Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de *TI*

Laerte Peotta de Melo

Orientador: Paulo Roberto de Lira Gondim

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM - 330/08
Brasília / DF: Março/2008

Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de *TI*

Laerte Peotta de Melo

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

Paulo Roberto de Lira Gondim, Doutor, Ene/UnB
Orientador

Vagner José do S. Rodrigues, Doutor, Universidade Federal de Goiás
Examinador Externo

Paulo Henrique Portela Carvalho, Doutor, Ene/UnB
Examinador Interno

Brasília, 14 de Março de 2008

FICHA CATALOGRÁFICA

Melo, Laerte Peotta de.

Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de *TI* / Laerte Peotta de Melo. Brasília , UnB, 2008.

181 p., 210 x 297 mm. (ENE/FT/UnB, Mestre, Dissertação de Mestrado - Universidade de Brasília. Faculdade de Tecnologia.)

Departamento de Engenharia Elétrica

1. Risco Digital, 2. Segurança da Informação, 3. Política de Segurança, 4. Tecnologia da Informação, 5. Gestão de Risco

PUBLICAÇÃO: PPGENE.DM - 330/08

REFERÊNCIA BIBLIOGRÁFICA

Laerte Peotta de Melo(2008). Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de *TI*. Dissertação de Mestrado, Publicação PPGENE.DM - 330/08 14 de Março de 2008, Departamento de Engenharia Elétrica, Universidade de Braslia, Brasília-DF, 181 p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Laerte Peotta de Melo
TÍTULO DA DISSERTAÇÃO: Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de *TI*
GRAU/ANO:(Mestre)/2008.

Laerte Peotta de Melo (peotta@gmail.com)
Campus Universitário Darcy Ribeiro - Asa Norte
CEP 70910–900 - Brasília - DF - Brasil

Dedicatória

A *Deus* que tudo criou.

A minha esposa *Valéria* e minhas filhas *Nicole* e *Natália* pela compreensão e paciência.

Aos meus pais, *Melo* e *Teresa*, por terem me ensinado que os valores da vida estão na simplicidade.

Ao professor e orientador *Paulo Gondim*, pela grande paciência e prazer em ensinar, mostrando o caminho a seguir quando imaginava não haver.

Ao Professor Doutor *Louis Pasteur*, que mesmo eu não o tendo conhecido e ele não estar mais entre nós, uma de suas frases me acompanha sempre: *"Um pouco de ciência nos afasta de Deus. Muito, nos aproxima"*.

Agradecimentos

A meus colegas de trabalho da Diretoria de Gestão da Segurança: *Carlos Eduardo Versati, Fernando Augusto Higa, Vinicius Marques, Daniel Lyra, Dino Amaral, Francimara Viotti, José Bergo*, que me apoiaram e me ajudaram neste árdua caminhada.

Aos amigos e colegas de divisão *Érico, João, Tavares e Xander*.

Ao colega e engenheiro de *software José Benedito*, pelas idéias inovadoras.

Aos meus colegas da Universidade de Brasília, que quando eu estava cansado sempre apareciam e me convidavam para um café ou apenas para uma conversa motivadora: *Simone Cintra, Pablo, Carino Rodrigues, Paulo, Vaguetti* e tantos outros que me apoiaram.

Aos professores que dividiram seus conhecimentos comigo: *Leonardo R. A. X. Menezes, José Camargo, Maria Emília* e por fim, mas não menos importante, *Anderson Nascimento*, pela sua grande capacidade intelectual e por estar sempre disposto a uma conversa.

Ao colega acadêmico professor *João Eriberto* pelo apoio e incentivo.

Ao Dr. *Helvio Peixoto*, que cedeu seus conhecimentos e técnicas me dando o incentivo necessário neste trabalho.

Ao Dr. *Leslie Lamport* criador do latex, *Linus Torvalds* idealizador do *linux* e *Patrick Volkerding* o criador do *Slackware*, onde esta dissertação foi escrita.

Resumo

Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de *TI*

Autor: Laerte Peotta de Melo

Orientador: Paulo Roberto de Lira Gondim

Programa de Pós-graduação em Engenharia Elétrica

Brasília, Março de 2008

Com o surgimento dos computadores passaram a ser necessárias ferramentas automatizadas para proteger a informação armazenada, tentando proteger também os recursos, ou seja, os próprios computadores e a reputação de uma organização. A utilização de redes de computadores e processamentos de sistemas distribuídos geraram um ganho considerável com o tratamento das informações, melhor qualidade dos processos e maior velocidade na disponibilização da informação. Surgiu também a necessidade de um sistema de segurança mais adequado, que garantisse a integridade, confidencialidade e disponibilidade da informação. Normas como a *ISO 17799* e *ISO 27001* tratam de segurança da informação, e sugerem fortemente a criação de um modelo para gestão de risco. A Governança corporativa caminha para a integração com *TI* com a utilização de metodologias como o *COBIT* e *ITIL*. Neste trabalho elaborou-se um estudo do tema gestão de risco em *TI*, assim como a proposta de integração e criação de ferramenta que informasse o risco em tempo real à divulgação de uma vulnerabilidade.

Palavras-chave: Risco Digital, Segurança da Informação, Política de Segurança, Tecnologia da Informação, Gestão de Risco

Abstract

Proposal the Methodology the Risk Management in the Corporate Environment of Information Technology

Author: Laerte Peotta de Melo

Supervisor: Paulo Roberto de Lira Gondim

Programa de Pós-graduação em Engenharia Elétrica

Brasília, Março de 2008

With the emergence of computers have become automated tools necessary to protect the information stored, also trying to protect the resources, or their own computers and reputation of an organization. The use of computer networks and distributed processing systems generated a considerable gain to the processing of information, better quality of the processes and greater speed in the availability of information. He came up also the need for a security system more complex, which ensures the integrity, confidentiality and availability of information. Standards such as ISO 17799 and ISO 27001 deal of information security, and strongly suggest the creation of a model for management of risk. The Corporate Governance headed for integration with TI with the use of methodologies such as COBIT and ITIL. In this paper sought is a study of the theme of risk management in IT, as well as the proposed creation of tool integration and to inform the risk in real-time disclosure of vulnerability.

Keywords: Digital Risk, Security Information, Security Policy, Information Tecnology, Risk Assessment

Sumário

Lista de Tabelas

Lista de Figuras

Lista de Símbolos, Nomenclatura e Abreviações

ABNT	Associação Brasileira de Normas Técnicas
BSC	Balanced Scorecard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IDS	Intrusion Detection System
IEC	the International Electrotechnical Commission
IP	Internet Protocol
ISO	International Standards Organization
MD5	Message Digest
NBR	Normas brasileiras
ODBC	Open Data Base Connectivity
PIB	Código de Identificação do Bem
POC	Proof of concept
SGSI	Sistema de gestão da segurança da informação
SI	Segurança da Informação
SQL	Structured Query Language
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagrama Protocol
UML	Unified Modeling Language
UP	Unified Process
XML	Extensible Markup Language

Capítulo 1

Introdução

1.1 Contexto

A informação é o bem mais precioso de uma organização. Antes do surgimento dos computadores, as informações eram armazenadas em papel e colocadas em grandes arquivos de aço. Informações mais valiosas ficavam em cofres de segurança.

Com o surgimento dos computadores passaram a ser necessárias ferramentas automatizadas para proteger a informação armazenada, tentando proteger também os recursos, ou seja, os próprios computadores e a reputação de uma organização.

A utilização de redes de computadores e processamentos de sistemas distribuídos gerou um ganho considerável com o tratamento das informações, melhor qualidade dos processos e maior velocidade na disponibilização da informação. Surgiu também a necessidade de um sistema de segurança mais efetivo, que garantisse a integridade, confidencialidade e disponibilidade da informação.

A segurança é um problema cada vez mais importante. Nos últimos anos, a quantidade de ataques e invasões a sistemas aumentou consideravelmente. Segundo uma pesquisa feita pela empresa de consultoria *IDC* [18][19] realizada em 2005, envolvendo 90 das 500 maiores empresas, mostra que, em 2006, 80% pretende incrementar os investimentos em segurança em 35%.

Outro aspecto relevante envolvendo a área de segurança é a necessidade de transparência das informações por parte das organizações, cada vez mais exigida pelo mercado. Isso pode ser confirmado com o número crescente de exigências dos órgãos reguladores. Para enfrentar os novos desafios da Governança corporativa, as áreas de *TI* contam com alguns modelos de gestão que, se corretamente aplicados, asseguram a conformidade com as melhores práticas de processos e segurança da informação. Os principais modelos são:

- COBIT[1] [38] para a governança de TI;
- ITIL[2] [60] para a gestão de serviços de TI;
- ISO 17799[1], ISO 27001 [40] ou a BS-7799 [9] para a gestão de segurança da informação;
- Normas para gestão de risco como a *AS/NZS 4360* [6]
- Norma exclusiva para gestão de risco *ISO 31000* [39] (a ser lançada em 2008).

A segurança está intrinsecamente ligada à avaliação dos riscos e ameaças, que deve ser baseada em uma análise de risco completa e constante. Sempre há um nível de risco associado a qualquer ativo. Um sistema seguro é aquele em que todas as ameaças possíveis foram analisadas e todos os riscos avaliados e aceitos.

Fica claro que um ambiente sem ameaças e sem riscos é uma tarefa difícil, para não dizer quase impossível, aonde se quer chegar é obter um ambiente com suas ameaças mapeadas e com o risco aceitável. É claro que deve encontrar um ponto de equilíbrio entre o que proteger e qual nível de proteção oferecer. Uma empresa que tem dados sigilosos pode necessitar de uma segurança maior, outras empresas podem não se preocupar tanto com seus dados e acabam optando por um nível menor de segurança.

Uma coisa é certa, em qualquer ambiente sempre se deve esperar o pior, buscando fazer o melhor, antecipando o problema.

1.2 Motivação

A segurança da informação visa proteger dados críticos de uma empresa. Essas informações geralmente são armazenadas eletronicamente, enviadas por e-mail, gravadas em filmes, arquivos de computador, faladas ou mesmo expostas. No entanto, as informações são essenciais para se manter a competitividade de uma organização, a simples divulgação de um determinado assunto pode levar a empresa à falência, denegrindo a imagem ou mesmo perdendo a competitividade. A falta efetiva de segurança pode atingir a integridade das organizações e colocar em risco a sua existência.

Com a grande utilização dos computadores, tornou-se clara a necessidade de investimentos em segurança, seja através de infra-estrutura, ou de ferramentas automatizadas para proteger arquivos e informações armazenadas em meio digital.

Outras mudanças importantes que afetaram diretamente a área de segurança foram a inclusão de sistemas distribuídos e a criação de redes utilizadas para

[1]Control Objectives for Information and related Technology
[2]Information Technology Infrastructure Library

transmitir informações entre uma central de processamento e o usuário do sistema. O termo segurança de rede é, de certa forma, incorreto, pois quase todas as organizações possuem seus equipamentos interconectados, então o termo mais correto seria segurança de inter-rede [57].

Não existem limites claros entre a segurança física e a lógica [56], pois a segurança é dependente do seu elo mais fraco, que constantemente é associado ao usuário do sistema. Como exemplo, pode-se citar o vírus de computador, que pode chegar via inter-rede ou ser introduzido através de um disquete, no entanto, após a contaminação são necessárias ferramentas internas do sistema para se recuperar das ações do vírus.

A segurança envolvida em inter-redes, a princípio, não é simples para iniciantes, necessita de pessoas altamente capacitadas, e em diversas áreas de atuação. Os requisitos necessários para a segurança são auto-explicativos: confidencialidade, autenticidade e integridade, no entanto os mecanismos usados para atender a esses requisitos são complexos, e implementa-los pode ser uma tarefa árdua.

Quando se pretender desenvolver algum mecanismo que envolva segurança deve-se sempre considerar os ataques a que esses recursos estão sujeitos. Por esse motivo deve-se atentar a testes de segurança sucessíveis e planejados, buscando antever ataques complexos que busquem explorar um ponto fraco no mecanismo.

O número de incidentes reportados ao cert.br[3] pode não representar o valor correto, estaria sendo conservador, pois engloba apenas o que foi informado, existindo incidentes que, por qualquer motivo não tenham sido reportados.

