responsabilidades, exigindo uma boa Governança, maior ética nos negócios da empresas com participação no mercado mobiliário, buscando reparar a perda de confiança pública nos empresários norte-americanos e enfatizando uma maior clareza nas informações fornecidas aos investidores americanos, procurando utilizar padrões éticos na divulgação destas informações, atribuindo responsáveis pelas mesmas.

A SOX está organizada da seguinte forma, possui 11 títulos com um total de 1107 seções, que visam atribuir responsabilidades aos diretores das corporações. Segundo a lei, estes ficariam sujeitos a sanções que podem ir desde o pagamento de multas, que podem chegar a alguns milhões de dólares e até a condenação de prisão em regime fechado, bem como a punição aos auditores que legitimarem os balanços destas empresas de forma fraudulenta.

Segundo Mello [MEL, 2008], o controle exercido pela *SOX* nas atividades de auditoria e contabilidade destas empresas de capital aberto acaba afetando diretamente seus sistemas de tecnologia da informação, possibilitando separar os processos de negócios e a tecnologia no ambiente empresarial.

Na lei, a seção 404, trata de todos os processos de tecnologia. Nesta seção estão contidos todos os mandamentos sobre os controles necessários para os processos internos e seus sistemas contábeis, determinando uma avaliação periódica destes processos e obrigando a criação de relatórios financeiros que deverão ser

encaminhados aos órgãos fiscalizadores que confirmarão ou não as informações contidas nestes relatórios.

Estes relatórios são itens de extrema importância, devendo ser claros e diretos. Neles, segundo a *SOX*, alguns itens são obrigatórios, como a confirmação das responsabilidades dos gestores da empresa, as informações sobre a manutenção da base dos controles internos e outros procedimentos (subsídios para auditorias), avaliação sobre o acordo de cumprimento de metas ao final de cada ano contábil, verificação da eficiência dos procedimentos internos para emissão dos relatórios e a declaração de um auditor independente atestando sobre a avaliação dos procedimentos adotados pelos gestores, na qual o auditor é legalmente responsável pelas informações por ele validadas.

Com relação à segurança envolvendo TI, a *SOX* obriga as corporações a utilizarem as melhores práticas de segurança em redes e métodos rígidos para um maior controle e conhecimento da infraestrutura alcançada pela lei. É necessário implantar e manter controles para diversas situações como:

- Invasões em sistemas por *hackers*
- Ataques de negação de serviço ou contra a infraestrutura de rede
- Roubo de informações
- Fraudes internas e externas
- Comprometimento de senhas válidas
- Outros tipos de ameaças relacionadas a segurança da informação que possam vir a afetar o negócio da empresa.

A lei *Sarbanes-Oxley* acaba por afetar e interferir na área de TI em toda a cadeia relacionada à informação e comunicação da empresa. Em certos casos, o impacto é maior, tais como os sistemas financeiros e contábeis, pois estes serão continuamente auditados, sistemas de gerenciamento de logística e um conjunto de sistemas de comunicação e armazenamento das informações. Todos estes sistemas devem estar em plena conformidade com o que é requerido pela *SOX*.

Cabe ao administrador de TI a gestão sobre os recursos tecnológicos que são utilizados por funcionários da empresa e os controles para a fiscalização das aplicações das políticas de segurança utilizadas pela empresa. Cabe a ele também, garantir que tal política esteja plenamente adaptada aos requisitos da *SOX*, dispensando uma atenção especial aos serviços terceirizados, pois apesar de existir um contrato de terceirização de serviços, a empresa é responsável por toda a cadeia de negócio, inclusive os serviços terceirizados. Logo, devem constar na política de segurança cláusulas específicas sobre este assunto.

A *SOX* requer uma conformidade contínua, ou seja, não apenas um ato de certificação e conformidade único, mas sim um processo contínuo. A conformidade deve ser feita trimestralmente. As instituições que não atenderem às conformidades, não apenas da *SOX*, mas todas relacionadas à segurança, estarão sujeitas a uma maior exposição à fraude, publicidade desfavorável, impacto negativo e até mesmo ações judiciais.

As imposições da lei não devem ser vistas apenas como atos burocráticos a mais para serem atendidos e executados, sem fins justificáveis. Deve-se valer da oportunidade e implementar uma política de melhores práticas de segurança. Isso acaba por impactar todas as áreas subsequentes das corporações, tornando-as mais ágeis e competitivas, o que é sempre bem visto no mundo dos negócios, pois a transparência torna-se um atrativo não apenas para os clientes, mas também para os investidores.

A certificação *SOX* depende diretamente de uma política de gestão de risco, pois torna a organização totalmente gerenciada, onde seus riscos são mapeados, catalogados e estudados, atribuindo-se a eles valores, quantificando-os, permitindo assim a criação de controles desses riscos. Dessa forma, a organização passa a ser transparente e apta a operar no mercado americano.

Todo este movimento causado pela publicação da *SOX*, suas sanções e controles impostos, fez com que a ISO criasse a família de normas ISO/IEC 27000, como um padrão internacional para segurança da informação, um código de melhores práticas em segurança da informação mais precisamente, como será visto adiante.

2.3. A família de normas ISO/IEC 27000.

Nesta seção é apresentada a história da família de normas ISO/ IEC 27000, sua evolução e a forma como são estruturadas. Em seguida, segue um resumo da norma ISO / IEC 27002 [ISO, 2007], que é uma extensão da norma ISO / IEC 27001 [ISO, 2006]. Estas normas estabelecem parâmetros e princípios gerais para se iniciar, implementar, manter e melhorar o gerenciamento da segurança da informação de uma organização. Os objetivos esboçados neste padrão internacional fornecem uma orientação geral sobre os conceitos geralmente aceitos na gerência da segurança da informação.

Os controles e os objetivos deste padrão internacional são desenvolvidos para serem implementados a fim de seguirem as exigências identificadas por um processo de avaliação de risco. Este padrão é um guia prático para se desenvolver padrões organizacionais de segurança e práticas de gerência de segurança eficazes, além de ajudar a elevar o nível de confiança das atividades inter-organizacionais.

O padrão possui 11 cláusulas coletivas de controle de segurança, contendo um total de 39 categorias principais de segurança e uma cláusula introdutória sobre análise e tratamento de risco. Cada cláusula contém certo número de categorias principais de segurança, que serão vistas adiante, na qual cada categoria principal de segurança contém:

a) um objetivo de controle que indica o que deve ser obtido; e

b) um ou mais mecanismos que podem ser aplicados para se alcançar este objetivo de controle;

2.3.1. Uma breve história da família das normas ISO/IEC 27000

As normas ISO/IEC da família 27000 vem evoluindo através dos anos, passando por diversas mudanças até hoje. Abaixo segue a sequência destas mudanças até se chegar às normas atualmente utilizadas:

Pouco antes do escândalo da *Enron* que deu origem à lei *Sarbanes-Oxley*, uma série de documentos sobre segurança da informação foram publicados em meados da década de 90.

A primeira referencia sobre segurança da informação, batizada de BS (*British Standard*) 7799, surgiu baseada em dois documentos, o Manual de Política de Segurança da Informação da *Royal Dutch/Shell Group*, que descreve um padrão que dá ênfase a conceitos de segurança dos mainframes, sem fazer referências explícitas à Internet, o que sugere que este fora escrito uma década antes de sua publicação, no início da década de 90, e o Código DTI de Práticas para Gerenciamento de Segurança da Informação, publicado pelo Ministério Britânico do Comércio e Indústria em 1993, na forma de folhetos informais de acompanhamento.

Em 1995, o *British Standard Institute* – BSI – distribuiu a *British Standard* 7799 ou BS 7799, a primeira versão oficial de uma norma de segurança da informação. Em 1999, este mesmo instituto publicou uma segunda parte da BS 7799, denominada de "Parte 2", que descreve um Sistema de Gestão de Segurança da Informação.

Em 2000, depois de um difícil período de reflexão e análise internacional, a BS 7799 foi aprovada pela ISO/IEC e lançada em dezembro como a norma ISO/IEC 17799. Em 2005, a ISO/IEC 17799 foi significativamente atualizada adicionando-se novas sessões e o formato foi alterado para esclarecer cada "guia de implementação" de cada controle por ela descrito.

Após o escândalo da *Enron* e a publicação da *SOX*, a ISO/IEC dá início à construção da família de normas ISO/IEC 27000, com o intuito de que esta família de normas possa pautar os controles exigidos pela *SOX*.

Em 2006, a ISO/IEC publica a norma 27001, a primeira da família de normas 27000, baseada na "Parte 2" da BS 7799 de 1999.

Já em 2007, a ISO/IEC 17799 foi renumerada para ISO/IEC 27002:2007, com algumas modificações e correções a fim de torná-la parte integrante da família de

normas ISO/IEC 27000. Em abril de 2008, na reunião de Quioto, a ISO/IEC lançou um projeto de revisão desta versão de 2007 ao longo dos próximos três anos [I2K, 2008].

2.3.2. Escopo da ISO/IEC 27002

A norma ISO/IEC 27002:2007 é a última versão do "Código de prática para gestão de segurança da informação - Técnicas de Segurança – Tecnologia da Informação" que, como o próprio nome diz, é um padrão de boas práticas para segurança da informação internacionalmente aceito. Dezenas ou centenas de milhares de organizações no mundo seguem esta norma.

Segurança da informação é um tópico amplo e com ramificações em todas as partes das organizações modernas assim como a norma ISO/IEC 27002. Esta norma é relevante a todos os tipos de organizações, incluindo empresas comerciais de todos os tamanhos (desde uma empresa formada por apenas um empregado a multinacionais gigantes), organizações sem fins lucrativos, repartições públicas, governo, autarquias, qualquer organização que manipule ou dependa de alguma informação. Os requisitos específicos de Segurança da Informação podem ser diferentes em cada caso citado anteriormente, no entanto, a norma ISO/IEC 27002 tenta abranger todos estes pontos.

A norma diz respeito explicitamente à Segurança da Informação em um contexto amplo e geral, ou seja, a segurança de todos ativos que estão diretamente envolvidos com a informação propriamente dita, e não apenas aos sistemas de TI que manipulam estas informações, como a maioria pensa.

Os departamentos de TI são, geralmente, apenas custodiadores de boa parte dos ativos relacionados com as informações de uma organização e carregados com segurança, atribuindo a uma pessoa responsável o gerenciamento destes ativos – geralmente gerentes de TI juntamente com suas equipes. No entanto, ao contrário do que se imagina, uma grande parte das informações de uma empresa pode estar na forma escrita – mídia impressa, livros, documentos, etc. – e também na forma intangível, como por exemplo, o conhecimento e experiência dos empregados, onde em ambos os casos, nada tem a ver com a área de TI.

Logo, como citado anteriormente, a norma abrange todas as áreas e ativos que estão relacionadas com o ativo mais preciso de uma organização, a informação [I2K, 2008].

Cabe ressaltar neste momento como se dá o relacionamento entre as normas 27001 e 27002.

A norma ISO/IEC 27001 define formalmente os requisitos necessários para a construção de um SGSI – Sistema de Gerenciamento de Segurança da Informação. Ela incorpora em seu Anexo A um sumário dos controles da ISO/IEC 27002.

Atualmente, esta norma é amplamente divulgada e reconhecida pelo mercado como principal padrão de segurança da informação. Propõe a criação e manutenção de um Sistema de Gestão da Segurança da Informação e seu certificado é um dos mais buscados por empresas hoje em dia, pois com ele, cresce a relação de confiança de seus clientes e parceiros, proporcionando vantagens competitivas.

Ela utiliza o anexo A e, consequentemente, a norma ISO/IEC 27002 para indicar controles de Segurança da Informação adequados, que devem ser utilizados no SGSI. No entanto, como a norma ISO/IEC 27002 é apenas um código/guia de boas práticas em segurança da informação, as organizações são livres para selecionar e implementar outros controles não constantes nesta norma, de acordo com suas necessidades.

A norma ISO 27001 define que a segurança da informação deve atuar como um processo conhecido como ciclo PDCA (*Plan-Do-Check-Action*) (Planejar-Fazer-Verificar-Agir), ver Figura 2.1, que requer gestão e controle sobre o que se quer administrar.

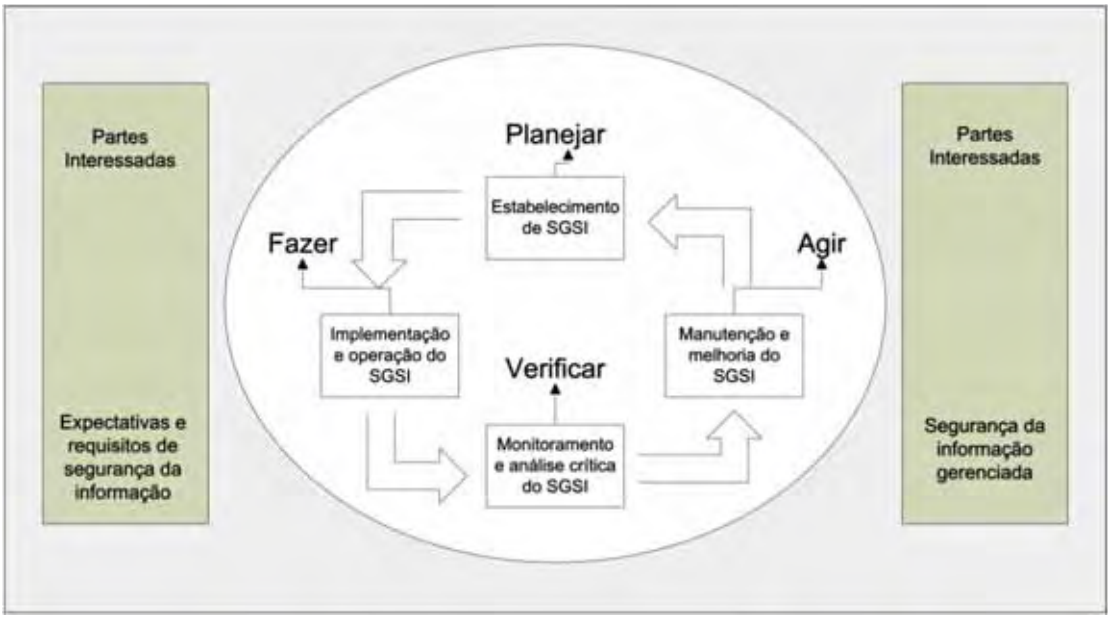

Figura 2.1: O ciclo PDCA da ISO/IEC 27701 [MEL, 2008]

Na fase Planejar, a meta é criar uma política para o SGSI, definindo objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e melhoria da segurança da informação.

Possuir a certificação ISO/IEC 27001 significa que a organização implementa e mantém de forma sistemática a gestão da segurança da informação, valendo-se do gerenciamento destes riscos que podem prejudicar o negócio. A norma estabelece uma definição, de maneira geral e abrangente, sobre os processos indispensáveis para o gerenciamento da segurança, destacando-se a definição de responsabilidades dentro da corporação no gerenciamento de riscos e a implementação de controles, visando o conhecimento tecnológico e procedimentos e processos de auditoria constantes a fim de se obter uma melhora contínua da qualidade. A norma também estabelece parâmetros para a gestão do risco, esses são: avaliação do risco, tratamento do risco, aceitação do risco e a comunicação do risco.

Dentre as recomendações constantes na norma ISO/IEC 27001, existe uma que se refere à implementação e operação de controles para se gerenciar riscos de segurança da informação de uma organização, no contexto de riscos de negócios globais da organização. É recomendado criar ou definir uma estratégia de avaliação

de riscos da organização, identificando uma metodologia de avaliação de risco adequada ao SGSI.

Após implementar um SGSI, a empresa estará preparada para agir pró - ativamente, antecipando os riscos, planejando e implementando soluções, medindo resultados e melhorando continuamente a segurança de um dos seus principais patrimônios – a informação.

2.3.3. Estrutura e forma da norma ISO/IEC 27002

A ISO/IEC 27002 é um código de boas práticas, ou seja, um documento consultivo genérico, e não verdadeiramente uma norma ou especificação formal, como a ISO/IEC 27001. Ela define um conjunto estruturado de controles, sugeridos para tratar os riscos de segurança das informações que abrangem os aspectos da confidencialidade, integridade e disponibilidade.

As organizações que adotam a norma ISO/IEC 27002 visam avaliar seus próprios riscos à segurança das informações e aplicar os controles adequados a fim de minimizá-los utilizando esta norma como orientação.

A norma sugere um vasto número de controles a serem vistos adiante, no entanto, ela não indica ou mostra quais controles podem ou não serem aplicados para cada caso em estudo, o que é um dos objetivos deste trabalho. Além disso, nenhum dos controles sugeridos pela norma é obrigatório, mas se uma organização que deseja ser certificada conforme a norma ISO/IEC 27001 optar, por exemplo, por não aprovar algo tão comum como a utilização de antivírus em suas máquinas, esta certamente deve estar preparada para demonstrar que esta decisão foi alcançada através de uma opção racional de gestão dos riscos de processo, e não apenas devido a uma ordem superior.