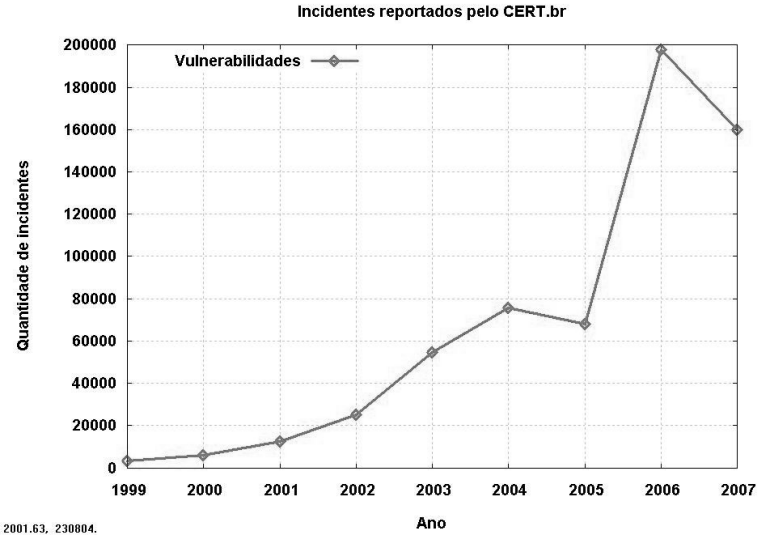

Figura 1.1: Incidentes reportados ao cert.br

Como se pode ver no gráfico da Figura 1.1 o número de incidentes é crescente, no entanto, no ano de 2007 houve uma ligeira queda, e diversos fatores podem

[3]www.cert.br

explicar essa queda, mas dificilmente um fator isolado seja responsável pela melhoria da segurança, o principal poderia ser a maior preocupação que empresas e usuários passaram a ter em relação à sua própria segurança, uma cultura sobre essa própria segurança está surgindo e se consolidando nas organizações, cada vez mais preocupada com o seu elo mais fraco.

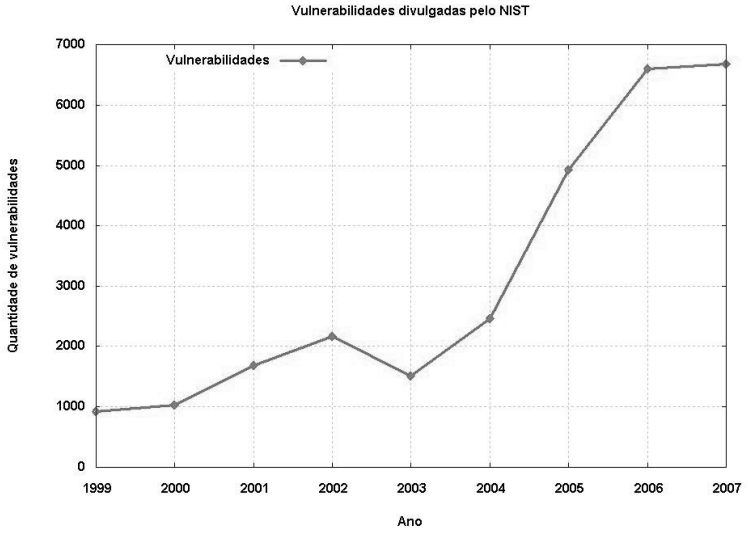

Figura 1.2: Vulnerabilidades divulgadas pelo *NIST*

Não somente os incidentes estão crescendo, o número de vulnerabilidades também vem aumentando (ver Figura 1.2). Isso se dá por diversos fatores, como um número maior de aplicativos, necessidade de liberação o mais rápido possível da aplicação desenvolvida, que por falta de testes mais estensivos, acaba por comprometer a segurança para que o software esteja disponível o quanto antes, entre outros diversos fatores.

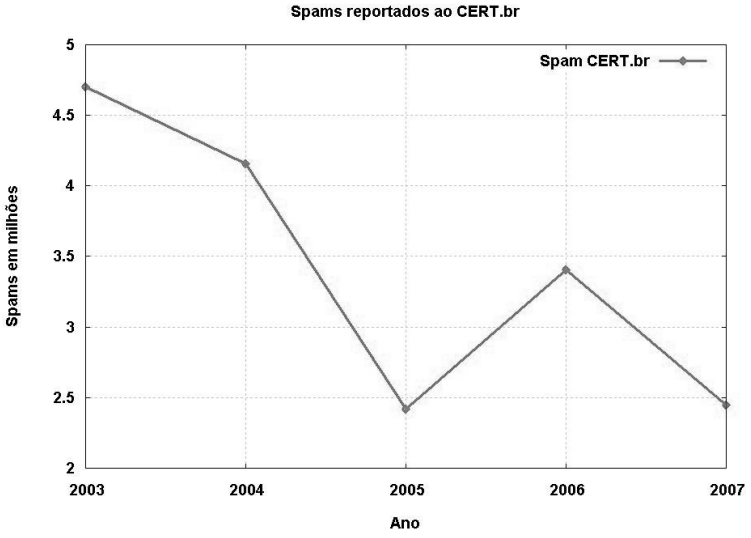

Figura 1.3: Estatística de *spam* publicada pelo cert.br

O grande número de *spams* (mensagens não solicitadas) inicialmente era crescente (Figura 1.3), no entanto diversos fatores contiveram esse problema, como maior preocupação com a segurança, instalação de mecanismos para evitar a proliferação desses *spams*, entre outros, e mesmo hoje, as pessoas estão mais conscientizadas, evitando essas mensagens. Isso se deve ao fato de que a utilização de computadores já se tornou popular, em algumas situações é considerado um eletrodoméstico. O próprio governo brasileiro busca implementar laboratórios de informática em escolas públicas, e para comunidades carentes, os chamados telecentros.

Com toda a comodidade das tecnologias recentes, pode ocorrer uma falsa sensação de segurança, onde algumas pessoas acabam se considerando seguras em suas casas, no entanto, essa segurança esbarra na utilização indiscriminada e sem preocupação do comércio eletrônico e acesso a bancos. Por esse motivo o *spam* se caracteriza por uma praga, enchendo as caixas de correios eletrônicos e tentando ludibriar as pessoas para que acessem essas mensagens e que, em alguns casos, instalam ferramentas que capturam informações críticas dos usuários como senhas de bancos, números de cartões de crédito, senhas de email, sites de relacionamentos, leilões entre outros.

Existe uma necessidade maior de segurança para sistemas compartilhados, que podem ser acessados pela intra-rede, tanto pela INTERNET, quando pela rede local. A base para a segurança entre o computador e esses sistemas é a utilização de criptografia que busca garantir os requisitos mínimos de autenticidade, confidencialidade e integridade, discutidos anteriormente neste capítulo.

1.3 Objetivos

Este trabalho busca elaborar um estudo referente a metodologias relacionadas à análise e gestão de risco, implementando uma ferramenta para localização de vulnerabilidades e ameaças, capaz de calcular um *score* para o risco de acordo com um *hardware* ou *software* vulnerável, priorizando as ações de correção de forma a atender do risco crítico ao menos crítico e mantendo a base de conhecimento utilizado.

1.4 Contribuição

Implementação de sistema de gestão de risco com identificação e tratamento de vulnerabilidades, utilizando a metodologia de informações sobre vulnerabilidades do *CVE* e cálculo do risco utilizando o *CVSS*, ambos livres, que permite uma adequação do risco ao ambiente onde este é executado.

Produzir uma ferramenta capaz de :

- Determinar o valor dos ativos de informação bem com a sua criticidade para a organização;
- Estimar uma determinada probabilidade de uma ameaça ocorrer e possibilitar o cálculo do risco;
- Identificar pontos vulneráveis e subsidiar decisões para eliminiar ou diminuir o risco;
- Permitir a criação de estratégia para mitigar os riscos;
- Possibilitar a correta identificação dos ativos.

Permitir conhecer informações sobre *hardware* e *software* que são obtidas através de inventário automatizado, que permite a correlação com as bases *CVE* e *CVSS*, identificando os ativos vulneráveis em tempo real e registrando em base de dados, permitindo uma ação para eliminar, mitigar, ou aceitar o risco.

Priorização de incidentes, permitindo uma tomada de decisão baseada na resposta apropriada para o problema mais crítico.

Também foi efetuado um estudo detalhado da metodologia *CVSS*, buscando mostrar o grande valor quanto a sua aceitação como padrão no cálculo do risco das vulnerabilidades.

1.5 Organização do trabalho

Seguiu-se a seguinte divisão do trabalho: O Capítulo 1 trata da introdução mostrando as premissas iniciais para este estudo e dados estatísticos da área. No Capítulo 2 segue uma breve descrição com conceitos sobre segurança da informação, vulnerabilidades, seu ciclo de vida e ameaças. Normas como *ISO* 17799 e *ISO* 27001, *Sarbanes Oxley*, modelos de gestão como o *COBIT* e *ITIL* e a governança de *TI*, assim como um modelo de integração são discutidas no Capítulo 3. Gestão de ativos e métodos para inventário, bem como suas ferramentas são tratadas no Capítulo 4. Os Capítulos 5 e 6 tratam de gestão de risco, onde são detalhados os modelos *CVSS* e *CVE* e as metodologias de risco conhecidas como o *OCTAVE, CORAS* e *AGRIS*, finalizando com um estudo comparativo entre essas metodologias, respectivamente. A metodologia proposta, sua integração com o *framework* e demonstração da ferramenta com os estudos de caso e requisitos considerados, assim como um estudo comparativo entre ferramentas para gestão de risco são apresentados no Capítulo 7. Finalizando, respectivamente com os Capítulos 8 e 9, as conclusões seguida pelas referências bibliográficas e anexos, onde constam a relação e conteúdo dos artigos publicados, bem como os requisitos do sistema e os estudos de caso, discutidos no Capítulo 7.

Capítulo 2

Conceitos sobre segurança da informação

A informação é o bem mais precioso para qualquer instituição, seja ela com fins lucrativos ou não. Um comprometimento da informação pode causar não apenas perdas financeiras, mas também perdas em relação à imagem, podendo ser mais desastrosa para a instituição.

A segurança da informação está envolvida com proteção dos dados, sendo caracteristicas básicas os atributos:

- Confidencialidade: assegura que a informação estará acessível somente a quem tem autorização para acessá-la;
- Integridade: assegura que a informação está integra, ou seja, não houve alteração entre a origem e o destino;
- Autenticidade: assegura que a informação é autentica, de quem realmente deve ser;
- Disponibilidade: a informação estará disponível quando necessário o acesso;
- Privacidade: um termo bastante complexo, mas pode se definir, de maneira universal, como um meio de se preservar a individualidade de cada pessoa, sendo a privacidade um direito adquirido por lei;
- Anonimato: manter a identidade de um indivíduo ou entidade escondida ou protegida contra terceiros;
- Não Repúdio: é a maneira de garantir que o emissor de uma mensagem ou informação não poderá negar sua autoria.

2.1 Vulnerabilidades

Vulnerabilidade é a fraqueza que pode ser explorada [26] em um sistema de informação que pode envolver pessoas, processos ou tecnologia[20].

A análise de vulnerabilidades é o primeiro passo para a gestão e análise de risco [27].

Existem diversos tipos de vulnerabilidade, mas neste estudo pode se dividir em dois grupos principais: Lógicas e físicas.

2.1.1 Vulnerabilidades lógicas

Este tipo de vulnerabilidade basicamente trata de falhas em *software*, que podem ser exploradas de diversas maneiras, seja localmente ou remotamente (maior risco). Algumas maneiras para se explorar esse tipo de vulnerabilidade são através de:

- *Exploits*: Programas automatizados para se obter algum privilégio ou ação não esperada pelo sistema;
- Envenenamento de dns: Conhecido como dns *poisoning* que altera uma tabela de endereçamento do dns redirecionando o tráfego para um endereço que não é o verdadeiro;
- *Buffer overflow*: Área de memória onde um programa está sendo executado, que executando um procedimento ilícito causa o estouro do *buffer* permitindo executar programas indesejados;
- Elevação de privilégios: Um usuário comum do sistema obtém, de maneira ilícita, permissão de acesso com maior privilégio.
- Negação de serviço: Conhecido como ataque *Denial of Service* ou *DoS*, basicamente busca sobrecarregar um determinado sistema, localmente ou remotamente, para que o serviço fique indisponível.

2.1.2 Vulnerabilidades físicas

A segurança física é tão importante quanto à lógica, agora caso a segurança física seja rompida não existe segurança lógica que resista[10] por muito tempo, pois um atacante pode por exemplo, utilizando-se de ferramentas apropriadas, inserir uma conta de usuário no sistema.

Monitores emitem radiação eletromagnética e essa radiação pode ser captada a distância, essa interceptação é conhecida como ataque *tempest*, sendo uma vulnerabilidade que pode ser eliminada instalando redes de proteção, evitando que

essa radiação escape ao ambiente, ou ainda, uma pessoa pode simplesmente olhar por cima dos ombros de alguém e obter a informação desejada.

Equipes de limpeza podem causar tantos problemas quanto um *hacker*, geralmente esse pessoal tem as chaves de todo o prédio, por isso trancar a sala de servidores não resolve o problema. Alguém descuidado pode desligar servidores, e até mesmo a chave geral, causando indisponibilidade.

É interessante saber que o nível de proteção solicitado depende do que se quer proteger e o seu valor para uma organização, também é coerente saber qual nível de sofisticação um intruso tem e sua motivação para obter a informação. Empresas que produzem armas devem se preocupar bem mais com a segurança do que empresas que produzem palitos de dentes.