A seguir, será mostrado como a norma ISO/IEC 27002 está estruturada.

2.3.4. Objetivos de Controle

Após a introdução, o escopo, a terminologia e a estrutura das seções, a norma ISO/IEC 27002 especifica 39 objetivos de controle para proteger os ativos ligados às informações das ameaças à sua confidencialidade, integridade e disponibilidade. Estes objetivos de controle, em efeito, compreendem uma especificação genérica de requisitos funcionais para uma arquitetura de gerenciamento de controles de segurança da informação em uma organização.

Contestar este objetivos de controle seria algo um tanto quanto incomum, pois seria muito difícil criar um argumento convincente para explicar o porquê de uma organização não estar em conformidade com estes objetivos de controle. Porém, alguns destes não são aplicáveis a todos os casos, os controles genéricos da norma não refletem necessariamente os requisitos necessários a cada organização.

No entanto, na maioria dos casos, estes objetivos de controle fornecem um excelente ponto de partida para definir um conjunto abrangente de axiomas ou de princípios de alto nível para políticas de segurança da informação, apenas com algumas ligeiras modificações em sua redação [I2K, 2008].

2.3.5. Controles específicos

Considerando o Anexo A da norma ISO/IEC 27001 que se refere a 139 controles, estes são, na realidade, apenas seções na norma ISO/IEC 27002, no qual e muitas destas propõem múltiplos controles de segurança específicos. A ISO/IEC 27002 sugere, literalmente, centenas de medidas de controle para melhores práticas em segurança da informação que as organizações devem considerar a fim de contemplar os objetivos de controle listados na ISO/IEC 27001.

A não obrigatoriedade destes controles específicos é um item chave que faz com que a norma seja amplamente aplicada, até mesmo como sendo a tecnologia de segurança, e dá aos utilizadores uma enorme flexibilidade em sua implementação. Com isso, a tarefa dos órgãos certificadores também acaba se tornando difícil, pois estes necessitam avaliar se uma organização está em plena conformidade com a

norma e, no entanto, não há um documento formal que os certifique na norma ISO/IEC 27002 propriamente dita.

Porém, as organizações podem implementar um Sistema de Gestão da Segurança da Informação como um todo, baseado na norma ISO/IEC 27001, valendo-se da norma ISO/IEC 27002 como fonte de controles ou também utilizando outras fontes, a fim de obter informações de segurança monitorando/gerenciando os processos.

2.3.6. A norma ISO/IEC 27002

Esta seção é um resumo do conteúdo da norma ISO/IEC 27002 da forma como a norma está estruturada. A figura 2.1 resume os principais pontos da norma e suas seções. As seções são descritas a seguir:

Figura 2.2: A norma ISO / IEC 27002 [I2K, 2008]

Seção 0: Introdução

Esta seção parte da questão ”O que é a segurança da informação?” e faz uma introdução explicando como fazer uso da norma.

Seção 1: Escopo

Apresenta recomendações para gestão da segurança da informação destinadas àqueles que são responsáveis pela preparação, implementação ou manutenção da segurança.

Seção 2: Termos e Definições

O termo “Segurança da Informação” é expressamente definido como a “preservação da confidencialidade, integridade e disponibilidade da informação”. Além destes, outros termos relacionados são também definidos nesta seção.

Seção 3: Estrutura da Norma

Esta seção explica que a essência da norma está em conter objetivos de controle, sugestões de controles e guias de implementação.

Seção 4: Avaliação de Riscos e Tratamentos

A norma ISO/IEC 27002 atual refere-se ao tema da Gestão de Risco em apenas uma página e meia, o que é um tanto quanto inadequado para a cobertura deste complexo tema que é um elemento central da segurança da informação atualmente, no qual este projeto visa atuar.

Seção 5: Política de Segurança

Nesta seção a norma dispõe a respeito de como deve ser estruturada uma política de segurança da informação, definindo os responsáveis pela construção e

manutenção da mesma e provendo diretivas de forma curta e direta para pautar a construção desta.

Seção 6: Organização da Segurança da Informação

Define uma estrutura de gerenciamento da segurança da informação flexível que deve ser concebida e implementada. Esta seção está dividida em duas sub-seções, Organização Interna e Partes Externas, nas quais são definidos parâmetros para organizar internamente a segurança da informação na instituição e controlar a segurança da informação quando são introduzidos produtos e serviços providos por terceiros.

Seção 7: Gestão de Ativos

Nesta seção a norma cita que uma organização deve estar em posição de compreender quais são as informações que detém ativos, ou seja, possuem um determinado valor, e gerir adequadamente a sua segurança. Para isso ela deve definir responsáveis por estes ativos, relacionando através de inventários os bens relacionados à segurança da informação (hardware, software, dados, sistema de documentação, armazenamento, equipamentos de suporte aos ativos, tais como ar-condicionado, *no-breaks* e geradores, além dos serviços de manutenção) e classificando a informação segundo a sua necessidade de segurança e de proteção, rotuladas de acordo com a classificação recebida.

Seção 8: Segurança em Recursos Humanos

A organização deve gerenciar os direitos de acesso ao sistema e ativos tanto para empregados ou prestadores de serviços, recém-contratados e até antes mesmo da contratação, ou que estão na ativa ou que estão se desligando da organização. Além disso, deve desenvolver trabalhos de conscientização sobre a segurança da informação, além de promover cursos e atividades educativas.

Seção 9: Segurança Física e de Ambiente

Equipamentos de TI valiosos à organização deverão ser fisicamente protegidos contra danos acidentais ou maliciosos, ou perda, superaquecimento, perda de potência elétrica, etc. Esta seção está dividida em duas sub-seções, Áreas Seguras e Segurança de Equipamentos, que descrevem a necessidade de camadas concêntricas de controles físicos para proteger instalações sensíveis ao acesso não autorizado que estão vinculadas aos ativos da organização.

Seção 10: Gerenciamento das Operações e Comunicações

Esta seção longa e detalhada descreve o padrão de segurança para os sistemas de controle e o gerenciamento das redes, abrangendo várias áreas relacionadas às operações e comunicações da organização de seu modo mais amplo possível. Está dividida nas seguintes sub-seções: Procedimentos e responsabilidades operacionais, Gerenciamento de serviços terceirizados, Planejamento e aceitação dos sistemas, Controles sobre códigos maliciosos, Cópias de segurança, Gerenciamento da segurança em redes, Manuseio de mídias, Troca de informações, Serviços de correio eletrônico e Monitoramento.

Seção 11: Controle de Acesso

Acesso lógico aos sistemas de TI, redes e dados deverão ser devidamente controlados para evitar a utilização não autorizada. Esta é uma seção detalhada que diz respeito a todos os requisitos de controle de acesso aos ativos de uma organização de uma forma ampla e completa. Está sub-dividida em: Requisitos de negócios para controle de acesso, Gerenciamento de acesso do usuário, Responsabilidades do usuário, Controle de acesso à rede, Controle de acesso ao sistema operacional, Controle de acesso à aplicação e à informação e Computação móvel e trabalho remoto.

Seção 12: Aquisição, desenvolvimento e manutenção de sistemas de informação

Rege que a segurança da informação deverá também ser levada em consideração durante os processos de especificação, construção/aquisição, análise, implementação e manutenção dos sistemas de TI a fim de garantir a segurança da organização em todas as etapas anteriores. Esta seção diz respeito a este tema fornecendo subsídios para a implementação de controles de segurança nestas etapas e está dividida em: Requisitos de segurança de sistemas de informação, Processamento correto nas aplicações, Controles criptográficos, Segurança dos arquivos do sistema, Segurança em processo de desenvolvimento e de suporte e Gestão de vulnerabilidades técnicas.

Seção 13: Gestão de incidentes de segurança da informação

Nesta seção a norma dispõe sobre a gestão dos incidentes de segurança da informação. Diz que as informações sobre eventos de segurança, incidentes e falhas deverão ser prontamente comunicadas e devidamente tratadas. Para isso, propõe a criação de um modelo de gestão destes incidentes. Está dividida em duas subseções: Notificação de fragilidades e eventos de segurança da informação e Gestão de incidentes de segurança da informação e melhorias.

Seção 14: Gestão da continuidade dos negócios

Esta seção descreve o relacionamento entre a área de TI e o planejamento de recuperação de desastre, gestão da continuidade de negócios e planejamento de contingência, que vão desde a análise e documentação até exercícios regulares e testes destes planos. Estes controles são destinados a minimizar o impacto de incidentes de segurança que ocorreram, apesar dos controles preventivos referidos em outros pontos da norma.

Seção 15: Conformidade

Esta seção fala sobre a conformidade dos processos de segurança da informação, tanto no aspecto técnico, como no aspecto legal, citando controles para se

ter conformidade nas normas e políticas de segurança da informação da empresa e colocando ainda considerações sobre auditorias de sistemas de informação.

Finalizada esta seção que resume a história e o conteúdo das normas ISO da família 27000, em seguida, é descrito o modelo *The Australian/New Zeland.*

2.4. O modelo *The Australian/New Zeland*

Atualmente existem alguns modelos conceituais para Análise de Risco amplamente reconhecidos e padronizados. Neste projeto, para a construção da assinatura, foi utilizado como base o modelo *The Australian/New Zeland* [ASN, 1999]. Este modelo foi escolhido devido ao fato de ser, dentre os modelos conhecidos, o que melhor se ajusta na Análise de Risco voltado para segurança. Este modelo é dividido em cinco fases sequenciais como mostrado na figura 2.3:

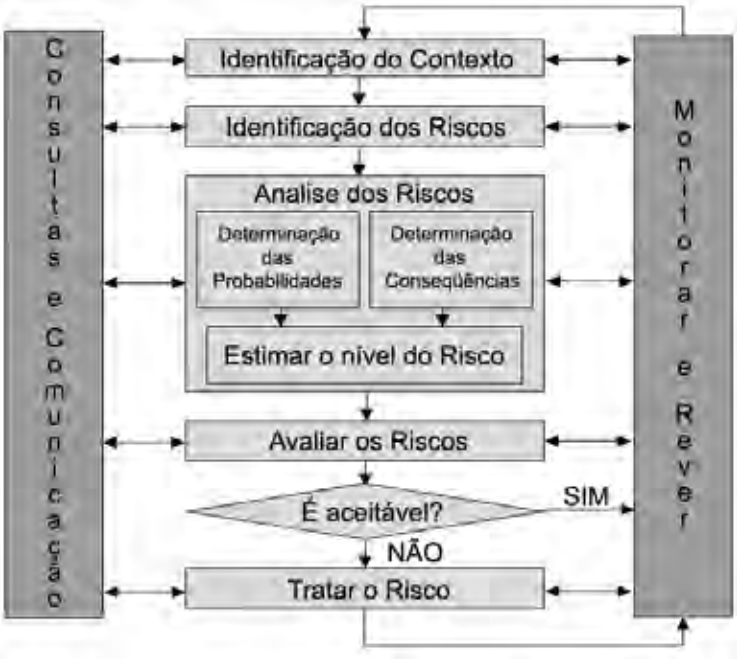

Figura 2.3: Uma visão geral do modelo [ASN, 1999].

Cada fase é dividida em subprocessos sequenciais, como ilustrados na figura 2.4:

Figura 2.4: O processo sequencial de análise [ASN,1999].

A seguir serão descritos os subprocessos mostrados na figura 2.4 e os conceitos envolvidos em seu funcionamento:

1. **Identificação de contexto:** Esta atividade consiste na identificação da área de interesse, identificação e avaliação dos recursos, e identificação dos requisitos de segurança.
   - **SWOT (*Strengths, Weaknesses, Opportunities and Threats*):** Este conceito, como o próprio nome diz, é utilizado para relatar a organização e o seu ambiente, identificando na organização os pontos fortes, as fraquezas, as oportunidades e as ameaças. Este contexto pode incluir o lado financeiro, operacional, competitivo, político, social, do cliente, cultural e aspectos legais das funções da organização detentora do sistema cliente.
   - **Contexto organizacional:** Antes de iniciar a Análise de Risco é necessário entender a organização e suas capacidades/potencialidades, assim como quais são suas metas, objetivos e estratégias utilizadas para atingi-las.
   - **Alvos:** Este conceito descreve as metas, objetivos, estratégias, escopo e parâmetros do sistema cliente a ser submetido à análise do risco.

- **Recursos:** Este conceito visa identificar os recursos e suas dependências assim como classificá-los dentro do sistema, de acordo com sua prioridade, baseado nas análises anteriores do contexto organizacional da empresa.
- **Requisitos de segurança:** O objetivo desta atividade é identificar requisitos de segurança para preservar os recursos identificados e avaliados no item anterior. Estes requisitos podem ser classificados como requisitos de confidencialidade, de integridade, de disponibilidade e de contabilidade (*log's* para supervisão).
- **Critério de avaliação dos riscos:** Este conceito descreve o critério utilizado para a avaliação de cada um dos riscos a serem classificados. Neste conceito serão especificadas as condições que deverão ser seguidas para que o sistema se comporte dentro do nível de risco requerido.

2. **Identificação dos riscos:** Esta atividade consiste na identificação de ameaças e vulnerabilidades dos recursos do sistema.
   - **Cenários de ameaças:** Este conceito é utilizado para identificar ameaças potenciais contra cada recurso identificado, e exibe um entendimento mais detalhado do sistema cliente a ser avaliado.
   - **Incidentes não desejados:** Este conceito contém desvios em potencial do comportamento do sistema. A diferença entre este conceito e o anterior está no fato de o anterior ser baseado em documentação de ameaças conhecidas que podem levar a comportamentos não desejados do sistema cliente, enquanto este consiste em análises de situações onde alguma ameaça tem levado o sistema ao comportamento não desejado, ou seja, dada a consequência, procura identificar as ameaças que podem levar àquela consequência.
   - **Identificação de vulnerabilidades:** Este conceito lista as fraquezas em potencial dos recursos do sistema cliente.

3. **Análise de Riscos:** Para realizar a análise dos riscos, é executada uma medida de consequência/impacto e estimada a probabilidade de ocorrência de cada risco.
   - **Estimativa das consequências:** Na atividade anterior, as consequências das ameaças são identificadas de forma concreta no conceito de incidentes não desejados, nesta atividade, o objetivo é determinar o nível de importância destas, isto é, seu impacto. Para descrever isto, é focado o conceito de *consequência* que contém as estimativas para cada resultado indesejado identificado, e uma descrição de cada uma destas consequências.
   - **Frequência de ameaças ao sistema:** esta atividade visa produzir um modelo em que serão especificadas as estimativas de frequência para as ameaças identificadas, ou seja, uma medição do número de vezes em que cada ameaça identificada foi registrada.
   - **Frequência de ocorrências de incidentes:** O objetivo deste conceito é determinar a probabilidade de ocorrência dos incidentes não desejados. Esta probabilidade depende de vários fatores, tais como, o valor do recurso sob ataque no âmbito do sistema cliente, as vulnerabilidades do recurso, e o grau de facilidade para a exploração destas vulnerabilidades. Todos estes fatores devem gerar dados a serem coletados do sistema cliente, a fim de se criar um espaço amostral grande o suficiente para gerar uma estimativa de frequência de ocorrências.

4. **Avaliação dos Riscos:** esta atividade visa avaliar riscos, o que significa determinar o nível, a prioridade e a categoria dos riscos, agrupando-os por temas ou categorias, além de determinar o relacionamento entre as categorias de riscos e atribuir prioridades a estas categorias resultantes destes relacionamentos.
   - **Estimativa de risco:** nesta atividade, o impacto de uma ameaça e sua probabilidade de ocorrência são combinados para estimar o nível do risco. Para isso, é construído um modelo que especifica o

nível do risco para cada incidente não desejado identificado anteriormente.

- **Prioridade dos riscos:** o objetivo aqui é avaliar cada incidente não desejado ordenando-os de acordo com o seu nível de risco estimado. Os riscos poderão ser priorizados de acordo com sua estimativa e outros fatores como se existisse a possibilidade de prevenção do risco, e esta ser possível de ser realizada.
- **Classes de riscos:** nesta atividade os riscos são organizados em classes ou temas, baseados em características comuns. Dessa forma, poderemos tornar os processos de tratamento mais eficientes, tratando-os em lote e não individualmente. Os riscos poderão ser agrupados de acordo com os meios ou ferramentas que poderão ser usados para preveni-los de uma ocorrência. O conceito de Taxonomia de Risco baseado em [WEB, 2005] é utilizado neste conceito para realizar a classificação dos riscos.
- **Relacionamentos entre classes de risco:** as relações de causa e efeito entre os riscos identificados serão listados nesta atividade. Ela ajudará no entendimento de um conjunto de riscos e na determinação dos inter-relacionamentos e dependências a serem consideradas posteriormente no desenvolvimento dos estágios de proteção. A idéia nesta atividade é determinar tipos de relacionamentos entre classes de risco. Estes relacionamentos poderão ser do tipo: “em conflito com”, “impede que” ou “suporta”, entre outros. Por exemplo, se for utilizada criptografia de chaves assimétricas para acesso a informações em um servidor, poderá ser comprometida a disponibilidade da informação e o seu monitoramento, se for o caso.
- **Prioridades de classes de risco:** Por fim, esta atividade fará uma classificação da classe de risco de acordo com as estimativas dos riscos contidos nesta, construindo assim um “ranking” dos problemas mais críticos com maior probabilidade de se tornarem uma ocorrência.