2.1.3 Ciclo de vida de vulnerabilidades

Toda vulnerabilidade tem um ciclo de vida definido para cada fase[30] que reflete diretamente no risco associado. Na Figura 2.1 são mostrados cinco pontos distintos e marcados pelo tempo: descoberta, divulgação, POC, exploração e correção da vulnerabilidade.

O tempo para descoberta de uma vulnerabilidade não pode ser medido, pois existem diversos fatores a serem ponderados, como: motivação, qualidade de um software ou hardware, utilização de um software, pois quanto mais utilizado, mais testado.

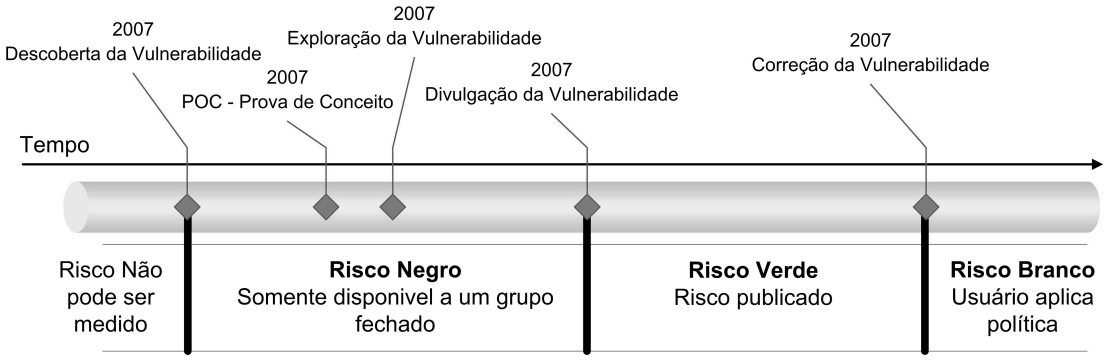

Figura 2.1: Ciclo de vida de vulnerabilidades

O tempo da descoberta e da divulgação é considerada a criação de um *exploit*, onde um grupo geralmente fechado testa e explora a vulnerabilidade. No intervalo dessa fase, geralmente, é criada uma prova de conceito, também chamado de POC. Esse grupo é conhecido como risco negro, pois a vulnerabilidade não é de conhecimento público, e pode estar sendo explorada sem conhecimento do fabricante ou usuário do software ou hardware.

O tempo entre a divulgação da vulnerabilidade e sua correção passa a ser de conhecimento público, essa fase é chamada de risco verde, no entanto, empresas

sérias de desenvolvimento podem ter um grupo constantemente procurando vulnerabilidades em seus produtos de maneira a se antever a esse tempo, ou seja, o grupo negro passa a fazer parte da empresa, e o tempo entre a descoberta e a correção da vulnerabilidade passa a ser uma única fase.

A divulgação ao público, sobre a existência de uma vulnerabilidade, geralmente é feita em *fóruns* e *websites* sobre segurança como *Securityfocus*[1], ISS[2] - *Internet security systems*, *Secunia*[3] - *Vulnerability and virus information* e *FrSirt*[4] - *French security incident response team.*

A divulgação é uma fase muito crítica, pois incorre em freqüentes ataques buscando explorar a vulnerabilidade, mesmo que de maneira não motivacional, apenas pelo fato de poder ser explorada, é nessa fase que as informações são repassadas: é disponibilizada gratuitamente ao público; é avaliada por especialistas na área de segurança e analistas de risco; é disponibilizada de maneira confiável independente do canal de comunicação.

O tempo a partir da criação de uma correção disponibilizada passa a ser chamado de risco branco, ou seja, a empresa utiliza um produto que possui uma vulnerabilidade e que tem correção, mas no entanto desconhece a própria vulnerabilidade.

2.2 Ameaças

Ameaça é qualquer circunstância ou evento com o potencial de causar impacto sobre a confidencialidade, integridade ou disponibilidade de informação ou sistemas de informação [32].

Ameaças fazem parte do cotidiano de toda empresa [21], qualquer tarefa a ser feita, ou mesmo equipamentos estão constantemente sujeitos a ameaças, que são definidas por uma ocorrência que pode danificar ou prejudicar uma atividade. As ameaças podem ser mal-intencionadas quando existe a intenção de prejudicar uma pessoa ou danificar um equipamento, ou pode não ser intencional quando um erro humano pode acarretar um prejuízo.

2.2.1 Tipos de ameaças

Deve-se considerar alguns tipos de ameaças, que basicamente são divididas em dois tipos [52]:

[1] http://www.securityfocus.com/
[2] http://www.iss.net/
[3] http://secunia.com/
[4] http://www.frsirt.com/

1. Ameaças Internas: De longe, a maior ameaça que as empresas sofrem vem de pessoas internas. Pode até parecer estranho, mas são essas pessoas de dentro da empresa que conhecem os ativos críticos, tem acesso a informações e sabem como funciona a estrutura da organização.

2. Ameaças Externas: Podem ser o principal agravante para empresas que mantém conexão direta com a Internet, ou outra forma de conexão com empresas terceiras, como uma extranet. Os métodos que pessoas externas utilizam são mais limitados se comparados com os utilizados pelas pessoas ligadas diretamente à organização. Neste ponto pode-se levantar diversos tipos de pessoas que podem gerar uma ameaça:

    - *Hackers*: profissionais de segurança que conhecem a fundo protocolos de rede, programação e sistemas operacionais de rede. Quando motivados ficam horas estudando cuidadosamente o alvo, analisando códigos fontes e códigos executáveis, fragilidades conhecidas, engenharia reversa, simplesmente para descobrir falhas ocultas em sistemas.
    - *Crackers*: Detêm os mesmos conhecimentos dos hackers, sendo uma diferença crucial entre eles: o ganho financeiro. São tidos como criminosos, roubando informações para revendê-las, usam todo o tipo de métodos e informações para poder ganhar acesso a uma determinada rede. Esse tipo de pessoa vem sendo recrutada pelo crime organizado geralmente para conseguir informações que de outra maneira seriam impossíveis de se conseguir.
    - *Script Kiddies*: Basicamente utilizam ferramentas automatizadas, que não são criadas por eles. Mas esse tipo de pessoa pode causar grandes danos, pois não procuram por um alvo em especial, e sim apenas testar uma ferramenta no maior número de redes possível, buscam ser reconhecidos como *hackers*.
    - Terroristas: A guerra da informação, hoje, é realidade e existem pessoas que procuram difamar organizações e governos através da rede de computadores. É a chamada *Cyberwar*. Não só organizações criminosas utilizam a Internet para cometer seus crimes, jovens adolescentes de diversos países tentam expressar suas ideologias atacando sites, desfigurando suas informações e divulgando suas crenças.

Existem diversos tipos de ameaças que podem comprometer um sistema ou uma rede:

- Ameaças físicas: Desastres, bombas, incêndio, falta de energia, alagamentos, etc;
- Ameaças humanas: Invasão, roubo, trapaça, suborno, espionagem, sabotagem e mesmo acidentes;
- Ameaças de *software*: Vírus, *worms*, *trojans*, *deny of services*.

É preciso criar uma modelagem que permita identificar e classificar as ameaças que possuem maior chance de afetar à organização.

O processo para se identificar ameaças deve ser contínuo e não apenas em momentos únicos, deve ser constantemente executado e em horários diferentes, pois é muito difícil identificar todas as ameaças em uma única procura.

A infra-estrutura de uma organização é dinâmica, sofre constantes alterações, sejam elas incluindo equipamentos, serviços, ou mesmo retirando de funcionamento esses equipamentos, mudando-se de lugar, entre outros tipos de alteração.

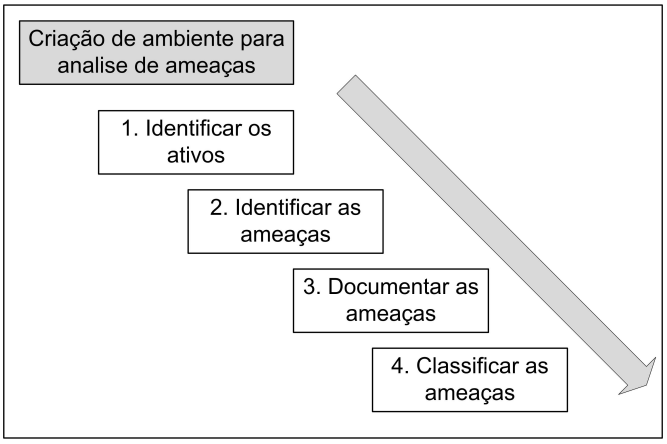

Figura 2.2: Ciclo para análise de ameaças

Por esse motivo a Figura 2.2 descreve os passos necessários para se criar um ambiente para análise de ameaças. A identificação dos bens ou ativos é o primeiro passo para uma análise de ameaças [23], é preciso conhecer o ambiente para poder gerenciar.O próximo passo é identificar as ameaças, infra-estrutura da organização e quais fatores podem comprometer a segurança.

É preciso documentar todas as ameaças encontradas [22], podendo ser feita a documentação através de relatórios definindo os pontos críticos centralizando todas as informações buscando facilitar as consultas.

O ponto mais crítico na criação do ambiente para análise de ameaças é como classificar as informações obtidas. As ameaças devem ser classificadas priorizando as mais críticas, as que representam maior risco para a organização.

O processo de classificação deve considerar a probabilidade dos danos que um ataque possa causar à infra-estrutura da organização. Pode ocorrer de algumas ameaças não causarem nenhum impacto aparente, não justificando uma ação quando se compara o risco causado com o custo para solucionar o problema, ou seja, o gasto sendo maior que o custo da informação, o que torna a solução inviável.

2.3 Tipos de ataques

Para entender de maneira completa as vulnerabilidades[11] e ameaças é necessário entender os ataques aos quais uma infra-estrutura está sujeita.

É um ataque à segurança do sistema que se deriva de uma ameaça inteligente [57], isto é, um ato inteligente que seja uma tentativa deliberada (especial no sentido de um método ou de uma técnica) de evadir serviços, de burlar e de violar a política da segurança de um sistema [55].

Ao longo do tempo os ataques a sistemas conectados à INTERNET tem se tornado mais sofisticados, no entanto a habilidade dos atacantes, bem como o conhecimento exigido, diminuíram consideravelmente (Figura 2.3), decorrendo basicamente da automatização desses ataques.

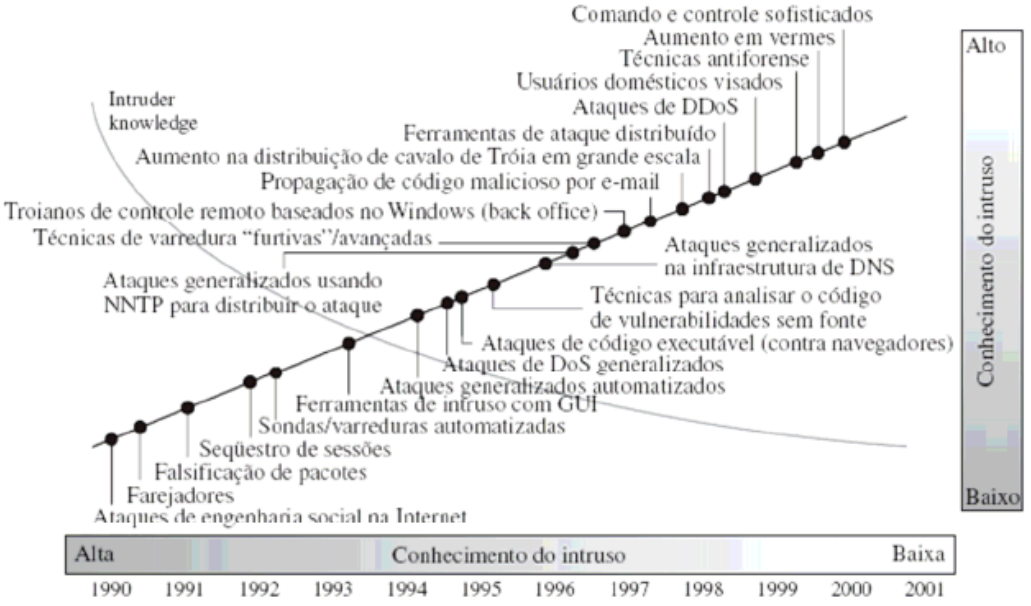

Figura 2.3: Sofisticação do ataques sobre o conhecimento exigido - *CERT*

É claro que o aumento dos ataques e suas complexidades não se deve apenas à automatização, fatores como o aumento da utilização da própria INTERNET[58] e da complexidade das aplicações são relevantes para este aumento.

Toda a rede pode, a qualquer momento, sofrer um ataque, seja através de equipamentos que estão prestando serviços pela INTERNET, ou dos equipamentos localizados na própria rede local da organização.