5. **Tratamento dos Riscos:** Esta é a atividade final no processo de Análise de Risco, que consiste na identificação das possíveis opções para o tratamento destes riscos e apresentação de métodos ou alternativas para a solução dos problemas identificados.
    - **Política de segurança:** um dos principais itens para tratamento de riscos e combate a vulnerabilidade é especificar uma política de segurança. Este conceito visa construir ou realizar alterações na política de segurança para que esta possa tratar os problemas identificados anteriormente.
    - **Requisitos de segurança:** foram identificados anteriormente os requisitos de segurança constantes no sistema cliente. Esta atividade visa reavaliar estes requisitos, reforçando-os de acordo com as necessidades identificadas no conceito de Avaliação dos Riscos, dessa forma, preparando-os para lidar com os riscos e ameaças encontrados.
    - **Arquitetura segura:** esta é uma possibilidade a ser considerada para o tratamento dos riscos encontrados. Criar uma arquitetura voltada para a segurança ou alterar a arquitetura atual do sistema cliente para uma arquitetura segura a fim de que este possa lidar com os problemas identificados é a proposta deste conceito.
    - **Teste:** esta atividade consiste em realizar testes nos requisitos de segurança do sistema a fim investigar a existência de mais problemas em potencial.
    - **Monitoramento:** este conceito visa especificar um mecanismo de monitoramento do sistema a fim de que este possa fornecer dados que auxiliem no tratamento de problemas de segurança em potencial. Mecanismos de monitoramento de tráfego, servidores de log's e outros que já existam no sistema cliente deverão ser revistos neste momento, retrocedendo ao conceito anterior de teste para identificar possíveis falhas nestes serviços.

Devido a este modelo ser conhecido e utilizado na literatura na área de análise de risco, o desenvolvimento da assinatura de risco desta dissertação de mestrado

toma-o como base, buscando atender aos conceitos nele relacionados a fim de garantir que todos os passos de uma análise de risco sejam cumpridos. A próxima seção mostra uma introdução sobre árvores de ataque, estrutura em que a assinatura de risco desenvolvida está baseada.

2.5. Árvores de ataque [SCH, 2001]

Árvores de ataque são estruturas que oferecem um meio metódico de se descrever ataques ou ameaças a um sistema e apresentar contramedidas a estes ataques a fim de evitá-los. Por extensão, as árvores de ataque oferecem um modo metódico de se representar a segurança dos sistemas. Elas permitem realizar estudos sobre o nível de segurança ou comparar a segurança de diferentes sistemas.

Basicamente, para se representar um ataque a um sistema utilizando uma estrutura em forma de árvore, deve-se partir do objetivo do ataque, a ser colocado na raiz da árvore e as diferentes maneiras de se conseguir este objetivo, devem ser colocadas como os nós folhas. Atribuindo-se valores aos nós, é possível realizar alguns cálculos básicos com a árvore, para se produzir afirmações sobre diferentes ataques contra o objetivo.

2.5.1. Árvores de ataque básicas

A figura 2.5 mostra uma árvore de ataque simples que mapeia um ataque contra um cofre físico. Cada árvore de ataque possui um objetivo, representado pelo nó raiz na árvore. O objetivo neste exemplo é abrir o cofre. Para abrir o cofre, o atacante pode atacar a fechadura, descobrir a combinação, cortar o cofre ou instalar o cofre incorretamente para que possa abrí-lo facilmente mais tarde.

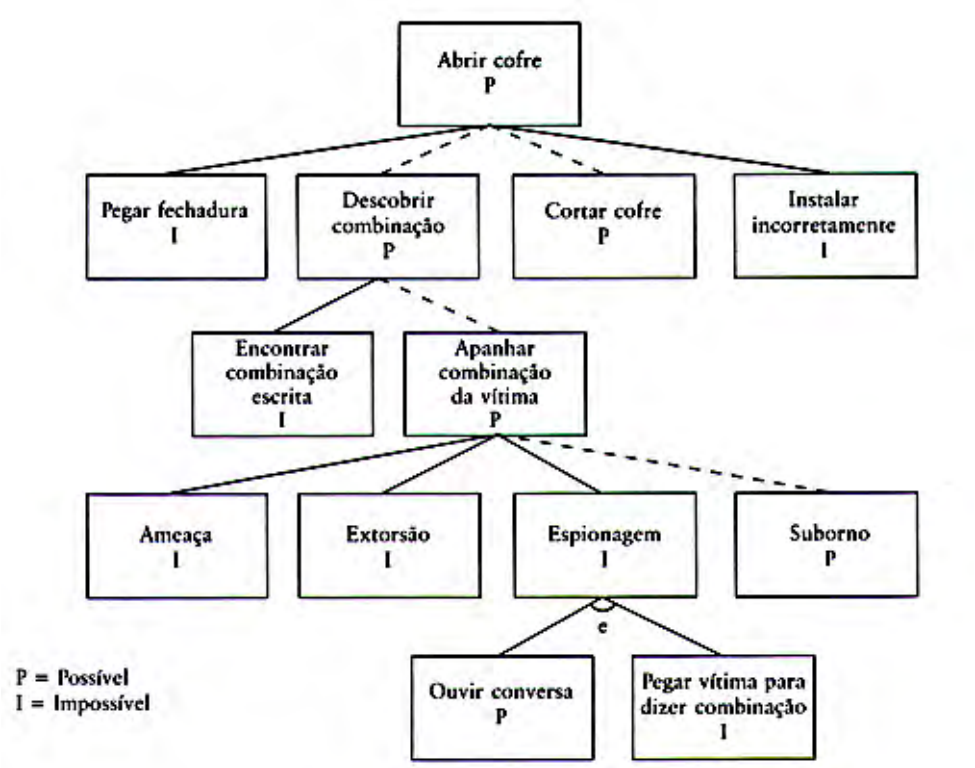

Figura 2.5: Exemplo de árvore de ataque [SCH, 2001].

Para descobrir a combinação, o atacante precisa encontrar a combinação escrita ou apanhá-la com o proprietário do cofre, e assim por diante. Cada nó então, torna-se um sub-objetivo, e os filhos desse nó são maneiras de se conseguir esse sub-objetivo.

Podemos observar na árvore que a mesma possui nós E e nós OU, onde, todo nó que não explicitar a assinatura de E, é considerado um nó OU. Os nós OU são alternativas: as quatro maneiras diferentes de se abrir o cofre, por exemplo. Nós E, representam diferentes etapas para se conseguir o mesmo objetivo. Neste caso, para espionar alguém dizendo a combinação do cofre, o atacante precisa espionar a conversa E fazer com que os proprietários do cofre digam a combinação. O atacante não pode conseguir o objetivo a menos que os dois sub-objetivos sejam satisfeitos.

Na figura 2.5, podemos adicionar aos nós algumas características, atribuindo valores aos nós, por exemplo, I = impossível e P = possível, para os nós folha da árvore. Quando se atribui tais valores, neste caso, presume-se que estas atribuições sejam os resultados de uma pesquisa completa no próprio cofre, será possível calcular

a segurança desse objetivo. Por exemplo, o valor de um nó OU é possível se qualquer um de seus filhos for possível, e impossível se todos os seus filhos também o forem. O valor de um nó E só é possível se todos os filhos forem possíveis, e impossível em caso contrario. As linhas tracejadas na figura 2.5 mostram todos os ataques possíveis, ou seja, uma hierarquia de nós possíveis desde uma folha até o objetivo.

Atribuir valores como I e P aos nós é apenas uma maneira de se ver a árvore. Qualquer valor sim/não poderá ser atribuído aos nós da árvore e depois propagado para cima na estrutura, dessa mesma forma. Além de valores binários, do tipo, sim/não, possível/impossível, os nós da árvore podem também receber valores do tipo custo para se cumprir um objetivo, dessa forma pode se obter o custo total envolvido em um ataque e também se o ataque necessita ou não de algum equipamento especial para ser concretizado, conforme mostrado na figura 2.6.

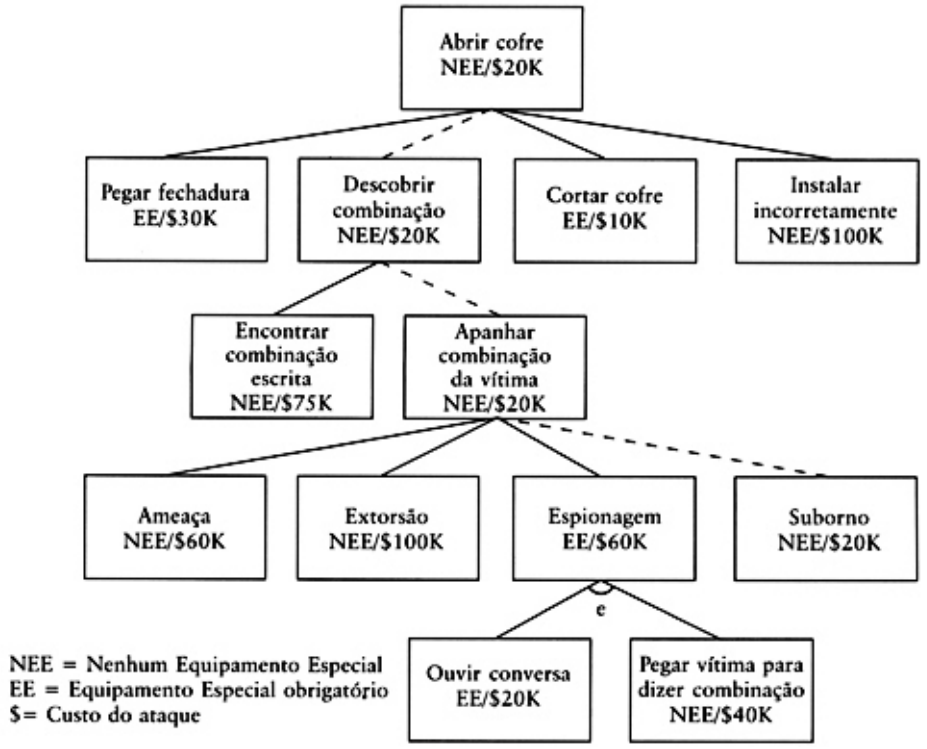

Figura 2.6: Uma árvore de ataque com atributos [SCH, 2001].

Na figura 2.6, a linha pontilhada nos mostra o ataque mais barato e que não necessita de nenhum equipamento especial para ser executado.

2.5.2. Ataques e Acidentes

Cabe neste ponto uma observação importante sobre árvores de ataque relacionada aos tipos de eventos que estas representam.

Existem dois tipos de ocorrências que podem comprometer a segurança de um sistema computacional. Uma ocorrência causada por uma escolha consciente e deliberada através do uso de um *exploit* é chamada de ataque. Ocorrências que resultam de eventos não intencionais, aleatórios ou de magnitude natural são chamadas acidentes.

As árvores de ataque focam principalmente ataques e não acidentes. Entretanto, em uma metodologia de análise de riscos, os riscos de que um acidente ocorra não podem ser desconsiderados. Logo, no modelo proposto nesta dissertação de mestrado, apesar de se basear nos conceitos de árvores de ataque, estes riscos são considerados.

A seguir, veremos uma breve descrição do modelo AISF – ACME! *Instrusion Signature Format* [SIL, 2002].

2.6. O modelo AISF - *ACME! Intrusion Signature Format* [SIL, 2002]

O AISF é uma estrutura de dados organizados em um conjunto independente de módulos contendo informações relacionadas, que permitem descrever de forma precisa e concisa as assinaturas de intrusão, modelando desde características descritivas ao conteúdo de dados dos pacotes.

Sua organização é baseada na especificação da linguagem XML (*Extensible Markup Language*) e DTD (*Document Type Definition*) [W3C, 2002]. XML permite criar uma marcação específica, definindo e compartilhando as idéias, caracterizando exatamente as capacidades que o AISF precisa para unificar e expor suas assinaturas.

O modelo tem como característica básica a divisão em módulos independentes. Essa característica traz benefícios de portabilidade e escalabilidade para o modelo. Cada módulo contém informações fortemente relacionadas e geralmente de necessidade recíproca.

Para que a padronização ocorra de maneira mais natural, o modelo utiliza um sistema capaz de armazenar e gerenciar estas informações. Esse sistema consiste na integração de um banco de dados com uma interface que possibilita a administradores de segurança espalhados pela Internet obter e contribuir com informações. Para tal, ele utiliza o *MySQL* [MyS, 2008], que é um gerenciador de base de dados leve e flexível e a interface utilizada é baseada na linguagem PHP (*Hypertext Preprocessor*) [PHP, 2002].

2.6.1. Visão Geral do Modelo AISF [SIL, 2002]

O AISF pode ser brevemente definido como uma proposta de padronizar a codificação de assinaturas de ataque, influenciando no armazenamento, processamento, intercâmbio e relato destas, de tal maneira que elas possam ser utilizadas livremente entre os sistemas e entidades envolvidas na detecção de ataques. Para o desenvolvimento deste projeto, o modelo foi modificado com o intuito de receber também assinaturas de riscos.

Tecnicamente, o AISF é uma estrutura de dados constituída por um conjunto independente de módulos, os quais servem como repositório de informações que se relacionam de forma intrínseca e que permitem uma documentação concisa e exata das assinaturas, contendo as características descritivas das assinaturas.

Sua organização é baseada na especificação do XML [W3C, 2002], provendo desta forma ganhos no que dizem respeito à simplicidade, adaptabilidade, alta portabilidade, manutenção e uso flexível. A linguagem XML permite que seja criada uma marcação específica para o modelo, definindo as idéias e compartilhando-as, o que caracteriza as capacidades que o AISF necessita para unificar e expor suas assinaturas.

Uma instância do AISF, denominada de agora em diante como AIS (*ACME! Intrusion Signature*), ou objeto AISF, é um documento XML corretamente formatado de acordo com o padrão do modelo, contendo os dados relevantes sobre um evento intrusivo. Com este projeto, o AISF passou a gerenciar além de eventos intrusivos, riscos associados a um sistema computacional. Para cada evento ou risco haverá apenas um objeto AISF, que, no entanto, pode ser revisado e resultar em novas versões.

O AISF é usado para facilitar o modo com que assinaturas de ataque e de riscos são armazenadas e processadas por um SDI (Sistema Detector de Intrusão) ou por uma metodologia de análise de riscos. Em uma visão macro de aplicação do AISF, vários objetos poderão ser armazenados em um banco de dados global, mantido por uma entidade segura, que pode controlar e utilizar estas instâncias, permitindo a adição de novos AISs sobre novos ataques e riscos. Utilizando o AISF, um SDI ou uma metodologia de análise de risco terá um sistema de administração de assinaturas padronizado.

Segundo Silva [SIL, 2002], o AISF poderá ser utilizado por sistemas menos complexos, levando em consideração a análise das assinaturas, como um simples detector de varreduras, ou um analisador de *dumps* gerados por um "*sniffer*" como o *tcpdump* [Tcp, 2008], comparando este *dumps* com os objetos AISF. A reportagem de alertas torna-se facilitada, uma vez que os AISs são gerados com textos descritivos, além dos próprios conteúdos úteis das assinaturas.

2.6.2. Módulos [SIL, 2002]

A utilização de módulos para organização das informações armazenadas é um dos pontos mais importantes do modelo. Segundo Silva, cada AIS é composto por dois ou mais destes módulos. Cada módulo possui um conjunto de campos com informações relacionadas. Toda a assinatura do modelo AISF deve obrigatoriamente possuir um módulo chamado *Signature Identification Module*, que será visto em detalhes adiante.

A organização em módulos tem ainda a sua importância destacada por

viabilizar as funcionalidades do modelo, como por exemplo, possibilitar que sistemas com capacidade de processamento e uso distintos utilizem a mesma estrutura para conseguir as assinaturas e que sistemas menos complexos, como um simples detector de *scans*, utilizem o AISF para conseguir padrões. Neste exemplo, a capacidade modular do modelo possibilita que sejam descartados os módulos que não interessam ao sistema, sem a necessidade de processar essas informações.

Outro aspecto dessa modularização que merece destaque é o que diz respeito ao versionamento do modelo. Este aspecto foi de fundamental importância no desenvolvimento deste projeto. Foram criados e adicionados ao modelo novos módulos para a descrição de assinaturas de riscos. Ainda assim, os programas que foram projetados e desenvolvidos que utilizam versões anteriores do AISF, podem utilizar estes novos AISs apenas descartando os módulos não compreendidos.

Para que estas funcionalidades sejam obtidas, basta que cada módulo do sistema contenha dois campos padrões. O primeiro campo do módulo deve obrigatoriamente ser o *Module Length* que indica quantos campos existem no módulo, contando inclusive ele mesmo. Este só não é utilizado no *Signature Identification Module*, que será visto mais adiante.