2.3.1 Ataques passivos

Esse tipo de ataque basicamente trata de espionagem e monitoração das comunicações[56], procurando obter informações através do vazamento de informações

como uma conversa telefônica, transferências de arquivos, envio de *e-mails* ou outras maneiras, por esse motivo é importante ter planejamento para impedir que essas informações sejam interceptadas e, caso sejam, que tenham sua confidencialidade garantida.

O ataque baseado na monitoração é bem sutil, no entanto existem ferramentas que tentam encontrar equipamentos que estão nessa situação, interceptando o tráfego e armazenando para futura análise. Mesmo o tráfego criptografado, neste caso, pode ser útil para encontrar padrões de utilização de *hosts* e faixas de *ip*.

Ataques passivos são bem difíceis de detectar (não impossíveis), pois não envolve diretamente a alteração do tráfego. Toda a comunicação autêntica ocorre, nem o emissor, nem o receptor percebem alguma diferença em suas comunicações. Por isso a prevenção a esses ataques é a solução, não a detecção.

2.3.2 Ataques ativos

Os ataques ativos atuam diretamente no fluxo da informação, modificando ou criando os dados de quatro maneiras possíveis: falsificação, repetição, modificação e negação.

A falsificação envolve uma entidade que se passa por outra diferente. Por exemplo uma seqüência de autenticação pode ser capturada e posteriormente repetida procurando uma seqüência válida para autenticação, permitindo que um usuário sem acesso ou com acessos mínimos consiga efetuar uma escalada de privilégios.

O ataque por repetição basicamente atua capturando pacotes e retransmitindo procurando obter um acesso não autorizado.

Modificação de mensagens altera parte do conteúdo de uma mensagem, ou busca retardar ou reordenar as mensagens.

Ataques de negação de serviços (*DOS - Deny of services*) busca impedir a utilização de um serviço tornando-o indisponível, também é utilizado para impedir que um sistema armazene *logs* como trilha de auditoria, para então executar um ataque mais elaborado. Esse tipo de ataque tenta sobrecarregar o servidor de um determinado serviço de modo que comprometa seu desempenho.

2.4 Ambiente seguro

A segurança está diretamente relacionada à proteção das informações e dos ativos que tem valor para uma organização [10], no que diz respeito a possíveis riscos. Inclui-se nessa lista bens materiais e intelectuais.

O quer que possa causar uma falha no sistema, e resultar em perda, deve ser considerada uma ameaça, o que significa perda de dados ou de disponibilidade do sistema, no entanto, isso é apenas o início do problema, pois a quantidade de formas como essa ameaça pode ocorrer é bastante vasta, tornando o problema de segurança algo difícil de se tratar.

Para se ter segurança implementada, algo deve ser sacrificado, ou seja, na medida em que se aumenta a segurança, diminui-se a facilidade de manuseio de um sistema ou utilização de uma rede. É preciso planejar uma maneira de se garantir a previsão de um incidente, entender a relação entre os serviços de uma rede e as maneiras para serem acessados os serviços.

A primeira fase em um desenvolvimento de uma infra-estrutura segura não é apenas localizar onde investir o orçamento de segurança, nem tão pouco montar um diagrama de rede de onde estão localizados os servidores e como protegê-los. Antes de qualquer fase inicial deve-se ter em mente alguns tópicos do planejamento, sendo listados os que são mais relevantes:

- Quais são os ativos mais relevantes para o negócio;
- Qual a importância de cada um dos ativos;
- Quais as possíveis ameaças a que esses ativos estão sujeitos;
- Quais as vulnerabilidades existentes.

A proteção dos ativos busca reduzir os riscos por eles sofridos, identificando as ameaças e conhecendo suas vulnerabilidades, com medidas preventivas onde se deve buscar:

- Identificar o que se pretende proteger;
- Avaliar as principais fontes de risco às quais se está sujeito;
- Desenvolver processos eficientes para se eliminar esses riscos.

A segurança é um problema cada vez mais evidente e importante, como discutido no Capítulo 1, os ataques estão cada vez mais complexos no entanto exigem cada vez menos conhecimento dos atacantes, a quantidade de ataques está crescendo junto com a utilização da tecnologia cada vez mais acessível. Por esse motivo a busca por ambientes cada vez mais seguros é constante e deve se ter em mente que não existe segurança 100% confiável, sempre existirá uma falha, seja ela através de vulnerabilidades lógicas em *softwares* ou ameaças de pessoas insatisfeitas que tem acesso permitido ao sistema.

Capítulo 3

Normas e modelos de gestão de segurança da informação

Antes de se falar em normas e modelos para gestão de segurança é necessário falar sobre um termo que vem sendo discutido há pouco tempo, governança em *Tecnologia da Informação*. Esse termo busca englobar e centralizar todas as metodologias que uma empresa necessita para implantar um sistema de gestão em seu ambiente tecnológico, visando sua administração da forma mais eficiente possível.

Enquanto a Governança corporativa busca criar e descrever um processo de tomada de decisão a Governança em *TI* busca um paralelo entre o ambiente tecnológico e o corporativo, buscando subsidiar a área corporativa com informações para uma decisão mais acertada e rápida.

Outra área que surge em paralelo e busca complementar a Governança em *TI* para suprir diversas outras exigências é o *security governance* (Governança em segurança). Enquanto a *TI* busca subsidiar informações e disponibilizar sistemas, a Governança em segurança persegue a qualidade na segurança em relação a essa informação, sua disponibilidade, integridade e outros fatores considerados importantes a fim de resguardar não só a informação, mas também a imagem da corporação.

3.1 *ISO 17799 e BS 7799*

A norma *ABNT NBR ISO/IEC 17799* está atualmente na versão de agosto de 2005. Exclusivamente, é uma norma que trata de segurança da informação colocando em ênfase os tópicos:

- Tecnologia de Informação;

- Técnicas de Segurança;
- Gestão da segurança da informação.

Em 1987, o departamento de comércio e indústria do Reino Unido *(DTI)* criou um centro de segurança comercial que teve, entre suas atribuições, a tarefa de criar uma norma de segurança das informações para o Reino Unido. Desde 1989 vários documentos preliminares foram publicados por esse centro, até que, em 1995, surgiu a *British Standard 7799 (BS 7799)*, que foi disponibilizada em duas partes para consulta pública, a primeira em 1995 e a segunda em 1998.

- *BS 7799-1*: Planejada como um documento de referência de boas práticas de segurança.
- *BS 7799-2*: Proporciona uma base para criar e gerenciar a segurança da informação de sistemas.

No ano de 2000, após incorporar diversas sugestões e alterações, a *BS 7799* foi transformada em padrão internacional com sua publicação na forma da *ISO/IEC 17799:2000* [41]. Em setembro de 2001, a *ABNT* homologou a versão traduzida da norma, denominada *NBR ISO/IEC 17799*.

Portanto a *NBR ISO/IEC 17799* é a versão padronizada e aceita pela ISO *(International Standards Organization)* da norma britânica *BS 7799*, que é amplamente utilizada pela comunidade internacional para a gestão de segurança de informações.

Uma comissão de estudo especialmente constituída pela *ABNT* desenvolveu seu trabalho partindo da versão revisada da *ISO/IEC 17799* [1] .

A *ABNT NBR ISO/IEC 17799* é um código de prática de gestão de segurança da informação. Ela se aplica à segurança da informação em sentido amplo. Fornece os melhores procedimentos, diretrizes e princípios gerais de implementação, manutenção e gestão da segurança de dados em qualquer organização, produzindo e utilizando informação em qualquer formato.

A norma abrange diversos tópicos da segurança da informação, tendo controles e requerimentos que devem ser seguidos, buscando garantir a segurança da organização. A implementação da proposta da norma é um processo demorado e bastante trabalhoso, no entanto, a imagem de uma organização passa a ser clara e mostra à sociedade a preocupação crescente com a privacidade e segurança dos clientes e usuários dessa empresa. Por essa razão existe atualmente um grande número de empresas que buscam a certificação, aderindo à citada norma.

Segundo a norma *ISO 17799:2000*, segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de

[1] Information technology-Security techniques-Code of practice for information security management.

forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. Ainda conforme especifica a norma, a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade. As informações que são protegidas com a implantação da norma: os dados armazenados nos computadores; as informações transmitidas por meio de redes; as conversações telefônicas; as informações impressas ou escritas no papel; as informações enviadas por fax; e os dados armazenados em fitas, discos ou microfilmes.

A norma não abrange apenas a segurança lógica, existem diversos aspectos que devem ser observados e são previstos pela segurança da informação, como a segurança física e em pessoas. Desta forma, variações de temperatura e da umidade do ar e quedas de energia elétrica são consideradas ameaças à informação. No ambiente de segurança em pessoas, pode-se citar fraudes, erros propositais ou não, sabotagens, roubo de informação. Outros aspectos são observados, como exigências contratuais com empresas terceirizadas.

Com o advento da terceirização, a área de segurança passou a ter mais preocupações, pois não deve apenas ter a visão da organização internamente, a própria terceirizada deve fazer o seu papel e se adequar ao plano de segurança da empresa, por isso existem acordos de nível de serviço que acabam implicando em atividades no tempo, modo de atuação e na qualidade da prestação dos serviços pela contratada, sob pena de severas multas.

Diante do exposto, especialistas no assunto sugerem a utilização das melhores prática do mercado. Neste sentido, podem ser utilizados como exemplo o *Control Objectives for Information and related Technology (COBIT)*, discutido no subtítulo 3.4, e a *NBR ISO IEC 17799* - Código de prática para a gestão da segurança da informação, que é composta de requerimentos a serem seguidos, enquanto a *ISO 17799* é um código de boas práticas *(Best pratics)*.

O *COBIT* é um conjunto de controles editado pela *ISACA (Information Systems Audit and Control Association)* que possui escritório no Brasil, na cidade de São Paulo. Atualmente o *COBIT* está na versão 4.1 e toda a documentação necessária para aplicação e utilização da metodologia pode ser obtida através do endereço `http://www.isaca.org/`. É bastante utilizado por empresas americanas, e vem crescendo no mercado brasileiro como framework de melhores práticas. Por outro lado, a *NBR ISO IEC 17799* é a norma emitida pela *ABNT*, que teve como base o resultado de um esforço conjunto de diversas empresas européias, que em 1987, começaram a elaborar um documento que servisse de orientação neste sentido, com critérios internacionalmente aceitos.

A norma vem ganhando espaço e já é considerada um padrão de segurança da informação. Segundo pesquisas recentes publicada pela empresa *Módulo Security*[2], 63,5% das maiores empresas brasileiras já utiliza a *ISO 17799*.

[2]http://www.modulo.com.br/

A utilização de controles buscando criar ou mesmo alterar um sistema de gestão da segurança, como políticas de segurança, melhores práticas, utilização de software e hardware, permite às empresas uma maior padronização de suas atividades, conseqüente monitoração de incidentes de segurança, com isso diminuem-se os impactos e seus riscos são mitigados.

Muitas empresas encaram o investimento em segurança como sendo prejuízo, pois não vêem retorno sobre o investido. No entanto, as empresas preocupadas com uma maior transparência e melhor atendimento e gerência de seu processo de negócio, logo perceberam um ganho expressivo em produtividade e qualidade, pois o conhecimento do próprio negócio passa a ser de suma importância para uma melhor competitividade.

Existe uma certificação para a norma *BS 7799*, no mundo todo existem em torno de 900 empresas certificadas, no Brasil existem apenas quatro: Serasa, Banco Matone, Samarco e Módulo Security. A norma *BS 7799* tem escopos bem definidos para a segurança da informação.

A idéia é criar um código de práticas de segurança no intuito de elaborar um Sistema de Gestão da Segurança da Informação (SGSI) nas empresas, onde a *BS 7799-1* de 2000 é o código propriamente dito onde as práticas visam à preservação da segurança da informação nas organizações.

A norma *BS 7799-2* de 2002 é um guia para a criação e manutenção de um SGSI (Sistema de Gestão da Segurança da Informação) seguindo o padrão *BS 7799-1*. É dividida em 16 capítulos, colocando os itens de maneira geral onde as sugestões devem ser implantadas de acordo com o ambiente e infra-estrutura:

1. Introdução / Definição de termos;
2. Objetivo;
3. Termos e definições;
4. Estrutura da Norma;
5. Análise/avaliação e tratamento de riscos;
6. Política de segurança da informação;
7. Organizando a segurança da informação;
8. Gestão de ativos;
9. Segurança em recursos humanos;
10. Segurança física e do ambiente;
11. Gerenciamento das operações e comunicações;
12. Controle de acessos;

13. Aquisição, desenvolvimento e manutenção de sistemas de informação;
14. Gestão de incidentes de segurança da informação;
15. Gestão da continuidade do negócio;
16. Conformidade.

Portanto a norma recomenda que os riscos sejam avaliados e tratados, assim como seja implantado um sistema para gestão dos ativos da organização.