O segundo campo obrigatório deverá ser o último denominado *Next Module*, responsável por indicar qual será o próximo módulo apresentado no objeto. O conteúdo desse campo é uma abreviação do nome do módulo seguinte, essa abreviação será apresentada a seguir juntamente com a descrição de cada um deles.

- ***Signature Identification Module (SigIdModule)****:* este é o primeiro e mais importante módulo do AISF. Ele é responsável pela identificação do objeto, assim como alguns detalhes do próprio modelo.
- ***Signature Information Module (SigInfoModule):*** é utilizado para representar informações mais descritivas sobre o ataque, como por exemplo, a descrição do evento intrusivo e os sistemas afetados por este evento. Assim como os módulos subsequentes, este módulo é opcional.
- ***Signature Characteristics Module (SigCharModule):*** pertence à classe dos

módulos informativos, que pode relatar informações inerentes ao ataque, por exemplo, a porcentagem de falsos positivos que o evento pode gerar em um SDI.

- ***Data Link Protocols Module for Ethernet (DlinkProtoModuleEth):*** refere-se aos dados do protocolo de enlace, no caso o Ethernet.
- ***Network Protocols Module for IPv4 (NetProtoModuleIPv4):*** descreve os dados inerentes à camada de rede, e no caso da pilha TCP/IP, o protocolo Ipv4.
- ***Transport and Control Protocols Module for TCP (TransConProtoModuleTCP):*** apresenta dados relativos à camada de transporte da pilha TCP/IP, isto é, o protocolo TCP.
- ***Transport and Control Protocols Module for UDP (TransConProtoModuleUDP):*** corresponde às informações relativas ao cabeçalho do protocolo UDP.
- ***Transport and Control Protocols Module for ICMP (TransConProtoModuleICMP):*** este módulo é responsável por representar informações relativas ao protocolo ICMP.
- ***Payload Information Module (PayloadInfoModule):*** é um dos módulos mais importantes do AISF. Ele pode armazenar informações a respeito da carga dos pacotes numa seção de ataque. É consideravelmente útil para descrever os ataques de penetração, como por exemplo, aqueles que exploram *buffer overflows*. Este módulo também é opcional.

A figura 2.7 mostra um diagrama de inter-relacionamento entre os módulos do modelo.

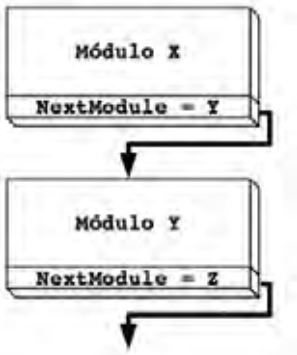

Figura 2.7: Diagrama de inter-relacionamento entre os módulos [SIL, 2002].

A estrutura completa do modelo AISF está descrita no Anexo A desta dissertação.

Para este projeto, foram criados novos módulos para a descrição das assinaturas de risco. Estes seguiram o mesmo padrão e estrutura dos módulos já existentes no modelo AISF, conforme mostrado anteriormente.

Foi visto nesse capítulo a fundamentação teórica necessária para o entendimento do trabalho desenvolvido. O próximo capítulo apresenta a assinatura proposta e o projeto desenvolvido.

3. Desenvolvimento

3.1. Descrição

Este trabalho propõe a criação de uma Assinatura de Risco para ser utilizada em uma metodologia de Análise de Risco, baseada no conceito de árvores de ataque e nas normas ISO/IEC 17799, ISO/IEC 27001 e ISO/IEC 27002, compatível com o modelo AISF de gerenciamento de assinaturas. Esta assinatura deverá ser utilizada como um documento de base para um processo de análise de risco envolvendo ativos da organização.

3.2. Modelagem da assinatura

A assinatura desenvolvida para este projeto deve, para cada ativo da instituição relacionado a segurança da informação a ser analisado, elencar os riscos inerentes a ele, sendo que cada assinatura deve conter informações sobre este ativo, as vulnerabilidades a ele associadas, as ameaças vinculadas a estas vulnerabilidades, os custos e pré-requisitos para que este ativo seja comprometido explorando-se estas vulnerabilidades, o impacto ou prejuízo causado por esta ocorrência e a probabilidade de que tais ameaças sejam exploradas.

Por fim, a assinatura fornecer as contramedidas necessárias para se mitigar os riscos associados aos ativos, baseando-se nos controles dispostos na família de normas da ISO/IEC 27000, identificando quais controles devem ser aplicados em cada um dos casos.

3.2.1. Os controles da norma ISO/IEC 27001

Antes de mostrar a implementação da assinatura, faz-se necessário uma descrição acerca dos controles de segurança dispostos na norma ISO/IEC 27001 em seu anexo A.

Os 133 controles dispostos na norma estão organizados em 11 domínios e 39 objetivos. A nomenclatura destes domínios é organizada da seguinte forma: *A.X.X*, no qual *A* refere-se ao anexo *A* e *X.X* são números que estão alinhados diretamente com os números dos controles listados na norma ISO/IEC 27002, isso explica o primeiro domínio ser denominado A.5. A tabela 3.1 mostra todos os referidos domínios da norma:

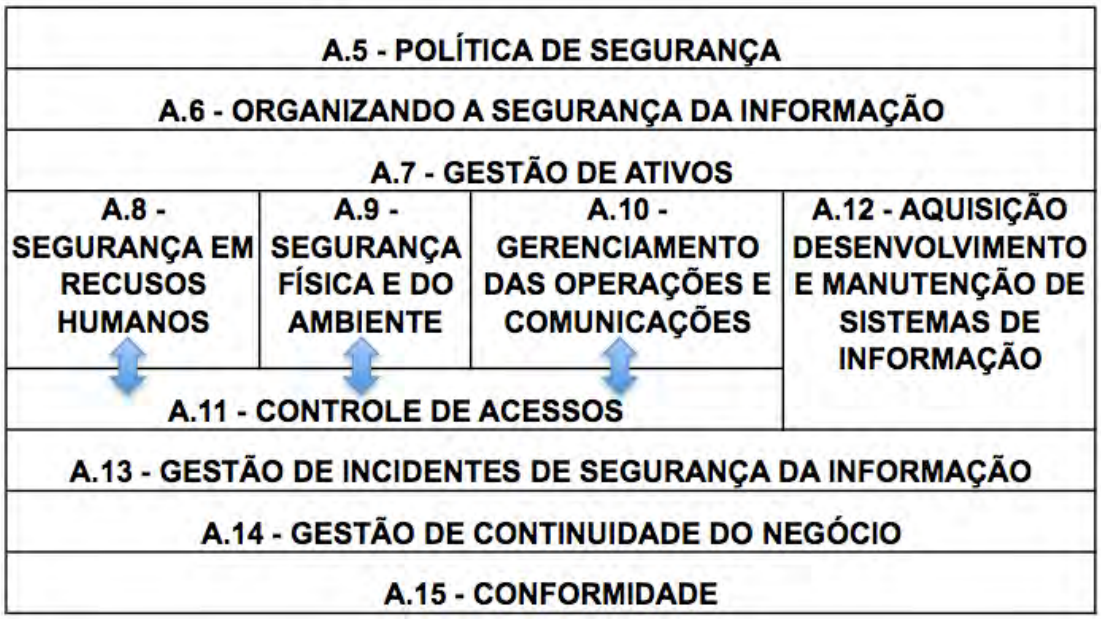

Tabela 3.1: Os domínios da norma ISO/IEC 27001.

Cabe observar que os domínios A.8, A.9 e A.10, possuem um relacionamento direto com o domínio A.11. Isso significa que a implementação dos controles de um contribui diretamente para que o objetivo do outro seja alcançado.

Os objetivos da norma seguem o mesmo padrão de nomenclatura. Por exemplo, no domínio A.7 – Gestão de ativos, a norma dispõe de dois objetivos:

- A.7.1 – Responsabilidade pelos ativos
- A.7.2 – Classificação da informação

Dentro destes objetivos estão os controles a serem aplicados para que estes sejam alcançados. Estes também seguem o mesmo padrão de nomenclatura, alinhado com a ISO/IEC 27002. Por exemplo, o objetivo A.7.2 citado acima, possui dois controles:

- A.7.2.1 – Recomendações para classificação.
- A.7.2.2 – Rótulos e tratamento da informação.

A assinatura desenvolvida faz referência direta aos controles da norma ISO/IEC 27001 através da nomenclatura padrão destes, ou seja, da seguinte forma: *A.X.X.X*. O operador (*) – todos – foi utilizado para se referenciar a todos os controles daquele objetivo, ou até de todos os objetivos e controles daquele domínio, por exemplo: controles aplicáveis – A.7.2.* ou A.7.*, respectivamente.

3.2.2. Métricas utilizadas na assinatura

No processo de avaliação do risco associado à assinatura, é necessária a atribuição de algumas métricas para o cálculo do risco. Algumas destas métricas necessitaram ser quantificadas de tal forma a facilitar a construção da assinatura por parte do analista responsável pelo SGSI.

Como exemplo, para estimar a probabilidade de uma ocorrência é utilizada a tabela 3.2 a seguir:

Probabilidade	Descrição
Muito baixa	Um evento que nunca ou que é altamente improvável de acontecer.
Baixa	Um evento improvável que ocorra, talvez, uma vez a cada três anos.
Média	Um evento que é provável que ocorra de uma forma relativamente frequente.
Alta	Um evento que é bem provável, e que se espera que ocorra várias vezes ao longo do ano.
Muito alta	Um evento que é altamente provável que ocorra, no mínimo uma vez ao mês, ou mais frequentemente.

Tabela 3.2: Cálculo de probabilidade de ocorrência.

No cálculo do impacto potencial de um risco aos negócios da corporação, a assinatura utiliza a tabela 3.3:

Impacto Potencial no Negócio	Operações no Negócio e Saúde Financeira	Obrigações Legais & Regulatórias	Reputação	Informação Pessoal
Baixo	Pouca ou nenhuma perda financeira	Nenhuma obrigação legal ou regulatória	Afeta de forma pequena ou limitada dentro da organização	Não causa embaraço ou constrangimento
Médio	Afeta pouco a eficiência do negócio / saúde financeira	Ruptura técnica de obrigação legal ou regulatória	Afeta de forma adversa as relações com clientes e acionistas	Pequeno embaraço ou constrangimento ao indivíduo
Alto	Causa séria perda financeira	Séria ruptura de requisitos legais ou regulatórios	Afeta seriamente as relações com clientes e acionistas	Sério embaraço ou constrangimento
Muito Alto	Pode levar à falência	Pode levar ao encerramento das atividades da empresa	Ameaça o futuro dos negócios	Embaraço ou constrangimento em larga escala

Tabela 3.3: Cálculo do impacto potencial sobre os negócios.

Cabe observar que o impacto sobre os negócios da empresa pode ser observado sob várias óticas. Na assinatura são consideradas as quatro óticas mostradas na tabela 3.3, Operações no Negócio e Saúde Financeira, Obrigações Legais & Regulatórias, Reputação e Informação Pessoal. Para garantir a flexibilidade do modelo, esta tabela pode ser parametrizada de acordo com as necessidades da instituição. Para determinar o impacto utilizando-se mais de uma ótica, é adotado o critério do maior impacto observado em todas as óticas consideradas.

A definição destas óticas de impacto foi uma das dificuldades encontradas no desenvolvimento deste trabalho. Exceto a ótica vinculada à questão financeira, operações e negócios que é mais comum, as demais e suas discretizações demandaram um tempo grande de pesquisa e construção. Discretizar o impacto com relação às obrigações legais, reputação ou questões pessoais de forma a não causar dúvidas no processo análise do impacto foi uma tarefa dispendiosa, pois estes são assuntos que envolvem um certo grau de subjetividade.

Tendo como base as duas tabelas anteriores, para efetuar o cálculo do valor de um risco a assinatura utiliza a metodologia disposta na tabela 3.4 a seguir, no qual Risco = Probabilidade * Impacto:

X		**Probabilidade**				
		Muito baixa	Baixa	Média	Alta	Muito alta
Impacto	Baixo	1	2	3	4	5
	Médio	2	4	6	8	10
	Alto	3	6	9	12	15
	Muito Alto	4	8	12	16	20

Tabela 3.4: Cálculo do valor do risco considerando-se probabilidade e impacto.

A questão financeira envolvida na análise do risco é uma das principais motivações que levaram ao desenvolvimento deste trabalho, pois, como já citado anteriormente, no mundo dos negócios todo e qualquer investimento deve ser justificado. A assinatura visa facilitar esta justificativa, logo esta dispõe de métricas capazes de fornecer subsídios para estes investimentos.

Justificar o investimento em segurança é algo difícil de ser apresentado pelo analista, pois segurança não é um produto tangível a ser adquirido ou uma prestação de serviço que trará algum lucro ou benefício direto ao investidor.

Dentre as métricas empregadas na assinatura, uma das principais é a que trata dos custos e investimentos envolvidos na análise de risco. Esta é uma métrica complexa para se avaliar. No entanto, para facilitar esta avaliação na construção da assinatura, estes custos foram agrupados de acordo com a visão do lado afetado, ou seja, o lado da instituição e o lado do atacante. Deve ficar claro que este último só existe no caso de ataque, ou seja, de ocorrências intencionais, não sendo considerado em acidentes causados por eventos externos não intencionais ou de causas naturais.

Do lado da instituição detentora do sistema existem dois custos a serem considerados: o custo causado por uma ocorrência de exploração de uma vulnerabilidade do sistema por uma ameaça, que é mensurado no cálculo do impacto visto anteriormente, e o custo de investimento em uma contramedida para evitar a exploração de uma vulnerabilidade. O emprego de contramedidas será mostrado mais

adiante.

No lado do atacante, se este existir, a assinatura considera mais duas outras métricas relacionadas aos custos: o lucro obtido com a exploração de uma vulnerabilidade, ou seja, a motivação do atacante, e o custo do investimento necessário para se obter êxito na exploração, ou seja, o custo/benefício do ataque.

A métrica de custos não deve estar restrita apenas ao aspecto financeiro. Dependendo da análise de contexto feita na construção da assinatura, os custos financeiros de um risco – tidos como investimento monetário propriamente dito – podem não fazer sentido. Por exemplo, um servidor de arquivos de uma universidade não guarda dados financeiramente rentáveis a um atacante de forma direta, como números de cartões de crédito, ou cadastro de pessoas e clientes. Nele estão armazenados informações a respeito de linhas de pesquisa, dados sobre a universidade, trabalhos desenvolvidos, dentre outras informações que possuem valor tangível ou intangível.

Neste caso, os custos devem ser analisados por uma segunda ótica, de maior importância para a instituição, que é a relevância daqueles dados para a instituição detentora e a questão dos danos à reputação ou à imagem desta, caso uma ocorrência seja registrada. Já pensando no lado do atacante, a motivação ou lucro obtido não seria financeiro, mas sim também pela questão de reputação ou roubo de propriedades intelectuais, no caso de um servidor web da universidade.

Para o cálculo e atribuição destes custos no lado atacante, a assinatura utiliza as tabelas 3.5 e 3.6, que também podem ser parametrizadas conforme as necessidades da organização. A primeira métrica analisada é a da motivação, ou seja, o lucro ou benefício obtido pelo atacante com o incidente. Esta métrica é analisada sob duas possíveis óticas: a da notoriedade do fato, e a do lucro financeiro, conforme mostrado nas tabelas 3.5 e 3.6, respectivamente.

Notoriedade	Descrição
Nenhuma	Nenhuma, autor não será reconhecido, fato irrelevante.
Baixa	Divulgado apenas entre poucas pessoas, não trará benefícios ao autor.
Média	Divulgado a pessoas do meio e comunidades locais, autor já é conhecido.
Alta	Divulgado a nível nacional, mídia televisiva, imprensa, etc.
Ampla	Amplamente divulgado, internacionalmente, trará grande 'mérito' ao autor.

Tabela 3.5: Cálculo da notoriedade de um incidente.

Lucro Financeiro	Descrição
Nenhum	Não trará lucro algum, sem remuneração.
Pequeno	Não altera a situação financeira do atacante, pequenos valores.
Médio	Melhoria da situação financeira, atinge o valor de bens móveis, veículos, barcos.
Alto	Situação financeira altamente melhorada, atinge valores de imóveis.
Muito Alto	Autor torna-se milionário.

Tabela 3.6: Cálculo do lucro financeiro de um incidente.

A segunda métrica a ser analisada no lado do atacante é a do investimento necessário para se obter êxito na exploração de uma vulnerabilidade. Novamente, a assinatura prevê uma análise desta métrica sob duas óticas: a do investimento financeiro e a do conhecimento técnico necessário, podendo ser adicionadas novas óticas de acordo com a necessidade da organização. Estas óticas estão descritas nas tabelas 3.7 e 3.8, respectivamente.

Investimento Financeiro	Descrição
Alto	Não compensará o lucro obtido, inviável.
Médio	Compensará o lucro obtido, porém não disponível a qualquer um.
Baixo	A maioria da população conseguirá bancar o investimento.
Nenhum	Nenhum investimento financeiro será necessário.