3.2 *ISO / IEC 27001*

Em conseqüência da utilização da norma *BS 7799-2* surgiu a norma *ISO/IEC 27001* de 2005, com uma errata de 2006, amplamente divulgada e reconhecida pelo mercado como principal padrão que busca a criação e manutenção de um sistema de gestão da Segurança da Informação. Atualmente, este é um dos certificados mais buscados por empresas que identificam na confiança de seus clientes e parceiros, vantagens competitivas.

A Segurança da Informação atua com o processo conhecido como *PDCA (Plan-Do-Check-Action)* (Planejar-Fazer-Verificar-Agir), ver Figura 3.1, que requer gestão e controle sobre o que se quer administrar.

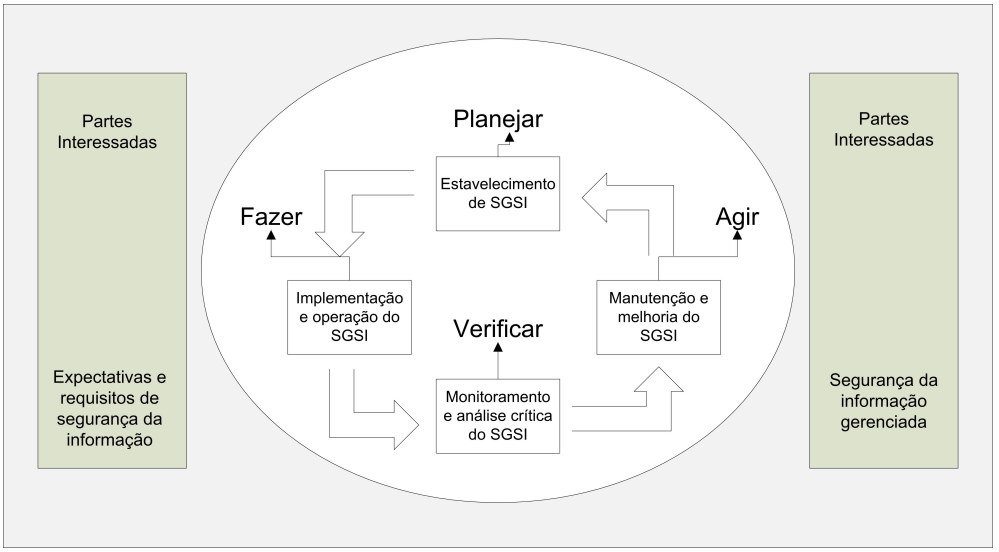

Figura 3.1: Processo de segurança

Em Planejar a organização tem como base criar política do *SGSI*, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação para entregar resultados conforme as políticas globais de uma organização e objetivos.

Possuir a certificação *ISO 27001* significa atuar sistematicamente nesta gestão através do gerenciamento dos riscos de segurança da informação que podem prejudicar o seu negócio.

A norma estabelece uma definição geral sobre os processos necessários para o gerenciamento da segurança, destacando no fator gerenciamento de risco as responsabilidades dentro da empresa e a implementação de controles visando o conhecimento tecnológico e procedimentos e processos de auditoria constantes para melhora contínua da qualidade. Também é estabelecido que a gestão do risco inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco.

Após implantar um Sistema de Gestão da Segurança da Informação, a empresa estará preparada para agir pró-ativamente, antecipando riscos, planejando e implementando soluções, medindo resultados e melhorando continuamente a segurança, um de seus principais patrimônios - a informação.

A norma *ISO 27001* tem dentre outras recomendações a implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização. É recomendado criar ou definir uma estratégia de avaliação de risco da organização, identificando uma metodologia de avaliação de risco adequada ao *SGSI*.

3.3 *SOX - Sarbanes Oxley*

Foi nos Estados Unidos, em 2002, que surgiu o ato da legislação federal denominado The *U.S. Public Company Accounting Reform and Investor Protection*, mais conhecido como *Sarbanes-Oxley Act*, sua principal base é o esforço para melhoria do gerenciamento corporativo e da qualidade da auditoria, que faz parte da Governança corporativa.

Nesta lei, foram criados parâmetros para um maior controle das companhias de capital aberto e suas subsidiárias em que suas ações são negociadas nas Bolsas de *New York* e *Nasdaq*, que porventura incluíram diversas empresas estrangeiras que negociam papéis e valores nos Estados Unidos. A partir do momento em que a lei foi promulgada, o que era apenas uma recomendação passou a ser obrigação, exigindo uma boa Governança e maior ética nos negócios de empresas com participação no mercado imobiliário, buscando reparar devido à perda da confiança pública nos governantes empresariais norte-americanos e enfatizando uma maior clareza nas informações prestadas aos investidores americanos, procurando utilizar padrões éticos na divulgação dessas informações.

A *Sarbanes-Oxley* contém 11 títulos e possui 1.107 seções, procurando imputar responsabilidades aos diretores de corporações, que podem ser de pagamento de multas, podendo chegar a alguns milhões de dólares e à condenação de prisão em regime fechado, bem como punição aos auditores que legitimarem os balanços das

empresas de forma fraudulenta.

Ao controlar as atividades de auditoria e contabilidade das empresas de capital aberto, acaba por afetar diretamente em seus dispositivos nos sistemas de tecnologia da informação, possibilitando separar os processos de negócios e a tecnologia no ambiente empresarial.

Na seção 404 são tratados os processos de tecnologia que trazem os mandamentos sobre os controles necessários para os processos internos e seus sistemas contábeis, determinando uma avaliação anual desses processos e obrigando a criação de relatórios financeiros a serem encaminhados aos órgãos fiscalizadores, que deverão confirmar ou não as informações desse relatório.

O relatório é um item muito importante a ser abordado, deve ser claro e direto, existindo alguns itens obrigatórios:

- Confirmação de responsabilidades dos gestores da empresa;
- Informações sobre a manutenção da base dos controles internos e outros procedimentos;
- Avaliação sobre o acordo de cumprimento de metas, ao final de cada exercício contábil;
- Verificação da eficiência dos procedimentos internos para emissão dos relatórios;
- Declaração de um auditor independente atestando sobre a avaliação dos procedimentos elaborada pelos gestores.

O ato *Sarbanes-Oxley* obriga a se utilizar de práticas de segurança de redes e métodos rígidos para um maior controle e conhecimento de infra-estrutura que tem alcance da lei, deve-se ter controles para diversas situações como:

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

Para a área de *TI*, o *SOX* acaba por afetar e interferir em toda a cadeia da informação e comunicação da empresa. Alguns recursos no entanto devem ter um impacto maior, que é o caso dos sistemas financeiros e contábeis, sistemas de relacionamento, gerenciamento de logística e um conjunto de sistemas de comunicação e armazenamento das informações. Esses sistemas devem estar de acordo com o que é requerido pela *SOX*.

O administrador de *TI* deve ter uma grande atenção aos recursos tecnológicos quanto da utilização pelos funcionários e de suas políticas de segurança utilizadas na empresa, devendo existir uma adaptação da política ao ato *Sarbanes-Oxley*, com uma especial atenção aos serviços terceirizados, pois a empresa passa a ser responsável por toda a cadeia do negócio, mesmo os terceirizados, portanto deve constar na política de segurança cláusulas que tratam esse assunto.

O ato *Sarbanes Oxley* requer uma conformidade contínua, ou seja, não é um certificação ou conformidade única. A conformidade deve ser feita trimestralmente e instituições que não atendam à conformidade, não apenas a *SOX*, mas todas relacionadas à segurança, estão sujeitas a:

- Maior exposição à fraude;
- Publicidade desfavorável;
- Impacto negativo;
- Ações judiciais.

As imposições não devem ser vistas apenas como uma burocracia a mais a ser atendida e executada, deve-se aproveitar a oportunidade e implementar uma política de melhores práticas de segurança que acabam por impactar todas as áreas subseqüentes, tornando a empresa ágil e bastante competitiva, pois a qualidade e transparência torna-se um atrativo não apenas para clientes, mas também para investidores.

A certificação *SOX* depende fortemente de uma política de gestão de risco, pois torna a organização totalmente gerenciada, onde seus riscos são mapeados e a eles é dado um valor, permitindo a criação de estratégia para controle desses riscos, com isso a organização passa a ser transparente e apta a operar no mercado Americano.

3.4 *COBIT - Control Objectives for Information and related Technology*

O *COBIT* foi criado em 1994 pela *ISACF - Information Systems Audit and Control Foundation*, que posteriormente passou a se chamar *It Governance Institute*,

partindo de um conjunto de objetos de controle e que foi evoluindo através de padrões internacionais e cooperação técnica em *TI*[15].

O modelo evoluiu bastante procurando se alinhar a modelos como o *COSO (Committee of Sponsoring Organizations of the Treadway Commission)*[29] Comitê das Organizações patrocinadas, *ITIL* (discutido no capítulo 3.5) e *ISO 17799* (abordado no capítulo 3.1).

Uma definição simples para o *COBIT*: é uma estrutura de relações e processos para dirigir e controlar o ambiente de *TI*[28], orientando-a às metas da organização e oferecendo métricas estruturadas com base no *BSC* (*Balanced Scorecard*) em suas quatro perspectivas:

1. Financeira;
2. Clientes;
3. Processos;
4. Inovação/Aprendizado.

Além da Auditoria de Sistemas, o *COBIT* é muito utilizado para a Governança de *TI*, seguindo padrões para um ambiente globalizado.

O objetivo das práticas propostas pelo *COBIT* é prover controle buscando o sucesso na entrega de produtos providos pela *TI*, simplesmente pela perspectiva do negócio, tendo o seu foco voltado para controle e não na execução, por esse motivo o *COBIT* deve prover:

- Relacionamentos com os requisitos do negócio;
- Organização das atividades de *TI* seguindo um modelo de processos;
- Identificação dos principais recursos de *TI*, possibilitando um maior controle e gestão desses recursos;
- Preparação dos objetivos de controle que deverão ser utilizados na gestão.

O modelo é genérico e permite representar os processos comumente encontrados nos serviços de *TI*, sendo entendido tanto para os operadores, quanto para os gerentes de negócio, permitindo a visão de executar (operação) e a visão de governar (gestores).

Outra vertente para a utilização do *COBIT* é o *security governance* (Governança em segurança), com a crescente demanda por segurança e conseqüentemente exigência por parte de administradores e gestores de empresas, acaba por surgir este novo termo que vem sendo amplamente utilizado para se definir a gestão de segurança em *TI*, e que envolve bem mais que apenas a utilização de

uma norma de segurança como a *ISO 27001*, passando a exigir muito mais que isso, sugerindo controles e métodos de identificação de ativos e seus respectivos inventários.

3.4.1 Cronologia de evolução do *COBIT*

- 1994: Primeira versão elaborada pela *ISACF*;
- 1998: Segunda versão, incluindo documentação de alto nível, controles, objetivos detalhados e criação do conjunto de ferramentas e padrões para implementação;
- 2000: Terceira versão publicada pelo *ITGI - It Governance Institute*, com objetivos voltados a Governança de *TI*;
- 2005: Quarta versão, maior integração com normas, regulamentações e *compliance* como *Basiléia II* e *Sarbanes-Oxley*.
- 2007: Versão 4.1 disponível gratuitamente pelo *ITGI*, inclui orientações sobre análise de desempenho, diretrizes de desempenho e métodos para se medir os resultados da implantação.

3.4.2 *COBIT* 4.1

A Governança de *TI* tem ganhado muita importância, pois ilustra a responsabilidade da alta direção nas estruturas organizacionais e nos processos em que a *TI* suporta a organização, sustentando os negócios e as estratégias da organização.

O *COBIT* 4.1 trata de Governança de *TI* em quatro dimensões, denominados Domínios:

1. Planejamento e Organização (*PO - Planning and Organization*): Contém uma visão estratégica para a Governança de *TI*, buscando uma melhor realização dos objetivos;
2. Aquisição e Implementação (*AI - Acquisition and Implementation*): Qualifica tanto a identificação de soluções a serem desenvolvidas e/ou adquiridas como a implementação e integração ao ambiente, assegurando que o ciclo de vida destas soluções é adequado ao ambiente organizacional;
3. Entregas e Suporte (*DS - Delivery and Support*): Domínio responsável em verificar o tratamento de serviços demandados pelos processos de negócios, recursos para a continuidade operacional, o treinamento e a segurança das operações. É neste domínio que se assegura a entrega de informações através do processamento de dados dos sistemas aplicativos, bem como todo o suporte necessário para sua operação inadequada ou em situações estranhas;

4. Monitoração (*M - monitoring*): Administra o processo de controles da organização de *TI* e a garantia de independência nas auditorias existentes. É fundamental para avaliar contínua e regularmente a qualidade e a conformidade dos controles implantados.

Nesses quatro domínios existem, de forma detalhada, 34 processos de controles de alto nível e para estes processos foram criados 318 objetivos de controles necessários para analisar e atender aos requisitos de *TI* e, conseqüentemente, aos objetivos do negócio.