Tabela 3.7: Cálculo do investimento financeiro do atacante.

Conhecimento Técnico	Descrição
Avançado	Necessário um 'expert' no assunto com muito tempo de estudo (anos) para a execução do trabalho.
Intermediário	Necessário um conhecedor do assunto com tempo razoável de estudo (meses) para a execução do trabalho.
Básico	Qualquer um pode executar o trabalho bastando para isso pouco tempo de estudo (semanas).
Nenhum	Nenhum conhecimento técnico é necessário.

Tabela 3.8: Cálculo do investimento em conhecimento técnico do atacante.

Obtidos estes dados, a assinatura utiliza a metodologia exposta na tabela 3.9 para realizar o cálculo do custo/benefício do incidente para o atacante ou agente de ameaça.

X			Motivação				
		Notoriedade	Nenhuma	Baixa	Média	Alta	Ampla
		Lucro Financeiro	Nenhum	Pequeno	Médio	Alto	Muito Alto
Investimento	Alto	Avançado	1	2	3	4	5
	Médio	Intermediário	2	4	6	8	10
	Baixo	Básico	3	6	9	12	15
	Nenhum	Nenhum	4	8	12	16	20
	Financeiro	**Conhecimento técnico**					

Tabela 3.9: Cálculo do custo/benefício da exploração de uma vulnerabilidade.

A métrica de análise dos custos dos investimentos em contramedidas necessárias para mitigar um risco possui uma forma de cálculo na assinatura que difere das métricas anteriores. Na atribuição do valor do risco e do custo/benefício ao atacante as métricas e os valores são inclusos nos nós intermediários da árvore que compõe a assinatura, como será mostrado adiante. Já os custos dos investimentos em contramedidas são calculados nos nós folha da assinatura, pois estes estão diretamente ligados ao controles dispostos na família das normas ISO/IEC 27000. Estes custos devem ser mensurados e analisados comparando-os com o valor do Risco (Impacto X Probabilidade) e do Custo/Benefício, quando este existir, associados ao Cenário de Ameaça. As tabelas 3.10 e 3.11 mostram a forma como a assinatura calcula o custo da contramedida e o compara com o Risco e com o Custo/Benefício atribuído, respectivamente:

Custo da contramedida	Descrição
Nenhum	A implementação não gera nenhum custo.
Baixo	Não afeta a vida financeira da empresa.
Médio	Afeta pouco as finanças, necessário um programa de redução de custos.
Alto	Custo elevado para a empresa custear, necessário financiamento externo.
Muito Alto	Investimento muito alto, pode levar a empresa à falência se não funcionar.

Tabela 3.10: Cálculo do custo da contramedida.

X			Custo da Contramedida				
Faixas de Risco / Custo benefício	Nível	Faixa	Muito Alto	Alto	Médio	Baixo	Nenhum
	Baixo	1-2	1	2	3	4	5
	Médio	3-6	2	4	6	8	10
	Alto	7-12	3	6	9	12	15
	Crítico	13-20	4	8	12	16	20

Tabela 3.11: Análise de custo para implementação das contramedidas.

As faixas de Risco/Custo Benefício da tabela 3.11 foram construídas considerando os intervalos entre as diagonais da tabelas de Cálculo do Risco e de Custo Benefício, tabelas 3.4 e 3.9 respectivamente. Partindo do nível critico 20 localizado na última linha, na última coluna, a diagonal acima de 20 é 12, dessa forma, fica delimitado o primeiro intervalo 13 a 20 – Crítico, a diagonal subsequente ao 12 é 6, delimitando próximo intervalo 7-12 e assim sucessivamente.

Discretizar estas métricas de custos de forma a não causar dúvidas no momento da utilização destas tabelas foi um trabalho dispendioso. Uma das formas foi a associação dos valores a fatores externos, tais com marcas de tempo, valores de bens e reconhecimento da mídia a fim de tornar mais didática a utilização das mesmas.

Com esta análise a assinatura elenca as contramedidas a serem implementadas criando um ranking de facilidade/prioridade de implementação. Quanto maior for a classificação da contramedida, mais fácil sua implementação, ou seja, o seu custo torna-se facilmente justificável. Por exemplo: dado um risco calculado como critico, as contramedidas de custo menor possuem valores maiores, ou seja, são mais

facilmente implementáveis.

3.2.3. A estrutura da assinatura

A assinatura, como mencionado anteriormente, é estruturada em forma de árvore, semelhante a uma árvore de ataque e possui alguns níveis obrigatórios e outros não obrigatórios.

A figura 3.1 mostra a estrutura básica de uma assinatura que serviu como um dos estudos de caso desta dissertação. Trata-se de uma assinatura de riscos para um *Web Server* localizado no interior do Laboratório ACME! de Pesquisa em Segurança da UNESP de São José do Rio Preto – SP.

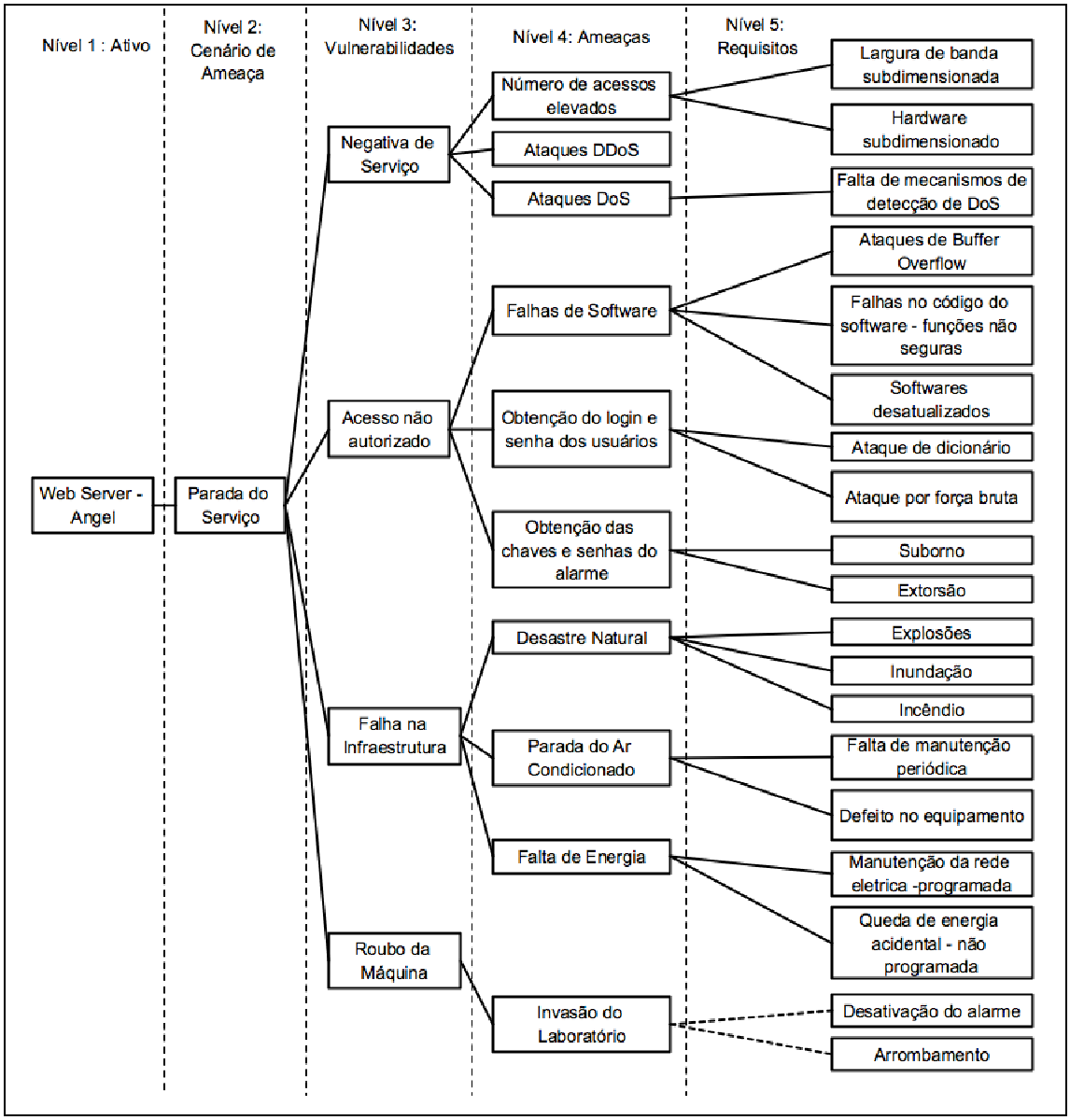

Figura 3.1: Assinatura para Web Server do Laboratório ACME! – UNESP .

Como mostra a figura 3.1, a assinatura está dividida em níveis. O primeiro nível é o dos Ativos, neste constam os ativos relacionados à segurança da informação que serão analisados, neste exemplo, o *Web Server*.

O nível 2 elenca os Cenários de Ameaça àquele ativo, ou seja, os riscos que estão associados ao ativo do primeiro nível. Neste exemplo, consta apenas o cenário/risco de parada do serviço, no entanto, a assinatura para o Web Server possui outros riscos que serão mostrados mais adiante.

No terceiro nível estão expostas as vulnerabilidades que podem levar a uma

ocorrência do cenário de ameaça do nível superior. O nível subsequente da árvore lista as ameaças que podem fazer com que estas vulnerabilidades sejam exploradas. O nó *Invasão do Laboratório*, do nível 4, possui nós filhos ligados por linhas intermitentes. Esta diferenciação é feita para identificar de forma fácil que se trata de um nó E e os outros, de nós OU.

Os nós da assinatura podem ser de dois tipos, assim como nas árvores de ataque: Nós *OU* e Nós *E*. Um nó *OU* é satisfeito quando um de seus filhos o é, enquanto um nó *E* somente é satisfeito quando todos os seus filhos são.

Na modelagem da assinatura, todos estes quatro primeiros níveis são obrigatórios. Já o quinto nível, Requisitos, não é um nível obrigatório para assinatura. Neste nível estão listados os requisitos necessários para que uma ameaça se concretize e torne-se uma ocorrência, ou seja, o *modus operandi* de um ataque ou os eventos necessários para um incidente de magnitude natural ou provocado sem intenção.

Além destes 5 níveis, existe ainda no modelo, um sexto e último nível, não apresentado na figura por uma questão de simplificação, onde estão listadas as contramedidas que devem ser adotadas. No capítulo 4, é mostrado um diagrama completo desta assinatura – figura 4.1.

Para se chegar a este modelo final proposto em 6 níveis, foi necessário efetuar vários testes com menos níveis e mais níveis. Com menos níveis, a assinatura não conseguia endereçar todas as métricas propostas, ou seja, não cumpriria o que foi proposto. Já com mais níveis, a assinatura endereçaria todas as métricas, porém dificultaria a sua construção, pois seria muito extensa e poderia induzir o responsável pela construção a redundâncias.

3.2.4. O módulo AISF

Como mostrado anteriormente, uma das principais características do modelo AISF é a modularidade. Devido a esta característica, as alterações no modelo são relativamente simples.

Usando a especificação deste modelo foi criado um novo módulo, o *Risk Signature Module*, que descreve os nós da assinatura com seus respectivos campos. Cada nó da assinatura é representado por um *Risk Signature Module*. Estes nós possuem diferentes informações de acordo com o seu nível na árvore. No entanto, para manter o modelo simples e sucinto, a estrutura XML desenvolvida para o nó é genérica, utilizada em todos os nós da assinatura independente, do nível em que este se localiza.

A figura 3.2 mostra uma descrição do módulo *Risk Signature Module* do AISF desenvolvido:

Campo	Descrição
ModuleLength	Identifica quantos campos tem o módulo, contando com o próprio campo. Este campo deve ser preenchido como um inteiro.
ID	Identificador do nó. Composto pelo Nível+Sequencial.
Father	ID do nó Pai, caso não haja nó pai (Raiz) o campo este campo é suprimido.
Type	Tipo de nó, "E" ou "OU".
Content	Conteúdo do nó, em literal.
Impact	Impacto que pode ser atribuído ou calculado automaticamente.
Probability	Probabilidade que pode ser atribuída ou calculada automaticamente.
Risk	Risco calculado, Probabilidade X Impacto.
Profit	Lucro para o atacante.
Investment	Investimento necessário para o atacante.
Benefit	Custo Benefício (Lucro X Investimento).
Countermeasure	Custo da contramedida.
NextID	Identifica qual será o módulo subsequente no AIS. Este campo deve conter o ID do próximo módulo.

Figura 3.2: Descrição do Risk Signature Module desenvolvido para o AISF .

Para que o módulo desenvolvido seja reconhecido pelo modelo AISF foram

necessárias algumas modificações no DTD (*Document Type Definition*) do modelo. Foi adicionado aos elementos AISF o *RiskSigModule* (abreviação para *Risk Signature Module*), que trata da descrição dos elementos que o compõem o módulo e o conteúdo destes elementos. Tais modificações são mostradas na figura 3.3.

```
<!ELEMENT AISF (SigIdModule,SigInfoModule?,SigCharModule?,DLinkProtoModuleEth?,
          NetProtoModuleIPv4?,TransConProtoModuleTCP?,TransConProtoModuleUDP?,
          TransConProtoModuleICMP?,PayloadInfoModule?,RiskSigModule?)>

<!ELEMENT SigIdModule (Version,ID,Name,SerialNumber,Credits,NextModule)>
<!ELEMENT SigInfoModule (ModuleLength,SecurityLevel,Category,Description,OtherIDs,
                         Impact,AttackScenario,TargetSystem,NextModule)>
<!ELEMENT SigCharModule (ModuleLength,EaseOfAttack,FalsePositive,
                          FalseNegative,RecommendedActions,NextModule)>
<!ELEMENT DLinkProtoModuleEth (ModuleLength,SourceAddress,
                               DestinationAddress,NextModule)>
<!ELEMENT NetProtoModuleIPv4 (ModuleLength,TypeOfService,TotalLength,FragmentId,
                               Flags,FragmentOffset,TTL,Protocol,SourceAddress,
                               DestinationAddress,Options,NextModule)>
<!ELEMENT TransConProtoModuleTCP (ModuleLength,SourcePort,DestinationPort,
                                  SequenceNumber,AcknowledgeNumber,DataOffset,
                                  Flags,Window,UrgentPointer,Options,NextModule)>
<!ELEMENT TransConProtoModuleUDP (ModuleLength,SourcePort,DestinationPort,NextModule)>
<!ELEMENT TransConProtoModuleICMP (ModuleLength,Type,Code,
                                   ID,SequenceNumber,NextModule)>
<!ELEMENT PayloadInfoModule (ModuleLength,Size,Offset,Depth,Contents,NextModule)>
<!ELEMENT RiskSigModule (ModuleLength,ID,Father,Type,Contents,Impact,Probability,
                         Risk,Profit,Investment,Benefit,Countermeasure,NextID)>

<!ELEMENT Version (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT Name (#PCDATA)>
<!ELEMENT SerialNumber (#PCDATA)>
<!ELEMENT Credits (#PCDATA)>
<!ELEMENT SecurityLevel (#PCDATA)>
<!ELEMENT Category (#PCDATA)>
<!ELEMENT Description (#PCDATA)>
<!ELEMENT OtherIDs (#PCDATA)>
<!ELEMENT Impact (#PCDATA)>
<!ELEMENT AttackScenario (#PCDATA)>
<!ELEMENT TargetSystem (#PCDATA)>
<!ELEMENT EaseOfAttack (#PCDATA)>
<!ELEMENT FalsePositive (#PCDATA)>
<!ELEMENT FalseNegative (#PCDATA)>
<!ELEMENT RecommendedActions (#PCDATA)>
<!ELEMENT SourceAddress (#PCDATA)>
<!ELEMENT DestinationAddress (#PCDATA)>
<!ELEMENT TypeOfService (#PCDATA)>
<!ELEMENT TotalLength (#PCDATA)>
<!ELEMENT FragmentId (#PCDATA)>
<!ELEMENT Flags (#PCDATA)>
<!ELEMENT FragmentOffset (#PCDATA)>
<!ELEMENT TTL (#PCDATA)>
<!ELEMENT Protocol (#PCDATA)>
<!ELEMENT Options (#PCDATA)>
<!ELEMENT SourcePort (#PCDATA)>
<!ELEMENT DestinationPort (#PCDATA)>
<!ELEMENT SequenceNumber (#PCDATA)>
<!ELEMENT AcknowledgeNumber  (#PCDATA)>
<!ELEMENT DataOffset (#PCDATA)>
<!ELEMENT Window (#PCDATA)>
<!ELEMENT UrgentPointer (#PCDATA)>
```

```
<!ELEMENT Type (#PCDATA)>
<!ELEMENT Code (#PCDATA)>
<!ELEMENT Size (#PCDATA)>
<!ELEMENT Offset (#PCDATA)>
<!ELEMENT Depth (#PCDATA)>
<!ELEMENT Contents  (#PCDATA)>
<!ELEMENT NextModule (#PCDATA)>
<!ELEMENT ModuleLength (#PCDATA)>
<!ELEMENT Father (#PCDATA)>
<!ELEMENT Impact (#PCDATA)>
<!ELEMENT Probability (#PCDATA)>
<!ELEMENT Risk (#PCDATA)>
<!ELEMENT Profit (#PCDATA)>
<!ELEMENT Investment (#PCDATA)>
<!ELEMENT Benefit (#PCDATA)>
<!ELEMENT Countermeasure (#PCDATA)>
<!ELEMENT NextID (#PCDATA)>
```

Figura 3.3: DTD do AISF modificado para reconhecer o Risk Signature Module.

Na definição do modelo AISF desenvolvido por Silva [SIL, 2002] existem dois campos obrigatórios nos módulos: o campo *Module Lenght* e o campo *Next Module*. Estes descrevem o tamanho do módulo em número de campos e qual o próximo módulo, respectivamente. Nas assinaturas de ataque suportadas pelo modelo, o campo *Next Module* indica sempre um nó seguinte, este é único e sem repetições em toda a estrutura da assinatura. Este campo perde sua função nas assinaturas de risco, pois o *Risk Signature Module* se repete para todos os nós da árvore, deixando de ser único, o que poderia gerar problemas na estruturação da árvore no modelo AISF. Para contornar este problema, o campo *Next Module* foi substituído pelo campo *Next ID*, que contém o identificador do próximo nó/módulo da árvore. Esta modificação foi realizada, sem prejuízos ao modelo, devido a forma com que a assinatura foi projetada, um módulo *Risk Signature Module* será sempre sucedido por outro módulo *Risk Signature Module*.

Esta modificação não gera problemas com as assinaturas de ataque criadas utilizando as versões anteriores do AISF, pois foi mantida toda a estrutura de suporte, mostrada no Anexo A, do modelo original, mantendo a compatibilidade de versões.

Esse capítulo apresentou a descrição da modelagem da estrutura da assinatura desenvolvida, o módulo do AISF desenvolvido e o DTD do AISF modificado. O capítulo seguinte apresenta os resultados obtidos na aplicação da assinatura desenvolvida.

4. Resultados e Análises

Neste capítulo são apresentados os resultados e as análises obtidas neste projeto. Para ilustrar e comprovar o funcionamento do modelo proposto, é exibida uma assinatura de risco desenvolvida para um *web server*.

4.1. Assinatura de risco para *Web Server*

Esta assinatura foi desenvolvida, como já mencionado anteriormente, tomando-se como base um *web server* localizado no interior do Laboratório *ACME!* de Pesquisa em Segurança da UNESP de São José do Rio Preto – SP. A figura 4.1 mostra a estrutura desta assinatura.

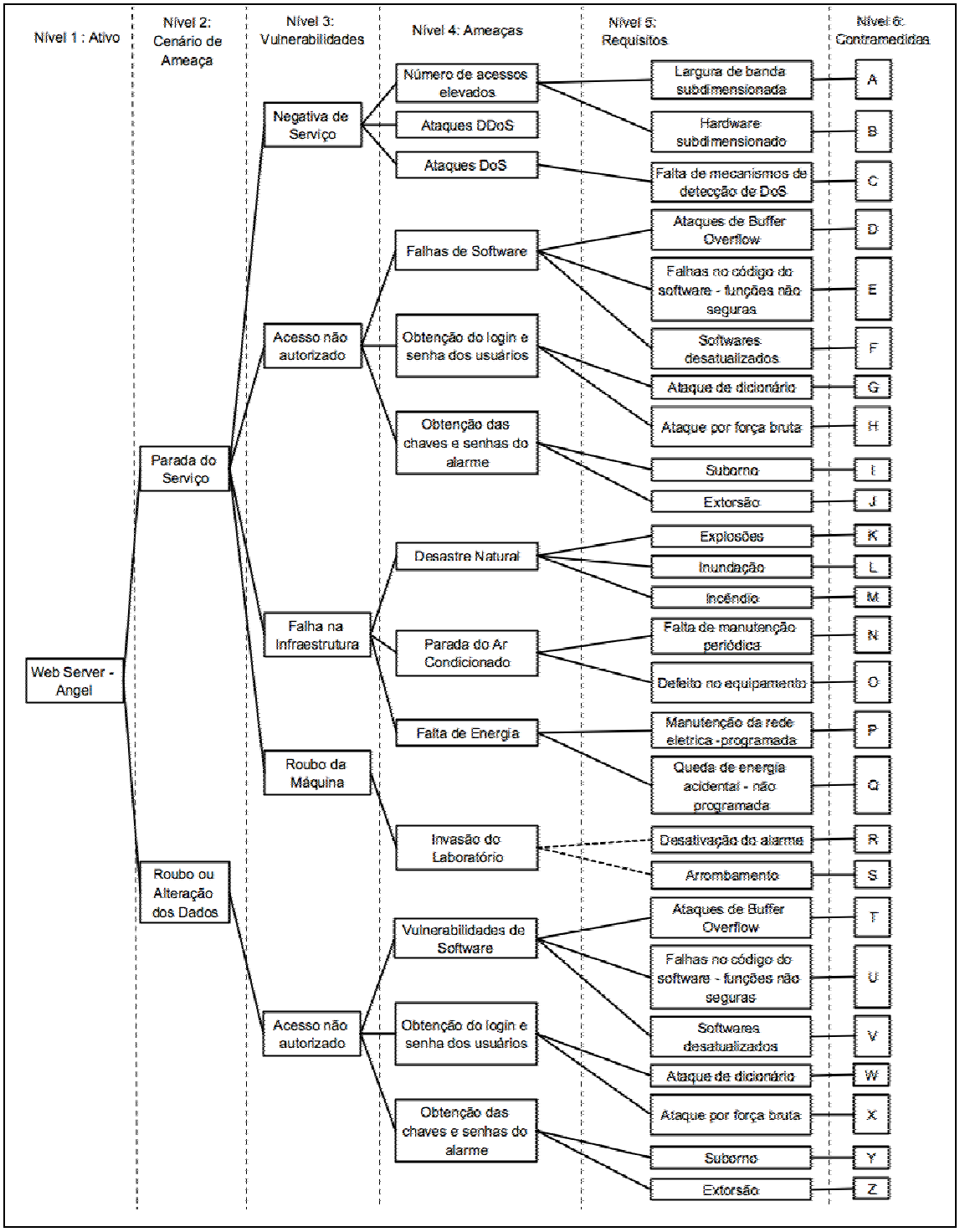

Figura 4.1: Assinatura de Risco para *Web Server*.

No diagrama, as contramedidas são representadas por letras do alfabeto por uma questão de simplificação do diagrama. No entanto, as letras devem ser consideradas como nós da árvore e, neste caso, como nós folhas. A tabela 4.1, a seguir, mostra as contramedidas aplicadas na assinatura representada pela figura 4.1.

Nó	Contramedidas
A e B	A.10.3.*
C	A.10.6.*
	A.10.10.*
D, E e F	A.5.*
	A.10.3.*
	A.10.4.*
	A.10.10.*
	A.12.5.*
	A.12.6.*
G e H	A.5.*
	A.10.10.*
	A.11.*
I e J	A.5.*
	A.7.1.*
	A.8.*
	A.9.*
	A.11.1
K a Q	A.9.*
R, S	A.9.*
	A.11.1
	A.11.2
	A.11.3
	A.14.*
T, U e V	A.5.*
	A.7.1.*
	A.10.*
	A.11.*
	A.12.*
W e X	A.10.4.*
	A.10.6.*
	A.10.10.*
	A.11.*
	A.12.3.*
	A.12.6.*
Y e Z	A.5.*
	A.6.*
	A.8.*

Tabela 4.1: Análise de custo para implementação das contramedidas.

A tabela a seguir elenca todos os controles da norma ISO/IEC 27001 utilizados na assinatura, mostrados na tabela 4.1, bem como seus respectivos objetivos.

Controles		Objetivos
A.5.*	Política de segurança	Orientar e apoiar a direção para a segurança da informação de acordo como os requisitos do negócio e com as leis e regulamentações relevantes.
A.6.*	Organizando a segurança da informação	Organizar a infraestrutura de segurança da informação, gerenciando inclusive a segurança relacionada a partes externas à organização.
A.7.1.*	Responsabilidade pelos ativos	Alcançar e manter a proteção adequada aos ativos da organização.
A.8.*	Segurança em recursos humanos	Dispõe sobre procedimentos de segurança em RH, atuando antes, durante e depois das contratações.
A.9.*	Segurança física e do ambiente	Relaciona procedimentos de segurança física de áreas e de equipamentos.
A.10.*	Gerenciamento das operações e comunicações	Garantir a segurança de serviços e comunicações da organização.
A.10.3.*	Planejamento e aceitação dos sistemas	Minimizar o risco de falhas no sistema.
A.10.4.*	Proteção contra códigos maliciosos e códigos móveis	Proteger a integridade do software e da informação.
A.10.6.*	Gerenciamento da segurança em redes	Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.
A.10.10.*	Monitoramento	Detectar atividades não autorizadas de processamento da informação.
A.11.*	Controle de acesso	Controlar o acesso tanto quanto físico quanto lógico à organização.
A.11.1	Requisitos de negócio para controle de acesso	Controlar o acesso à informação.
A.11.2	Gerenciamento de acesso do usuário	Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.
A.11.3	Responsabilidade dos usuários	Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação
A.12.*	Aquisição, desenvolvimento e manutenção de sistemas	Garantir a segurança da informação em aquisições, no desenvolvimento e na manutenção de sistemas ligados à informação.
A.12.3.*	Controles criptográficos	Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.
A.12.5.*	Segurança em processos de desenvolvimento e suporte	Manter a segurança de sistemas aplicativos e da informação.
A.12.6.*	Gestão de vulnerabilidades técnicas	Reduzir os riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
A.14.*	Gestão da continuidade do negócio	Criar controles para gerir e manter a continuidade do negócio mesmo em momentos de crises.

Tabela 4.2: Controle e objetivos utilizados na assinatura de risco para Web Server.

Dada a estrutura da assinatura com suas contramedidas, e relacionamentos entre os nós, o modelo agora trata a questão das métricas aplicadas à análise de risco.

Como já citado anteriormente no capítulo 3 (3.2.4), a estrutura do nó desenvolvida para a assinatura de risco, segundo o modelo AISF, contempla vários campos. Alguns destes campos estarão preenchidos, dependendo do nível em que o nó está localizado na assinatura, enquanto outros estarão em branco.

Partindo dos nós folha para o nó raiz, temos a seguinte disposição dos campos preenchidos nos seguintes níveis:

Nível 6: Contramedidas – o campo *Countermeasures* é preenchido neste nível, onde nele constará o custo total de implementação das contramedidas, de acordo com a discretização constante na tabela 3.10.

Nível 5: Requisitos – o campo *Investment* é preenchido neste nível, onde nele deve constar o investimento necessário por parte do atacante para conseguir aquele requisito, de acordo com as tabela 3.7 ou 3.8, conforme a ótica empregada na análise.

Nível 4: Ameaças – o campo *Probability* é preenchido neste nível, são descritos as probabilidades de uma ameaça ser confirmada, conforme descrito na tabela 3.2

Nível 3: Vulnerabilidades – neste nível são colocadas as métricas referentes ao impacto que a exploração de uma vulnerabilidade pode causar à organização detentora do sistema, e qual o lucro obtido pelo atacante com a exploração desta vulnerabilidade, de acordo com as tabelas 3.3 e 3.5 ou 3.6, e conforme a ótica empregada na análise. Os campos *Impact* e *Profit* são preenchidos neste nível. Em seguida, os campos *Risk* e *Benefit* são calculados e preenchidos. A forma como deverão ser calculados estes valores é mostrada logo adiante.

Nível 2: Cenário de Ameaça – Neste ponto, os campos *Risk* e *Benefit* são preenchidos de acordo com o tipo de nó, conforme mostrado adiante.

Nível 1: Ativo – Raiz da árvore onde, por fim, chega-se a um parecer sobre os riscos inerentes ao ativo. Ou seja, obtém-se o valor dos riscos (Impacto X Probabilidade), dos Custos/Benefícios ao atacante (Investimento X Lucro) e a dualidade custos (Risco a ser mitigado X Investimento em contramedidas).

O cálculo dos valores dos riscos (campo *Risk*) e custos/benefícios (campo *Benefit*) envolve uma lógica de propagação dos valores das métricas que depende do tipo de relacionamento do nó pai com os nós filhos. A propagação ocorre sempre no sentido contrário da árvore, ou seja, dos nós filhos para os nós pais. Se um nó pai é do tipo *OU*, a situação que ele representa acontecerá somente se um ou mais dos seus nós filhos aconteça. Neste caso, na propagação das métricas para a realização dos cálculos supracitados, um nó pai receberá como valores para suas métricas os mesmos valores contidos no nó filho que representar o pior caso dentre os seus filhos, como mostrado na sub-árvore derivada da assinatura da figura 4.2:

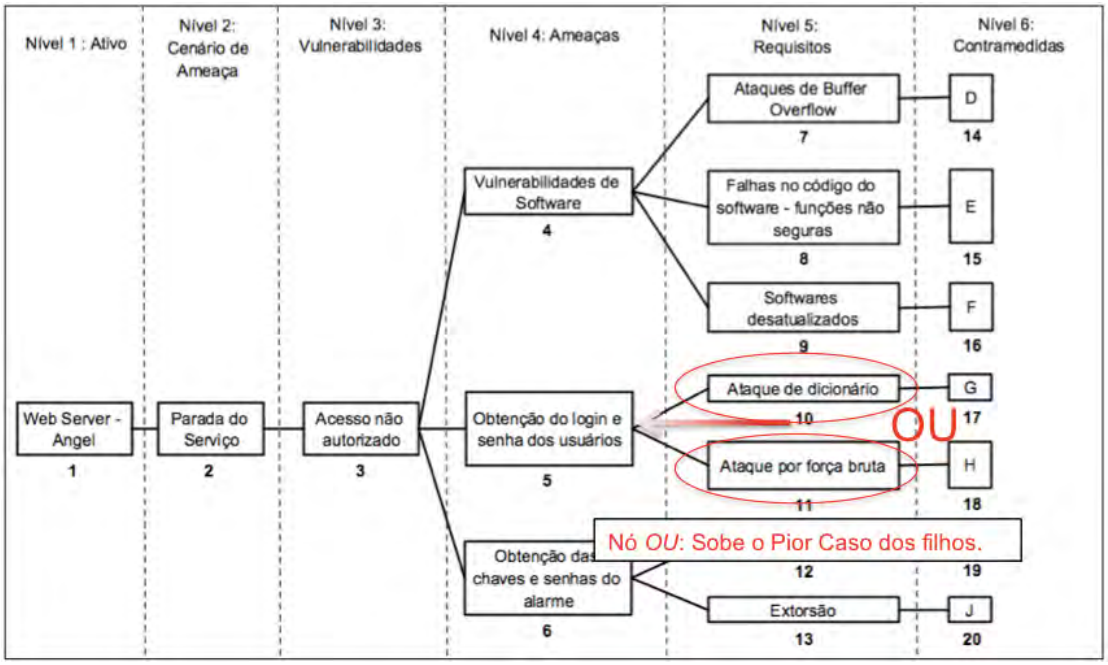

Figura 4.2: Exemplo de propagação dos dados na assinatura.

Para uma melhor visualização dos componentes da assinatura, os campos que contém as informações dos nós foram suprimidos na figura e estes foram numerados de forma sequencial, crescente por nível da árvore. Estes números serão incluídos no campo ID (nível + sequencial) de cada módulo *Risk Signature Module* do AISF. As tabelas a seguir mostram como cada nó deste exemplo é preenchido.