Como resultado de avaliação desses objetivos, criam-se as estratégias para mitigação de riscos existentes, baseados nos resultados obtidos. Para cada um dos 34 processos, o *COBIT* contempla os fatores críticos de sucesso e determina os indicadores de resultados *(KGI) (key goal indicator)* indicador das metas principais) e de desempenho *(KPI) (key performance indicator)* indicador dos desempenhos principais), que geram as métricas para a avaliação da Governança de *TI*, para diretrizes de auditoria e para a segurança da informação.

O *COBIT* apresenta um modelo para atestar a maturidade de cada processo em uma escala de seis estágios possíveis, sendo eles:

0 - Não existe;

1 - Inicial;

2 - Repetível e intuitivo;

3 - Processos definidos;

4 - Gerenciados;

5 - Processos otimizados.

3.4.3 Utilizando o *COBIT* em segurança da informação

Para o *Security Officer*, o *COBIT* é utilizado como um modelo para um programa de segurança da informação, integrando segurança com os objetivos de *TI* relacionados aos negócios e também estruturando políticas, normas e procedimentos de segurança da informação.

Nos processos, existem objetivos focados para *SI*, tais como:

- DS5: Garantir a segurança dos sistemas;
- PO9:Avaliar e gerenciar riscos de *TI*;
- DS3: Gerência de performance e capacidade;

- DS7:Treinamentos a usuários;
- DS10: Gerência de problemas e incidentes;
- DS12: Gerência de ambientes (Segurança física).

A estratégia do *COBIT* faz com que ele assuma diversas funções dentro da organização:

- Uma ferramenta: para a Governança de *TI*;
- Aderência da *TI* ao negócio: Requisições orientadas e fundamentadas das áreas-fim da organização, atendendo aos objetivos estratégicos;
- Garantia de qualidade: Integração e maior detalhamento buscando interagir com os padrões e práticas de mercado, como:*ITIL, ISO 17799, PMBOK (Project Management Body of Knowledge) e PRINCE2 (Projects in Controlled Environments)*;
- Gestão de risco: Controles objetivos e detalhados;
- Governança corporativa: Habilita e facilita a arquitetura empresarial;
- Procedural: Definição de fluxos e processos de *TI*;
- Comunicação: Unifica a linguagem e divulga os processos de *TI*, em todos os níveis da organização;
- *Feedback*: Estimula os comentários, sugestões e recomendações para um ciclo evolutivo.

O *COBIT* pode ser utilizado na implementação de controles para a Governança de *TI*, que é diretamente ligado a segurança da informação, pois a melhoria desses controles traz ganhos em produtividade e transparências com a definição dos objetivos a serem implementados.

Dessa maneira o *COBIT* interage entre as áreas de gestão de riscos, gestão de serviços em *TI* (*ITIL*) e gestão da segurança da informação.

Esses modelos incluem, para cada área, recomendações de boas práticas permitindo alinhar os objetivos às estratégias de Governança garantindo que as áreas de uma organização interajam e que os processos e atividades alcancem os objetivos do negócio com isso reduzindo os riscos operacionais.

Esta proposta não é a de implantar o COBIT em uma organização, e sim instruir sua utilização em conjunto com a metodologia de gestão de risco, subsidiando as informações coletadas pela metodologia a serem utilizadas em um *framework* mais geral de Governança.

3.5 *ITIL - Information Technology Infrastructure Library*

O *ITIL* foi desenvolvido na Inglaterra no final dos anos 80 pela *CCTA (Central Computer and Telecomunications Agency)*, no início era composto por mais de 30 livros sendo 10 processos chaves que buscavam a melhoria das operações das organizações, aprimorando os níveis de serviços e diminuindo os custos com a perda de tempo e trabalhos repetitivos.

Em termos gerais o *ITIL* é um conjunto de padrões que disponibiliza os fundamentos para o gerenciamento dos recursos e processos de *TI*. Possui uma abordagem prática dos processos que envolvem a produção e entrega dos serviços de *TI*. No entanto, seu foco principal é no serviço que a tecnologia da informação presta para a organização, sempre buscando o aumento da qualidade desses serviços.

O *ITIL* é dividido em 10 processos principais e quatro processos de apoio que são chamados de processos satélites. Os processos principais são agrupados em dois grupos:

Grupo de suporte aos serviços *(Service support set)*:

- Gestão de configuração e de ativos;
- Controle de incidentes / *helpdesk*;
- Gestão de problemas;
- Gestão de mudanças;
- Gestão de liberação.

Grupo de Serviços prestados *(Service delivery set)*:

- Gestão de níveis de serviço (*SLA - service level agreement*);
- Gestão de disponibilidade;
- Gestão de desempenho e capacidade;
- Plano de continuidade de negócios;
- Custeio e gestão financeira.

Os processos de apoio são:

- *SLA*;

- Segurança;
- Informação;
- Rede e operações.

Na gestão de segurança, o *ITIL* possui um processo específico, colocando como pilar a importância do plano de gerenciamento da segurança da informação e considerando os contratos de níveis de serviços como o processo do negócio e os da *TI*. Também recomenda que o correto gerenciamento da segurança deve fazer parte do trabalho da gerência em todos os níveis.

3.5.1 Utilizando o *ITIL* em segurança da informação

Como itens fundamentais para a segurança, o *ITIL* recomenda fortemente alguns procedimentos que possibilitam essa evolução:

- Catálogo de serviços: A equipe de *TI* deve disponibilizar informações descrevendo os serviços por ela executados e em que condições são executados bem como qual parte do negócio requer este serviço;
- *OLA's (Operational Level Agreement)*: Internamente deve existir um acordo para prestação de serviços, visto como um *SLA* mais enxuto, mas devendo prever quase que totalmente as condições para entrega do serviço, incluindo os custos;
- *UC's Underpinning Contracts*: São contratos de prestação de serviços por empresa externa, devendo ser previstas as condições e penalidades sofridas em casos como penalidades, condições de saída, bônus, entre outras;
- Base de dados dos ativos que fazem parte da empresa, bem como todas as configurações atualizadas, incluindo *software* e *hardware*, bem como toda a documentação atualizada, procedimentos de execução e a devida classificação do ativo em relação à segurança, conforme descrito no Capítulo 2;
- *Service Desk*: Criação de ponto central para contato com todos os usuários de *TI*, sendo esta área gestora de todos os incidentes (inclusive os de segurança) e com o foco geral em continuidade dos serviços e gerenciamento dos contratos de *SLA*;
- Gestão de problemas: Para se resolver um problema deve se conhecer esse problema, por este motivo a gestão de um incidente deve ser aplicada, devendo aprender com os incidentes, definindo a relação e suas causas e quais procedimentos adotados para evitá-los. Com essa ação busca-se conhecer as vulnerabilidades de segurança documentando todas as ações, desde como o

incidente foi descoberto, qual procedimento adotado para sua solução e determinando um procedimento para acompanhamento do problema, mesmo depois de ter sido resolvido;

- Gestão de mudanças: Centraliza todas as mudanças no ambiente de *TI*, utiliza fortemente a base de conhecimentos adquiridos através da gestão de problemas, buscando apoiar-se na documentação dos incidentes;

O *ITIL*, assim como o *COBIT*, recomenda criar uma base de conhecimento, relacionando os ativos que fazem parte da infra-estrutura de uma organização, devendo criar procedimentos para classificação dos ativos, assim como uma relação de *hardware* e *software* considerada importante para a organização.

Recomenda-se a utilização do *ITIL* como plataforma de gestão corporativa, sendo que a gestão de risco não depende totalmente do *ITIL*, mas sua implementação dá subsídio para um controle mais eficiente do ambiente organizacional.

3.6 Integração entre os modelos *COBIT*, *ITIL* e Segurança da informação com as normas *BS-7799, ISO 17799 e ISO 27001*

A integração entre modelos de gestão de *TI*, como o *COBIT*, e serviços em *TI* como o *ITIL* aplicado com foco em segurança da informação que possui os objetivos de controle detalhados para gerenciamento de segurança.

Os objetivos de controle relacionados às melhores práticas para segurança deverão ser identificados no modelo *COBIT*. A avaliação em níveis de maturidade do *COBIT* para cada objetivo de controle se integrará com as normas de segurança como ISO 17799 e ISO 27001 que possuem a capacidade de obtenção de um processo contínuo de melhoria da qualidade da segurança.

Os objetivos propostos pelo *COBIT* deverão ser mapeados e atribuídos um valor, conforme recomendado pelas normas de segurança aqui tratadas. Por esse motivo um mapeamento completo da infra-estrutura de *TI* da organização é tão importante.

O modelo macro da integração é mostrado na tabela 3.1, onde é proposta a infra-estrutura para criação de controles e recomendações para criação de um sistema de gestão de risco.

Tabela 3.1: Integração entre os modelos *COBIT*, *ITIL* e normas de segurança da informação

	Operacional	**Tático**	**Estratégico**
Controles	ISO 17799, COBIT: Entrega e suporte. Aquisição e implementação	ISO 17799, COBIT: Entrega e suporte	ISO 17799, Análise de risco, COBIT: Auditoria, monitoramento, planejamento e organização
Pessoas	ITIL: Suporte a Serviços	ITIL: Entrega de Serviços	COBIT: Auditoria e Monitoramento
Processos	ITIL: Suporte a Serviços	ITIL: Entrega de Serviços	COBIT: Auditoria e Monitoramento
Tecnologia	Ferramentas de Gerenciamento (inventário)	Ferramentas de Gerenciamento (inventário), Ferramentas para testes de vulnerabilidade, Ferramentas para análise de logs	Ferramentas automatizadas para análise de Risco. Ferramentas automatizadas para a extração de conhecimento.

O relacionamento entre modelos *COBIT* e *ITIL* e a norma de segurança utilizados em um modelo de Governança com foco em segurança [7] é mostrado na tabela 3.2, onde os objetivos de controle do modelo *COBIT* são correlacionados com as normas de segurança, e além disso, são mostrados os objetivos de controle em referência ao *ITIL*.

Tabela 3.2: Relacionamento entre os modelos *ITIL* e *COBIT* e a normas de segurança para gestão de risco

Nível	**Objetivos de Controle do COBIT**	**Referência *ISO 17799***	**Referência *ITIL***
Estratégico	**PO - Planejamento e Organização**		
	PO1-Definir um Plano Estratégico de *TI*	Cap. 6.1	
	PO2-Definir a Arquitetura da Informação	Cap. 6.1.2	
	PO3-Determinar a Direção Tecnológica	Cap. 5	
	PO9-Avaliar e gerenciar riscos de *TI*	Cap. 4.1 e 6.2	
Operacional e Tático	**AI - Aquisição e Implementação**		
	AI1-Identificar Soluções Automatizadas	Cap. 6.1.4	X
	AI2-Adquirir e Manter Software Aplicativo	Cap. 12	X
	AI3-Adquirir e Manter a Infra-estrutura Tecnológica	Cap. 14.1.4	X
	AI4-Desenvolver e Manter Procedimentos	Cap. 5	X
	DS - Entrega e Suporte		
	DS3: Gerência de performance e capacidade; DS4-Garantir Continuidade dos Serviços	Cap. 14	X
	DS5-Garantir Segurança dos Sistemas	Cap. 10.8.5	X
	DS7-Treinamentos a usuários	Cap. 8.2.2	X
	DS10-Gerenciar de problemas e Incidentes	Cap. 13	X
	DS11-Gerenciar Dados	Cap. 15.1.4	X
	DS12-Gerência de ambientes (Segurança física)	Cap. 9	X
Estratégico	**M-Monitoramento**		
	M1-Monitorar os Processos	Cap. 10.10	
	M2-Avaliar a Adequação do Controle Interno	Cap. 12.2.2	
	M3-Obter certificação Independente	Cap. 10.3.2	
	M4-Providenciar Auditoria Independente	Cap 10.10.1	

Este modelo não contempla todos os controles, pois o foco é a criação de infra-estrutura para uma gestão de risco.

Capítulo 4

Gestão de Ativos

Segundo a norma *ABNT NBR ISO/IEC 17799* de 2005, o item gestão de ativos foca a responsabilidade pelos mesmos, ou seja, todos os ativos da organização devem ser identificados e atribuídas responsabilidades sobre a sua manutenção baseada em controles.

É conveniente que os ativos identificados sejam documentados e a eles atribuídos uma grande importância.

Para uma gestão de risco mais eficiente, deve-se partir do princípio de que se conhece toda a infra-estrutura tecnológica. Existem diversas maneiras conhecidas para se obter essa informação:

- Através de pesquisas manuais de descoberta na rede;
- Utilizando-se de entrevistas com responsáveis diretos pela infra-estrutura;
- Visitando todos os pontos de conexão;
- Catalogando por inventário todos os componentes da rede;
- Automatizando o processo de identificação e inventário.