Nivel1	
ModuleLength	13
ID	11
Father	-
Type	OU
Content	Web Server - Angel
Impact	Alto
Probability	Baixa
Risk	6
Profit	Médio
Investment	Basico
Benefit	9
Countermeasure	Baixo
NextID	22

Nivel 2	
ModuleLength	13
ID	22
Father	11
Type	OU
Content	Parada do Serviço
Impact	Alto
Probability	Baixa
Risk	6
Profit	Médio
Investment	Básico
Benefit	9
Countermeasure	Baixo
NextID	33

Nivel 3	
ModuleLength	13
ID	33
Father	22
Type	OU
Content	Acesso não autorizado
Impact	Alto
Probability	Baixa
Risk	6
Profit	Médio
Investment	Basico
Benefit	9
Countermeasure	Baixo
NextID	44

Nivel 4	
ModuleLength	9
ID	44
Father	33
Type	OU
Content	Vulnerabilidades de Software
Probability	Baixa
Investment	Basico
Countermeasure	Baixo
NextID	45

ModuleLength	9
ID	45
Father	33
Type	OU
Content	Obtenção de Login e Senha de usuário.
Probability	Muito Baixa
Investment	Basico
Countermeasure	Nenhum
NextID	46

ModuleLength	9
ID	45
Father	33
Type	OU
Content	Obtenção de Chaves e Senhas de Alarme.
Probability	Muito Baixa
Investment	Basico
Countermeasure	Nenhum
NextID	57

Nivel5	
ModuleLength	8
ID	57
Father	44
Type	OU
Content	Ataques de Buffer Overflow
Investment	Intermediario
Countermeasure	Baixo
NextID	58

ModuleLength	8
ID	58
Father	44
Type	OU
Content	Falha no código do Software - funções não seguras
Investment	Avançado
Countermeasure	Baixo
NextID	59

ModuleLength	8
ID	59
Father	44
Type	OU
Content	Software Desatualizado
Investment	Basico
Countermeasure	Baixo
NextID	510

ModuleLength	8
ID	510
Father	45
Type	OU
Content	Ataque de Dicionário
Investment	Avançado
Countermeasure	Nenhum
NextID	511

ModuleLength	8
ID	511
Father	45
Type	OU
Content	Ataque por força bruta
Investment	Basico
Countermeasure	Nenhum
NextID	512

ModuleLength	8
ID	512
Father	46
Type	OU
Content	Suborno
Investment	Basico
Countermeasure	Nenhum
NextID	513

ModuleLength	8
ID	513
Father	46
Type	OU
Content	Extorsão
Investment	Basico
Countermeasure	Nenhum
NextID	614

Nivel 6					
ModuleLength	6	ModuleLength	6	ModuleLength	6
ID	614	ID	615	ID	616
Father	57	Father	58	Father	59
Content	A.5.*; A.10.3.*; A.10.4.*; A.10.10.*; A.12.5.*; A.12.6.*	Content	A.5.*; A.10.3.*; A.10.4.*; A.10.10.*; A.12.5.*; A.12.6.*	Content	A.5.*; A.10.3.*; A.10.4.*; A.10.10.*; A.12.5.*; A.12.6.*
Countermeasure	Baixo	Countermeasure	Baixo	Countermeasure	Baixo
NextID	615	NextID	615	NextID	617

ModuleLength	6	ModuleLength	6	ModuleLength	6
ID	617	ID	618	ID	619
Father	510	Father	511	Father	512
Content	A.5.*; A.10.10.*; A.11.*	Content	A.5.*; A.10.10.*; A.11.*	Content	A.5.*; A.7.1.*; A.8.*; A.9.*; A.11.1
Countermeasure	nenhum	Countermeasure	nenhum	Countermeasure	nenhum
NextID	618	NextID	619	NextID	620

ModuleLength	6
ID	620
Father	513
Content	A.5.*; A.7.1.*; A.8.*; A.9.*; A.11.1
Countermeasure	nenhum
NextID	-

Tabela 4.3: Nós AISF da Assinatura.

No exemplo apresentado de uma sub-árvore com todos os nós do tipo *OU*, a propagação do pior caso chega ao nó raiz, partindo dos nós folha, ou seja, o maior risco dentre os filhos representa o nível de risco do ativo (raiz). A figura 4.3 mostra este caso, os índices em destaque representam este caminho dentre os nós filhos da assinatura, ou seja, o maior risco deste exemplo.

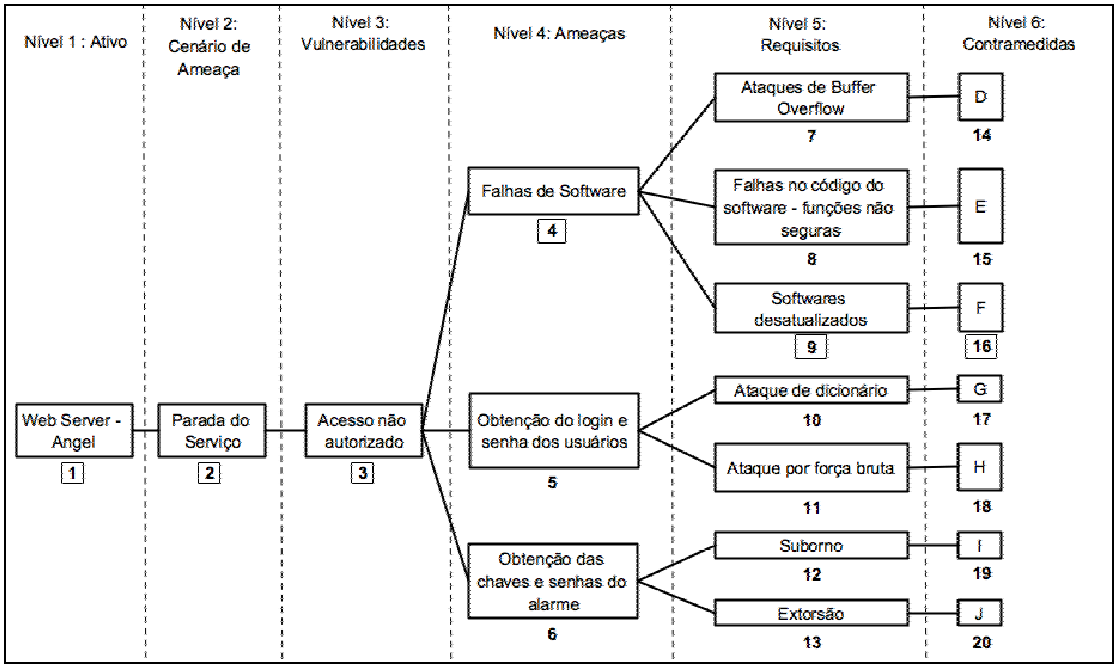

Figura 4.3: Exemplo de propagação do pior caso na assinatura.

No caso do nó pai ser do tipo *E*, a situação que ele representa acontecerá se e somente se, todos os filhos aconteçam. Neste caso, nos cálculos das métricas efetuados pelo nó pai será atribuído a este, na propagação dos valores das métricas, o melhor caso dentre os filhos, como mostrado na sub-árvore derivada da assinatura da figura 4.1 e mostrada na figura 4.4 a seguir.

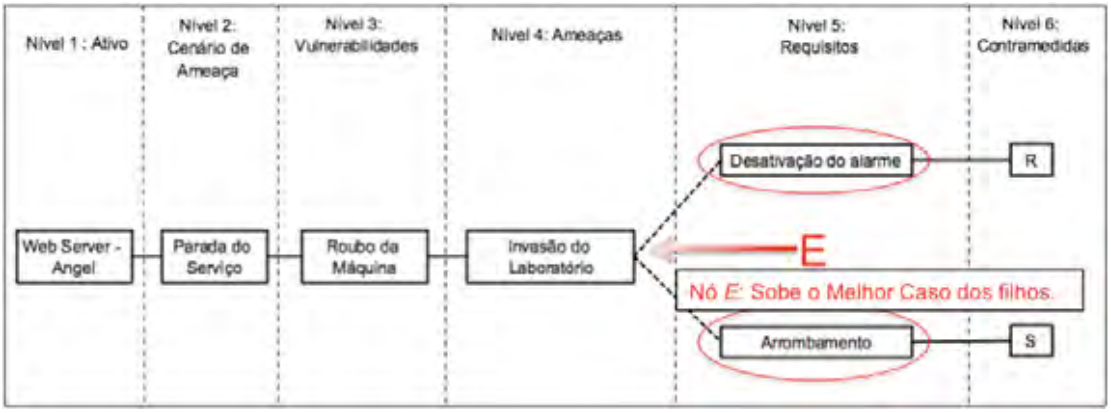

Figura 4.4: Exemplo de propagação do melhor caso na assinatura.

Para que haja uma invasão do laboratório, nível 4, é necessário a desativação do sistema de alarme e o arrombamento da porta. Neste caso o atendimento de apenas um dos requisitos do nível 5 da assinatura não garante o sucesso do ataque. Dessa forma, deverá ser propagado para o nó pai o melhor caso dentre os dois nós filhos. Isso porque, somente a ocorrência do pior caso – o pior caso é o que possui o maior

risco, ou seja, maior impacto e/ou probabilidade de ocorrer – não garante o sucesso da ameaça na exploração da vulnerabilidade. Para que a vulnerabilidade seja explorada, também é necessária que a ocorrência do melhor caso se concretize, o que é menos provável de ocorrer.

Assim, a assinatura se torna dinâmica com esta propagação das métricas. Isto ocorre posto que com a implementação de uma contramedida a probabilidade de uma ocorrência originária de uma ameaça se concretizar é reduzida. Desta forma ocorre um efeito de ajuste e realimentação em todos os nós superiores, fechando um ciclo de realimentação.

A implementação das contramedidas deverá seguir uma ordem de prioridades. Esta ordem poderá ser baseada em dois fatores, o risco atribuído a um ativo ou o custo/benefício do ataque a um atacante. Qualquer um dos valores escolhido deverá ser confrontado com o custo de implementação da contramedida, de acordo com a tabela 3.11. Dessa forma, o maior valor resultante do confronto entre as métricas tem maior prioridade na fila implementação.

4.2. Resultado

Na análise de risco realizada no *Web Server Angel* do Laboratório ACME!, da UNESP de São José do Rio Preto, a assinatura foi capaz de elencar todos os riscos inerentes ao ativo de forma ampla e direta, indicando as contramedidas a serem implementas a fim de que o risco inerente ao ativo fosse reduzido a um nível aceitável.

Segundo a análise feita, a assinatura da figura 4.1 mostra que o maior risco atualmente associado ao *Web Server* em estudo refere-se a uma possível parada do serviço devido a uma falha de infraestrutura, ou seja, não se trata de um ataque mas sim de um fator externo, não intencional. Mais precisamente, a assinatura mostra que os eventos de maiores probabilidades de ocorrência são: uma parada do sistema de ar

condicionado e uma falta de energia repentina, não coberta por um sistema de *no-breaks* ou gerador conforme mostrado na figura 4.5.

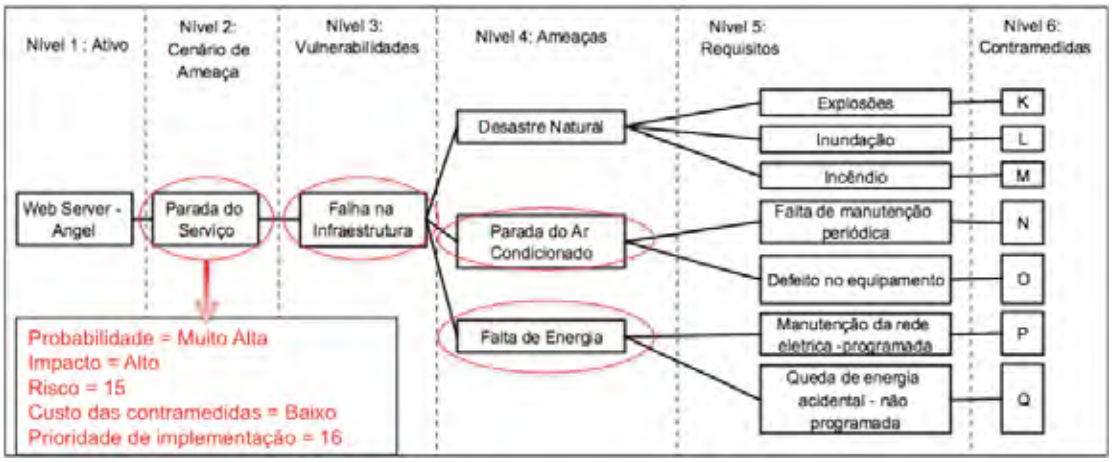

Figura 4.5: Pior caso identificado na assinatura em estudo.

Como contramedidas necessárias para a mitigação deste risco, indicadas na tabela 4.1, a assinatura apresenta o grupo de controles A.9 a serem implementados, da seguinte forma:

A.9.1 – Áreas Seguras: tem como objetivo prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

A.9.2 – Segurança de equipamentos: Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

Considerando-se a atual instalação e a infraestrutura do *Web Server* já existente, a assinatura considera que o custo para implementação de tais controles é determinado como “BAIXO”. O impacto de uma Parada do Serviço é determinado como “ALTO” causando a parada de diversos serviços e a probabilidade de que uma Parada do Serviço ocorra é “Muito Alta”, o que resultaria de acordo a tabela 3.4 em um risco de valor 15. Considerando o valor do risco e custo de implementação das contramedidas, a tabela 3.9 mostra que a prioridade de implementação destas é 16, o que representa uma prioridade ”CRÍTICA”, tendo em vista que a prioridade máxima na fila de implementação é 20.

Esse capítulo apresentou detalhes sobre a assinatura desenvolvida, seu funcionamento e sua implementação, bem como os resultados obtidos na sua

aplicação em um Web Server. O capítulo seguinte apresenta as conclusões do presente trabalho.

5. Conclusões e Trabalhos futuros

A assinatura mostrou-se um modelo bastante versátil e altamente adaptável a diversas situações de análise de diferentes riscos inerentes aos ativos da organização.

A proposta principal deste trabalho baseava-se na criação de um modelo que gerasse uma padronização da análise de risco voltada a segurança da informação. Esta padronização é necessária para simplificar o processo de análise de riscos. Desta forma, a assinatura criada, compatível com o modelo AISF garante esta padronização passível de ser adotada em escala, ainda inexistente até o momento segundo conhecimento do autor.

Este padrão foi concebido para servir de base para uma ferramenta de análise de risco voltada para segurança da informação. Um trabalho futuro poderá estar relacionado com a implementação de um banco de dados com estas assinaturas, para diversos ativos relacionados à segurança da informação, a idéia principal é possuir um *pool* de assinaturas de risco disponíveis. Dessa forma, dado um ativo, bastaria efetuar uma busca neste banco de dados procurando por assinaturas de risco relacionadas àquele ativo. O sistema então forneceria esta assinatura contendo todos os riscos endereçados ao ativo com as métricas em branco, bastando que o responsável pela análise avalie o cenário atual da organização e preencha as métricas. Ao final a assinatura mostraria quais são os maiores riscos ao sistema e as principais contramedidas necessárias para a mitigação dos riscos inerentes ao ativo.

Ainda como conclusão desta pesquisa, é importante mencionar que as assinaturas desenvolvidas e que foram propostas e incorporadas ao modelo não possuem quaisquer limitações quanto a número de nós que estão ligados a um ativo. Dessa forma, o modelo torna-se flexível e adaptável para diversas situações, aferindo-lhe a possibilidade de aplicação em outras áreas que não somente a tecnologia da informação. Neste aspecto, deve-se mencionar que estudos preliminares encontram-se em andamento no grupo de pesquisa, visando a utilização do modelo proposto neste trabalho para a aplicação de análise de risco de veículos aéreos autônomos. As análises iniciais têm se mostrado bastante promissoras.

Devido à esta flexibilidade mencionada, o padrão desenvolvido permite a criação de assinaturas genéricas que servirão como base para todo ativo daquele tipo, por exemplo, uma assinatura de risco para um banco de dados, a qual poderá ser utilizada para qualquer tipo de banco de dados, além da criação de assinaturas personalizadas para um determinado ativo, por exemplo, uma assinatura gerada para um *Web Server* localizado em um laboratório como mostrado no capítulo 4.

Uma das dificuldades encontradas no desenvolvimento do projeto foi a definição das métricas. Discretizá-las, definir em que nível da assinatura cada uma delas deveria ser inserida e como deveriam ser calculadas para se chegar a alguma conclusão foi uma das tarefas mais complexas na definição do modelo. Foram necessários vários testes até chegarmos à configuração atual da assinatura, dividida em seis níveis.

A dependência entre os riscos e contramedidas também é contemplada pelo modelo. A exemplo disso, quando há a implementação de um controle da norma ISO/IEC 27001 contido em um nó do nível 6 da assinatura vinculado a uma ameaça, esta contramedida pode influenciar de maneira positiva outras ameaças. Logo, as métricas da assinatura são recalculadas, causando uma redução geral do nível de risco do ativo.

Finalmente, o modelo atende aos propósitos ao qual foi projetado e concebido, criando algo inédito e de grande contribuição para a área de análise de risco voltada para segurança da informação: uma padronização para a assinatura de risco. Esta padronização facilitará o processo de análise de risco, pois como sua principal característica temos a flexibilidade e adaptabilidade frente aos diversos ativos e cenários possíveis, podendo atender diversos segmentos e tipos de organizações ou instituições.

Referências Bibliográficas

[ABD, 2002] Aagedal, J.; Braber, F.; Dimitrakos, T.; Gran, B.; Raptis, D.; Stolen, K.; **Model-based Risk Assessment to Improve Enterprise Security.** In Proceedings of the Sixth International ENTERPRISE DISTRIBUTED OBJECT COMPUTING Conference, 2002.

[AND, 2001] Anderson, R.; **Security engineering: A guide to building dependable distributed systems.** Cap. 2, 6, 7, 10, 11, 18, 21-23. New York, John Weley and sons, 2001.

[ASN, 1999] Standards Australia, **AS/NZS 4360: Risk Management**, Standards Australia, Standard, AS/NZS 4360, 1999.

[AVI, 2004] Avizienis, A.; **Basic concepts and taxonomy of dependable and secure computing.** In IEEE Transactions on Dependable and Secure Computing, Vol 1, pag. 11-33, 2004.