O processo de gestão de risco é continuo e deve ser sempre reavaliado em busca de inconsistências. Pode-se dividir o processo de condução de uma análise de risco em seis partes (Figura 4.1):

1. Planejamento e estratégia: planejar ações e criar estratégias de avaliação
2. Identificação: criar procedimentos para uma correta identificação dos riscos;
3. Qualificação: introduzir uma qualificação decorrente de uma vulnerabilidade;
4. Quantificação: possibilitar uma pontuação do nível de risco;

5. Impactos e respostas: criar procedimentos para se determinar o impacto sujeito e qual resposta deverá ser utilizada;

6. Monitoramento e Controle: determinar procedimentos para um constante acompanhamento para ações.

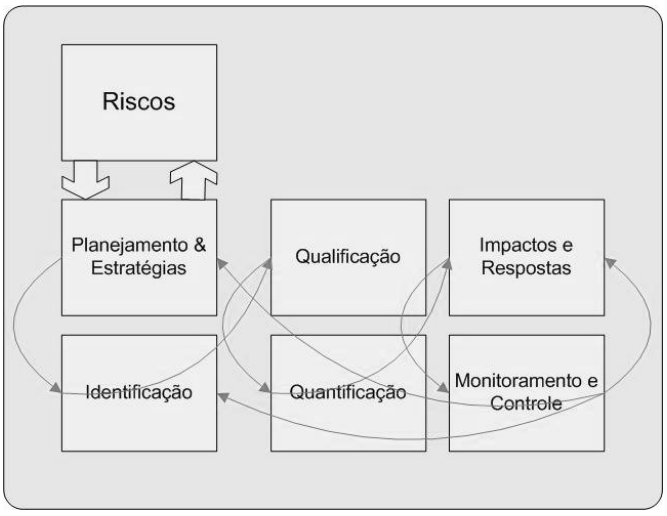

Figura 4.1: Processos Gestão de Riscos [54]

Desses pontos aqui descritos pode-se ter uma idéia que mesmo em redes de pequeno/médio porte (até 1000 máquinas) seria viável efetuar um dos itens acima. Infelizmente no momento que terminar de se coletar a última informação e conseqüentemente iniciar o processo de cálculo de risco, toda a análise estará baseada no passado, ou seja, a análise de risco não terá a mesma eficiência, e a cada minuto que se passa, menos eficiente estará. Com isso pode ocorrer uma falsa sensação de segurança.

4.1 Métodos para criação de inventário

Existem diversos métodos que podem ser utilizados para a criação da base de informações para inventário. Nesse capítulo são discutidos os métodos mais utilizados, considerando os pontos fortes e fracos de cada método.

4.1.1 Método Agressivo

O método agressivo é assim chamado pois utiliza como premissa o levantamento direto da informação, utilizando técnicas de teste de penetração para obter informações como:

- *IP* utilizado;

- Tipo do sistema operacional;
- Versões de softwares instalados;
- Serviços sendo executados;
- Usuários logados.

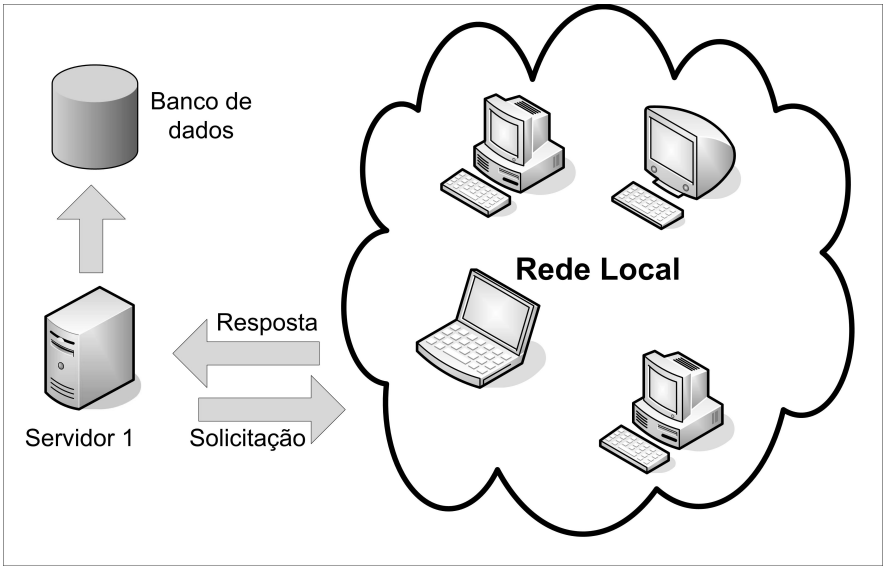

Figura 4.2: Método agressivo

Na Figura 4.2 o servidor 1 é responsável por executar as aplicações que irão obter as informações para o banco de dados do inventário. A comunicação inicia-se pelo servidor 1 em direção à rede, por esse motivo é de suma importância o conhecimento da infra-estrutura. Essa técnica deve ser executada com bastante cautela, para que os testes efetuados não prejudiquem a rede.

Essas informações podem não ser confiáveis, pois alguns sistemas respondem de maneira diferente que o usual e as ferramentas podem *entender* de maneira errada, comprometendo a base de dados a ser formada. Mas essas ferramentas não devem ser totalmente descartadas, pois, em conjunto com outros métodos que permitam confirmar os dados coletados, podem representar uma solução viável.

Algumas ferramentas que podem ser utilizadas para essa finalidade são:

- *NMAP*[1] *(Network Mapper)*: É uma ferramenta para levantamento de informações sobre portas e serviços a que estejam atendendo, comumente chamado de *portscan*, podendo também obter informações sobre qual sistema operacional a máquina alvo está operando, baseado em *fingerprints* nas respostas das solicitações enviadas;

[1]http://insecure.org/nmap/ (acessado em 20/04/2007)

- *NESSUS*[2] : Um *scanner* de vulnerabilidades que procura, baseado em um banco de dados, identificar e catalogar as vulnerabilidades encontradas. É uma ferramenta muito poderosa, sendo utilizada de maneira errada pode acarretar prejuízos maiores ainda, pois algumas verificações que o *nessus* faz podem acarretar em queda na parada do serviço na máquina alvo, ou mesmo a queda de toda a infra-estrutura de rede, devendo ser utilizada de maneira muito cuidadosa.

- *Wireshark*[3] O mais popular analisador de rede que existe, também conhecido como *sniffer*, verificando todo o tráfego que chega à interface e montando os pacotes para eventual análise, sua funcionalidade pode ser complexa, dependendo do nível de utilização. Infelizmente, sua atuação para coleta de informações pode não ser satisfatória, pois a grande quantidade de tráfego da rede pode dificultar o tratamento da informação obtida.

4.1.2 Método Passivo

A idéia desse método é aguardar que a informação a ser coletada chegue ao servidor, simplesmente analisando todos os pacotes da interface de rede. Esse método é muito demorado e também pouco confiável, pois trabalha basicamente com *fingerprints* e tratamento de pacotes *ip*, visando a identificação de informações simples como:

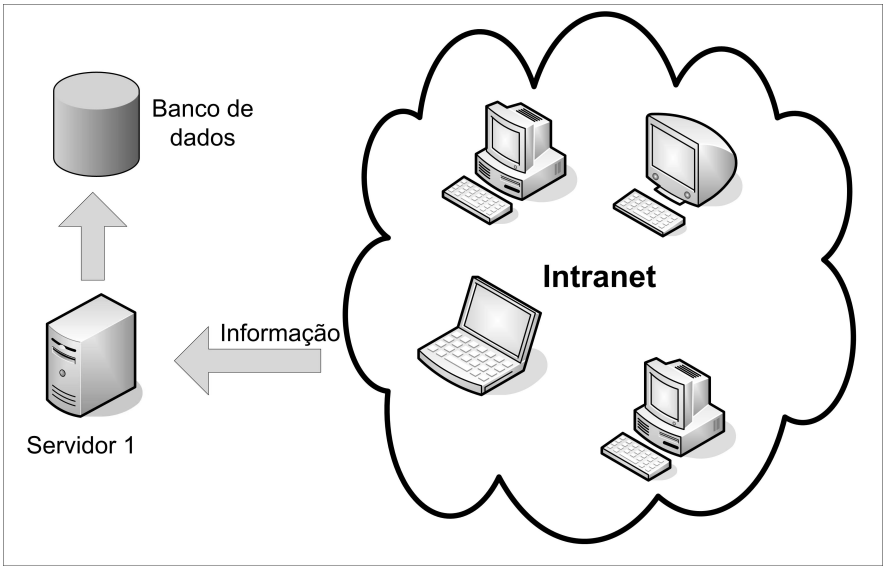

Figura 4.3: Método passivo

- Número de IP;

- Tipos de protocolos de rede;

[2]http://www.nessus.org/ (acessado em 20/04/2007)
[3]http://www.wireshark.org/ (acessado em 20/04/2007)

- Identificação de serviços;
- Identificação de sistemas operacionais (não confiável).

Conforme Figura 4.3, o servidor tem acesso apenas a *INTRANET*, pois o principio é não conhecer nada da rede, as informações devem chegar de maneira espontânea, portanto a maioria dos pacotes são *broadcasts*.

4.1.3 Requisitos para elaboração de inventário

A fim de automatizar a coleta de dados para inventário dos ativos a ferramenta deverá ter requisitos como:

- Possuir suporte característico cliente/servidor;
- Ter um banco de dados central, onde todas as informações serão armazenadas;
- Ser multi plataforma, de modo a poder ser executada em diversos sistemas operacionais;
- Ser gerenciável para que se possa solicitar informações a qualquer momento que se faça necessário;
- Consumir o mínimo de recursos necessários para o funcionamento do cliente;
- Ser capaz de informar, caso o cliente, por algum motivo, seja desabilitado;
- Poder ser reconfigurada a qualquer instante, de forma global, independente da vontade do usuário.

Desses requisitos iniciais, a ferramenta também deverá ser capaz de coletar diversas informações de inventário, sendo toda a informação enviada diretamente ao banco de dados central. Informações essenciais:

- Versão do sistema operacional corrente;
- Correções aplicadas e suas respectivas versões;
- Informações de usuários cadastrados e logados;
- Lista de softwares instalados e suas versões;
- Checagem de instalação de sistemas antivírus e suas atualizações;
- Informações sobre compartilhamentos;

- Informações de localização física do hardware (neste caso a informação deverá ser solicitada ao usuário);
- Lista de hardwares:
  - Quantidade de memória;
  - Tipo do processador;
  - Tamanho do disco rígido;
  - Placa de vídeo.

Após a coleta das informações para a geração de uma base de conhecimento da infra-estrutura de *TI* deve-se proceder à qualificação quanto a importância do ativo. Para tanto, um pequeno questionário pode ser adotado considerando cinco possibilidades:

1. Irrelevante
2. Relevante
3. Importante
4. Crítico
5. Vital

4.2 Ferramentas para gestão de ativos e inventário

A área que cuida da gestão de ativos não deve estar presa por métodos manuais, onde uma pessoa fica responsável por coletar informações manualmente indo de estação em estação. Esse método ficaria restrito apenas à localização de equipamentos físicos, não tendo informações como: *Hardware*, *softwares* e suas versões instalados, assim como controle de número de séries de *softwares* adquiridos, entre outros diversos fatores. É importante registrar que, no término da coleta das informações toda a base estaria ultrapassada, pois no intervalo entre a coleta, equipamentos novos poderiam ser instalados, *softwares* sendo atualizados e instalados, assim como *hardwares* terem sido atualizados.

Para uma efetiva gestão de ativos é necessário um controle automatizado ou mesmo semi-automatizado. Sem um controle efetivo do que existe em uma rede não é possível implementar uma Governança de *TI*, nem mesmo buscar qualquer conformidade seja ela *Sarbanes-Oxley*, *ISO* 27001 ou *ISO 17799*.

4.2.1 *CACIC*

O *CACIC* (Configurador Automático e Coletor de Informações Computacionais) é um software desenvolvido em conjunto com a Secretaria de Logística Tecnologia e Informações, do Ministério do Planejamento e a *DATAPREV* (Empresa de Tecnologia e Informações da Previdência Social) e liberado seu código fonte como sendo livre através da licença *GPL* (Licença pública geral). O funcionamento do sistema (Figura 4.4) é dado de acordo com um cliente com um agente instalado em um ambiente gerenciado, reportando ao módulo gerente e podendo ser efetuados comandos diretamente, como solicitação de informações por parte do gerente. O módulo gerente fica em um ambiente gerenciado pelo administrador e somente este pode reportar ao *webservice*, também chamado de super-gerente.