[CBR, 2008] Cert.br, **Incidentes Reportados ao CERT.br -- Abril a Junho de 2008.** Disponível em: <http://www.cert.br/stats/incidentes/2008-apr-jun/total.html>. Acessado em: 12 ago. 2008.

[CER, 2008] CERT/CC **– Computer Emergency Response Team - Coordination Center**, 2005. Apresenta dados sobre incidentes de segurança em redes de computadores. Disponível em: <http://www.cert.org/stats/cert_stats.html>. Acessado em: 12 ago. 2008.

[CCT, 2008] CERT/CC **– Cartilha de Segurança para Internet,** 2008. Glossário. Disponível em: <http://cartilha.cert.br/glossario/>. Acessado em: 02/01/2008.

[COH, 1998] Cohen F.; **A cause and effect model of attacks on information systems**, Computers & Security, Vol. 17(3), pp.211-221, 1998

[COR, 2000] CORAS, **CORAS: A platform for risk analysis of security critical systems**, 2000.

[GON, 2001] Gong, F.; **Characterizing intrusion tolerant systems: Using a state transition model.** In Proceedings of DARPA Information Survivability Conference and Exposition, 2001.

[I2K, 2008] **ISO27k Infosec Management Standards** – Disponível em: <http://www.iso27001security.com/>. Acessado em 29 de setembro de 2008.

[ISO, 1996] ISO/IEC, **Information technology – Guidelines for the management or IT security**. ISO/IEC 13335: 1996

[ISO, 2005] ISO/IEC JTC 1/SC 27, **Information technology - Security techniques**. ISO/IEC FDIS 17799: 2005.

[ISO2, 2005] ISO/IEC, **Information technology – Security techniques – Evaluation criteria for IT security.** ISO/IEC 15408: 2005.

[ISO, 2006] ABNT NBR ISO/IEC, **Técnologia da informação – Técnicas de Segurança – Sistema de gestão de segurança da informação – Requisitos** – ISO/IEC 27001:2006.

[ISO, 2007] ABNT NBR ISO/IEC, **Técnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação** – ISO/IEC 27002 - 17799:2005/Err.2:2007.

[LIT, 1993] Littlewood, B.; **Towards operational measures of computer security.** Journal of Computer Security, Vol.2, pag 211-229, 1993.

[LUR, 2004] LURHQ Threat Intelligence Group. **Dabber Worm Analysis**. Maio, 2004. Disponível em: <http://www.lurhq.com/dabber.html>. Acessado em: 19 set 2005. [WSP, 2004]B. Claise, Ed., **Cisco Systems NetFlow Services Export Version 9**. RFC 3954, out. 2004. Disponível em: <http://www.ietf.org/rfc/rfc3954.txt>. Acessado em: 20 set. 2005.

[MAR, 2006] Marron, J.; **Applications for cyber security – system and application monitoring.** In Proceedings of NPIC&HMIT, pag. 536-541, 2006.

[MEL, 2008] Melo, L. P.; **Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de TI.** Dissertação de Mestrado, Publicação PP-GENE.DM - 330/08 14 de Março de 2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília-DF, 181 p.

[MVF, 2001] Moore, D.; Voelker, G.M.; Savage, F. **Inferring Internet Denial-of-service activity.** In Proceedings of the 10th Usenix Security Symposium. Washington,D.C., Agosto, 2001. Disponível on-line: <http://www.usenix.org/publications/library/proceedings/sec01/moore.html>. Acessado em: 19 set 2005.

[MyS, 2008] **MySQL Home Page** – Disponível em: <http://dev.mysql.com/>. Acessado em 29 de setembro de 2008.

[NIC, 2004] Nicol, D.; **Model-based evaluation: from dependability to security.** In IEEE Transactions on Dependable and Secure Computing, Vol 1, pag. 48-65, 2004.

[PHP, 2002] **PHP Home Page** – Disponível em: <http://www.php.net>. Acessado em 29 de setembro de 2008.

[ROS, 2005] Ross, R.; **Recommended security controls for federal information system.** NIST Special Publication 800-53, 2005

[SIL, 2002] SILVA, A. R. A. da; SOUZA, M. de; CANSIAN, A. M. **AISF - A Proposal for Standard Intrusion Signature Representation**. [S.l.]: WSEAS Transactions On Systems, Abril 2003.

[SCH, 2001] Schneier, Bruce; **Segurança.com: Segredos e mentiras sobre a proteção na vida digital.** Tradução de Daniel Vieira – Rio de Janeiro: Campus, 2001.

[TCP, 2008] **Tcpdump** - Disponível em: <http://www.tcpdump.org>. Acessado em 30 de setembro de 2008.

[WEB, 2005] Webster, K.; Oliveira, K.; Anquetil, N; **A Risk Taxonomy Proposal for Software Maintenance.** In the Proceedings of the 21st IEEE International Conference on Software Maintenance (ICSM'05), 2005.

[W3C, 2002] **World Wide Web Consortium "XML (Extensible Markup Language) 1.0"-** Disponível em: http://www.w3.org/TR/2000/REC-xml-20001006, Acessado em 29 de setembro de 2008.

Bibliografia

[AL, 2003] Arce, I.; Levy, E. **An Analysis of the Slapper Worm.** In IEEE Security and Privacy. Vol. 1. N. 1. Janeiro, 2003.

[And, 1980] Anderson, J.P. **Computer Security Threat Monitoring and Surveillance.** James P. Anderson Co, Fort Washington, PA (1980). Disponível em: http://csrc.nist.gov/publications/history/ande80.pdf>. Acessado em: 02 abr. 2008.

[ATS, 2003] Abad, C.; Taylor, J.; Sengul, C.; Yurcik, W. **Log Correlation of Intrusion Detection: A proof of concept.** 19th Annual Computer Security Applications Conference (ACSAC), 2003.

[CER, 2001] CERT Coordination Center. **CERT/CC Denial of Service Attacks**. Disponível em: <http://www.cert.org/tech_tips/denial_of_service.html>. Acessado em: 02 abr. 2008.

[CSI, 2003] Computer Security Institute and Federal Bureau of Investigation. **CSI/FBI Computer Security Survey 2003**. Computer Security Institute Publication, 2003. Anual.

[FOR, 1998] Forouzan, B. A. **Introduction to data communication and networking.** McGraw-Hill: Singapore, 1998.

[HHD, 2002] Householder, A.; Houle, K.; Dougberty, C. **Computer Attack Trends Challenge Internet Security.** In Security & Privacy Magazine Suplement to IEEE Computer Magazine. 2002.

[KAE, 1999] Kaeo, M. **Designing Network Security**. Cisco Press: Indianapolis, 1999.

[KR, 2001] Kurose, J.F.; Ross, K.W. **Computer Networking: A top-down Approach featuring the Internet.** Addison-Wesley: São Paulo, 2003.

[KR, 2003] Kurose, J.F.; Ross, K.W. **Redes de computadores e a Internet: Uma nova abordagem.** Addison-Wesley: [s.n.], 2001.

[SAN, 2004] SANS Institute. **Internet Storm Center:** Cooperative Cyber Threat Monitor and Alert System, 2004. Disponível em: <http://isc.sans.org/trends.php>. Acessado em: 02 abr. 2008.

[SIQ, 2004] Siqueira, T. A. **ACME! Honeynet de Segunda Geração: Implementação de Novas Tecnologia**. 2004. Monografia (graduação em Ciência da Computação) – Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista (UNESP), São José do Rio Preto.

[STE, 1994] Stevens, W.R. **TCP/IP Illustrated, Volume 1: The Protocols**. Upper Saddle River: Addison-Wesley, 1994.

[TAN, 1997] Tanenbaum, A.S. **Redes de Computadores.** Tradução da 3a. Edição. Rio de Janeiro: Campus, 1997.

[THP, 2002] The Honeynet Project. **Conheça seu inimigo: O Projeto Honeynet.** São Paulo: Pearson Education, 2002.

[ZCC, 2000] Zwicky, E.; Cooper, S.; Chapman, D.B. **Building Internet Firewalls.** 2a. ed. Sebastopol: O'Reilly, 2000.

Anexo A - Estrutura do modelo AISF.

O modelo AISF é composto por módulos que servem para descrever o comportamento de um ataque. Cada módulo é composto por uma série de campos. Dentre estes existem dois campos que são encontrados em todos os módulos, são eles o *Module Length* e o *Next Module*:

- ***ModuleLength:*** Identifica quantos campos tem o módulo, contando com o próprio campo. Este campo deve ser preenchido como um inteiro, obviamente maior que 2.
- ***NextModule:*** Identifica qual será o módulo subseqüente no AIS. Este campo deve conter uma *string* que identifica o módulo (Exemplo: SigInfModule). No caso do último módulo da assinatura, este campo deve ser deixado em branco, ou preenchido com a *string NULL*.

  Os módulos do AISF são:

1. ***Signature Identification Module (SigIdModule)****:* este é o primeiro e mais importante módulo do AISF. Ele é responsável pela identificação do objeto, assim como alguns detalhes do próprio modelo.

   Descrição dos campos:
   ModuleLength: 7
   Version: Este campo identifica a versão do modelo AISF. Deve conter uma *string* de caracteres padronizada, observando o formato da versão atual do AISF *0.0.7*.
   ID: Contém uma *string* de caracteres que identifica o ataque descrito pelo AIS. É um número único, atribuído pela entidade que administra o modelo. Esta *string* de caracteres deve ser da seguinte forma: AIS-XXXXYY, onde XXXX corresponde ao ano no qual foi gerada a assinatura de ataque, e YY corresponde a um número que deve ser incrementado a cada novo AIS. Este número é importante para estabelecermos uma relação de causa/efeito, além de permitir uma busca mais ágil por assinaturas.

Name : Nome dado ao evento intrusivo especificado. Este deve ser uma *string* com nome relevante e relacionado ao problema**.**

SerialNumber: Número que descreve a versão do AIS, baseado na data de sua geração. Este número segue o padrão utilizado pelo BIND [ISC02], ou seja, YYYYMMDDXX, onde: YYYY corresponde ao ano, MM ao mês, DD ao dia, e XX serve como diferenciador de versões. EX.: 2002012300.

Credits: Campo que identifica o(s) autor(es) do AIS. Este deve ser uma *string* preenchida com o nome do indivíduo ou instituição que divulgou a assinatura de ataque.

NextModule: Identificação do próximo módulo.

2. ***Signature Information Module (SigInfoModule):*** é utilizado para representar informações mais descritivas sobre o ataque, como por exemplo a descrição do evento intrusivo e os sistemas afetados por este evento. Assim como os módulos subseqüentes, este módulo é opcional.

Descrição dos campos:

ModuleLength: 9

SecurityLevel: Decimal de 0 a 100 que descreve o nível de segurança, ou seja, quão perigoso este evento pode ser.

Category: *String* que define a categoria do evento intrusivo, em: *Scan* (varredura), *DoS* (negativa de serviço), ou *PenetrationAttack* (ataques de penetração).

Description: Texto que descreve todo o evento intrusivo.

OtherIDs: String contendo uma ou mais referências auxiliares para este ataque, como por exemplo o CVE da [CVE02], o número do *Advisory* do [CER02] ou outro.

Impact: Texto que descreve a conseqüência deste evento ou o estado do sistema após ser afetado pelo ataque.

AttackScenario: Este campo deve armazenar um texto com as condições necessárias para que a intrusão ocorra.

TargetSystem: Texto que descreve os sistemas que geralmente são afetados por este evento.

NextModule: Identificação do próximo módulo.

3. ***Signature Characteristics Module (SigCharModule):*** pertence à classe dos módulos informativos, que pode relatar informações inerentes ao ataque, como por exemplo a porcentagem de falsos positivos que este evento pode gerar em um SDI.

Descrição dos campos:

ModuleLength 6

EaseofAttack: Inteiro de 0 a 10 que define quão facilmente este ataque pode ser aplicado com sucesso sobre um alvo.

FalsePositive: Inteiro podendo variar de 0 a 10 que representa uma porcentagem estatística da ocorrência de falsos positivos na detecção deste ataque.

FalseNegative: Inteiro podendo variar de 0 a 10 que representa uma porcentagem estatística da ocorrência de falsos negativos na detecção deste ataque.

RecommendedActions: Texto que descreve as ações preventivas e/ou corretivas recomendadas para serem tomadas sobre um sistema, após detectar-se que o mesmo tenha sido afetado.

NextModule: Identificação do próximo módulo

4. ***Data Link Protocols Module for Ethernet (DlinkProtoModuleEth):*** refere-se aos dados do protocolo de enlace, e no caso retrata o Ethernet.

Descrição dos campos:

ModuleLength: 4

SourceAddress: Deve conter uma expressão que relaciona o endereço MAC de quem enviou o pacote.

DestinationAddress: Deve conter uma expressão que relaciona o endereço MAC do destinatário do pacote.

NextModule: Identificação do próximo módulo.

5. ***Network Protocols Module for IPv4 (NetProtoModuleIPv4):*** descreve os dados inerentes à camada de rede, e no caso da pilha TCP/IP, o protocolo Ipv4.

   Descrição dos campos:

   ModuleLength: 4

   TotalLength: Especifica o tamanho do cabeçalho e dados existentes no datagrama IP. Este deve ser especificado em hexadecimal, ou decimal equivalente.

   Protocol: Este campo deve conter o hexadecimal, ou decimal equivalente, do campo *Protocol* do cabeçalho IP.

   NextModule: Identificação do próximo módulo.

6. ***Transport and Control Protocols Module for TCP (TransConProtoModuleTCP):*** apresenta dados relativos à camada de transporte da pilha TCP/IP, isto é, o protocolo TCP.

   Descrição dos campos:

   ModuleLength: 12

   TypeOfService: Este campo pode ser preenchido com uma expressão relacionada com o hexadecimal do campo TOS do cabeçalho IP.

   FragmentId: Do mesmo modo que o anterior, este campo deve conter uma expressão relacionada ao campo *identification* do cabeçalho IP.

   Flags: Este campo refere-se as *flags* do protocolo IP. Deve conter uma expressão em hexadecimal.

   FragmentOffset: Este deve conter uma expressão com o valor em hexadecimal do deslocamento do pacote.

   TTL: Este campo deve conter uma expressão condizente com o campo TTL do IP. Este pode ser escrito em hexadecimal ou decimal;

   SourceAddress: Deve conter uma expressão relacionada ao IP origem do pacote. Este pode ser escrito das seguintes formas: em hexadecimal, na divisão padrão de oito em oito bits (Ex.: 192.123.201.1), ou ainda com alguma variável (Subseção XXXX). Se escrito na forma padrão, é ainda possível

definir uma máscara de rede (Ex.: 192.123.201.1/24).

DestinationAddress: Aceita o mesmo conteúdo do campo *Source Address*, mas deve relacionar-se ao endereço de destino dos pacotes.

Options: Deve conter uma expressão em hexadecimal correspondente ao campo *Options* do cabeçalho IP.

NextModule: Identificação do próximo módulo.

7. ***Transport and Control Protocols Module for UDP (TransConProtoModuleUDP):*** corresponde às informações relativas ao cabeçalho do protocolo UDP.

Descrição dos campos:

ModuleLength: 4

SourcePort: Expressão relacionada à porta UDP de origem. Pode ser escrito na forma hexadecimal, decimal, variável ou como um intervalo de portas (porta_inicio:porta_fim).

DestinationPort: Expressão relacionada à porta UDP de destino. Pode ser escrito na forma hexadecimal, decimal, variável ou como um intervalo de portas (porta_inicio:porta_fim).

NextModule: Identificação do próximo módulo

8. ***Transport and Control Protocols Module for ICMP (TransConProtoModuleICMP):*** este módulo é responsável por representar informações relativas ao protocolo ICMP.

Descrição dos campos:

ModuleLength: 6

Type: Hexadecimal ou decimal que representa o Tipo do ICMP

Code: Hexadecimal ou decimal que representa o Código do ICMP

ID: Contém as informações em hexadecimal ou decimal do campo ID do protocolo ICMP

SequenceNumber: Contém as informações em hexadecimal ou decimal do campo Sequence Number do protocolo ICMP

NextModule: Identificação do próximo módulo

9. ***Payload Information Module (PayloadInfoModule):*** é um dos módulos mais importantes do AISF. Ele pode armazenar informações a respeito da carga dos pacotes numa sessão de ataque. É consideravelmente útil para descrever os ataques de penetração, como por exemplo, aqueles que exploram *buffer overflows*. Este módulo também é opcional.

Descrição dos campos:

ModuleLength: 6

Size: Valor em hexadecimal correspondente ao tamanho em bits da carga de um pacote analisado.

Offset: Valor em hexadecimal correspondente ao deslocamento da carga onde deve se iniciar a busca por padrões.

Depth: Valor que define a dimensão da análise da carga, ou seja, quantos bits devem ser analisados dentro do pacote. Deve ser também em hexadecimal.

Contents: Conteúdo da carga de um pacote ou de uma conexão inteira. Será analisado mais detalhadamente na subseção 3.3.5.

NextModule: Identificação do próximo módulo