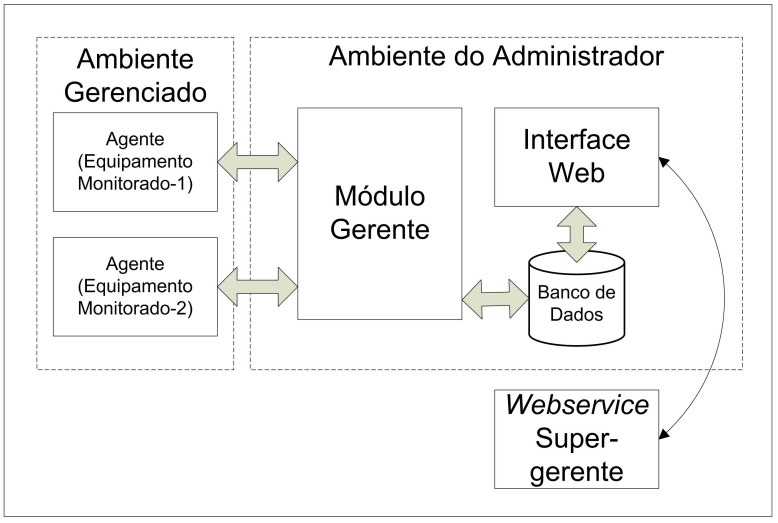

Figura 4.4: Arquitetura cliente/servidor do *CACIC*

Sua principal função é manter uma base de equipamentos e informações patrimoniais. No entanto diversas outras informações são disponibilizadas:

- Informações sobre os componentes de *hardware* instalados em cada equipamento e disponibilizá-las aos administradores de sistemas;
- Alertas, quando forem identificadas alterações na configuração dos componentes de hardware de cada computador;
- Diversas informações sobre os softwares instalados em cada computador;
- Identificar diretórios compartilhados;
- Informações de Patrimônio (*PIB*, localização, etc.) de cada equipamento;
- Alertas, quando forem identificadas alterações na localização física do computador;

4.2.1.1 Componentes do *CACIC*

A infra-estrutura do *CACIC* é composta por três componentes de operação:

1. Módulo Agente;
2. Módulo Gerente;
3. Módulo *WebService*.

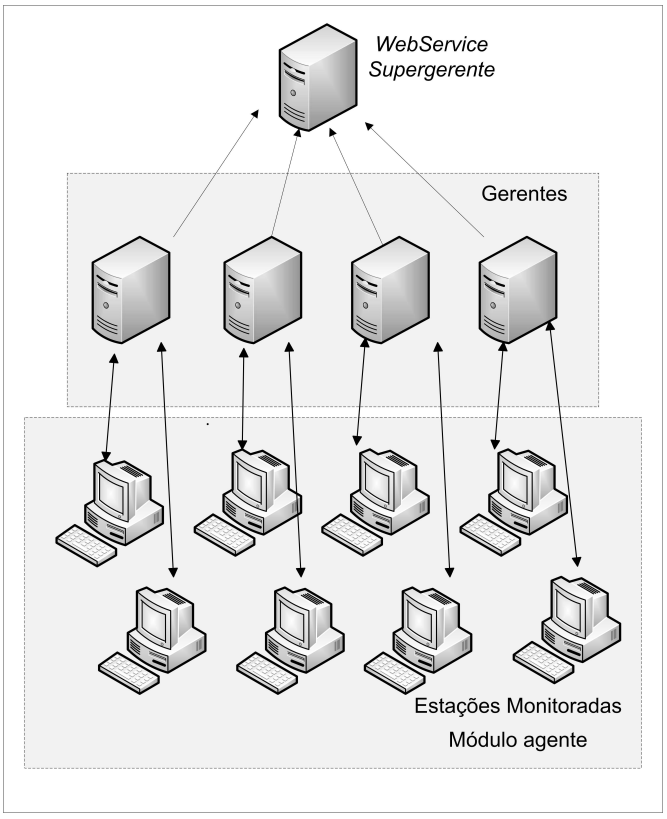

Figura 4.5: Diagrama de infra-estrutura do *CACIC*

4.2.1.2 Módulo Agente

O módulo agente (Figura 4.5) é responsável pelas estações monitoradas, basicamente é um software que deve estar instalado na estação ou servidor monitorado, coletando dados com a freqüência previamente definida na configuração inicial do agente, essa mesma configuração posteriormente pode ser modificada, dependendo apenas do módulo gerente. Pode-se definir quais informações são de interesse, sendo posteriormente enviadas para o gerente.

4.2.1.3 Módulo Gerente

O módulo Gerente trabalha com um conjunto de software que são instalados em um servidor, tudo integrado, permitindo a administração geral do sistema. O servidor deve conter a instalação conhecida como *LAMP* (*Linux-Apache-Mysql-PHP*), consiste de um sistema operacional baseado em *Linux*, com um servidor *Web* utilizando como software o *apache* e a linguagem de programação é o *PHP*.

A função do gerente é receber as informações coletadas pelos agentes, organizando e disponibilizando tais informações de maneira a facilitar as consultas. É esse módulo que permite a configuração de determinadas características e comportamentos dos agentes.

4.2.1.4 Módulo *Webservice*

Neste módulo encontra-se o super-gerente que é composto pelo mesmo conjunto de softwares do módulo gerente. No entanto, quem reporta as informações coletadas nesse caso é o gerente. Este sistema trabalhará de maneira a distribuir a uma infra-estrutura global a solução de coleta de informações. Pode-se ter uma visão global de toda a infra-estrutura.

4.2.2 *Tivoli* - Módulo gestão de ativos

O *tivoli* é um *software* de gerenciamento inteligente desenvolvido pela *IBM* que oferece diversas facilidades como:

- Gerenciamento de armazenamento: Gerencia e assegura a acessibilidade, disponibilidade e performance da informação armazenada;
- Segurança: É utilizado para proteger a confidencialidade, integridade, privacidade e a segurança dos sistemas;
- Gerenciamento de sistemas: É utilizado para monitorar, controlar e otimizar os recursos de computação;
- Gestão de ativos: Eficiência na gestão de ativos gerenciando todos os tipos de ativos em uma única plataforma.

O módulo gestão de ativos do *tivoli* foi construído com base em uma única plataforma de *software*, *Maximo Asset Management* [37], oferece uma visão abrangente de todos os tipos de ativos: produção, instalações, transporte e *TI*, em toda a organização, permitindo que se visualize todos os ativos, e identifique todo o potencial inexplorado dos mesmos.

O software *tivoli* é um aplicativo de gestão de ativos de *TI* que oferece suporte para controle de inventário, finanças, manutenção e contratos, permitindo acompanhar e gerenciar ativos de *TI* de maneira eficiente. Também ajuda a gerenciar compras, orçamentos e contratos de maneira mais eficaz. Permite controlar, de maneira pró-ativa, os esforços de cumprimento de licença de software, finanças e regulamentações. Identifica ativos subutilizados permitindo sua re-utilização e, muito importante, ajuda a controlar custos de *TI* e a se preparar com maior precisão para as necessidades futuras de *TI*.

Essa solução oferece uma visão bastante abrangente da infra-estrutura de *TI*, permite emissão de relatórios detalhados em uma interface de usuário de fácil configuração. No entanto, o custo da licença torna sua utilização para poucos. Outro ponto considerado contra é que se trata de software proprietário e com o seu código fonte fechado, a organização que escolhesse utilizar o *tivoli* ficaria dependente, caso necessitasse de uma alteração do programa por qualquer motivo.

Pelos motivos apresentados neste capítulo, a metodologia proposta pretende utilizar a solução de inventário proposta pelo *cacic*, que apesar de ser um *software* menos robusto que seu concorrente *tivoli* mostrou-se eficiente para este trabalho e que disponibiliza o código fonte para livre alteração seguindo o conceito de *software* livre pela licença *GPL* (licença pública geral).

Outra vantagem do *CACIC* é que permite um controle total por interface *web* e sua base de dados está totalmente disponível para estudo, permitindo maior facilidade de integração ao *framework*.

Capítulo 5

Gestão de Risco

A definição de risco pode ser feita de diversas formas, dependendo de qual situação o risco se aplica[35]. Então se pode definir risco como sendo a probabilidade de que uma situação física com potencial de causar danos possa acontecer, em qualquer nível, em decorrência da exposição, durante um determinado espaço de tempo, a uma vulnerabilidade.

O risco é considerado um evento incerto ou de data incerta que independe da vontade dos envolvidos, sendo um elemento de incerteza que pode afetar a atividade.

A gestão de risco está evidenciada na norma *ISO 27001* [40], de 2005, que trata em suas premissas básicas da implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais.

A norma *ISO 27001* [40] de 2005 também define a estratégia de avaliação de risco da organização, como:

- Identificar uma metodologia de avaliação de risco adequada ao *SGSI*, e aos requisitos de negócio, legais e regulatórios identificados para a segurança da informação;
- Desenvolver critérios para a aceitação de riscos e identificação dos níveis aceitáveis de risco. A metodologia de avaliação de risco selecionada deverá assegurar que as avaliações de risco produzam resultados comparáveis e reproduzíveis;

O gerenciamento de risco[4] mostra a importância de sua implementação, pois em continuação da norma *ISO 27001* [40], recomenda-se a identificação dos riscos:

- Os ativos dentro do escopo do *SGSI*, e os proprietários destes ativos;

- As ameaças para esses ativos;
- As vulnerabilidades que poderiam ser exploradas pelas ameaças;
- Os impactos de confidencialidade, integridade e disponibilidade.

Após a obtenção das informações referentes aos ativos é necessário analisar e avaliar os riscos:

- Avaliar o impacto para o negócio da organização que poderia resultar de uma falha de segurança, considerando as conseqüências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos;
- Avaliar a probabilidade realista, de como uma falha de segurança acontece à luz de ameaças e vulnerabilidades prevalecentes, e impactos associados a esses ativos, e aos controles implementados atualmente;
- Estimar os níveis de riscos;
- Determinar se o risco é aceitável ou requer tratamento que use o critério de aceitação de risco estabelecido.

O tratamento dos riscos busca a sua eliminação[31], no entanto, nem sempre isso é possível, por diversas razões[50], como: falta de correção, impacto sobre o produto tornando-o ineficiente, impacto negativo sobre o negócio, entre outros. Nesse caso deve-se identificar e avaliar as opções para o tratamento de riscos:

- Aplicar os controles apropriados;
- Aceitar os riscos conscientemente e objetivamente, provendo a satisfação clara às políticas da organização e aos critérios para aceitação de risco;
- Evitar riscos;
- Transferir os riscos de negócio associados a outras partes, por exemplo, corretores de seguro, provedores de serviço.

A fim de subsidiar este trabalho, em relação à proposta que é a de uma análise de risco constante e informado pelos ativos monitorados, a norma *ISO 27001* [40] propõe revisar as avaliações de risco a intervalos planejados e revisar o nível de risco residual e risco aceitável identificado, considerando mudanças de:

1. Organização;
2. Tecnologias;
3. Objetivos empresariais e processos;

4. Ameaças identificadas;
5. Efetividade dos controles implementados;
6. Eventos externos, como mudanças nos aspectos legais ou regulatórios, alterações das obrigações contratuais e mudanças no aspecto social.

5.1 Matriz de risco

Como o risco é um evento incerto, devem existir metodologias que, baseadas em informações coletadas, seja através de variáveis ou através de valores fixos, diminuam o impacto ou mesmo deixem de existir. Cálculos simples de risco podem ser feitos, como demonstrado pela Figura 5.1. Onde o risco pode ser medido através do produto entre as variáveis probabilidade, severidade e relevância, conforme Tabela 5.1.

$$Risco = (Probabilidade)(Severidade)(Relevancia) \tag{5.1}$$

O risco tem ocorrências incertas e através da tabela 5.2 é proposta uma classificação da probabilidade, com sua respectiva informação.

Tabela 5.1: Matriz de risco

Item	**Severidade**	**Probabilidade**	**Relevância**
1	Não disponível	Não disponível	Não disponível
2	Desprezível	Extremamente remota	Desprezível
3	Marginal	Remota	Menor
4	Crítica	Improvável	Moderada
5	Catastrófica	Provável	Séria

Não existe uma definição clara e objetiva sobre a freqüência e conseqüência do risco, isso por se tratar de um evento totalmente incerto, no entanto, a elaboração subjetiva de uma avaliação de risco pode mitigar ou mesmo extinguir o risco.

Tabela 5.2: Tabela de probabilidade de risco

Item	**Denominação**	**Descrição**
1	Extremamente remota	Ocorrência possível, mas improvável
2	Remota	Ocorrência não esperada
3	Improvável	Ocorrência pouco provável
4	Provável	Ocorrência esperada
5	Freqüente	Ocorrência esperada várias vezes

Por esse motivo, avaliações que possuem objetivos diferentes podem apresentar grandes variações, ou seja, em uma organização, a mesma situação de risco en-

volvendo as mesmas vulnerabilidades, pode ter valores totalmente inversos, onde em uma o risco é alto e em outra organização o risco pode ser inexpressivo.

O risco é uma relação entre a sua freqüência de acontecimento e a conseqüência gerada por esse acontecimento. Portanto, para que se possa calcular o risco, relacionando a ele um *score*, é necessário definir algumas variáveis como a freqüência de acontecimento e sua conseqüência em relação a cada vulnerabilidade.

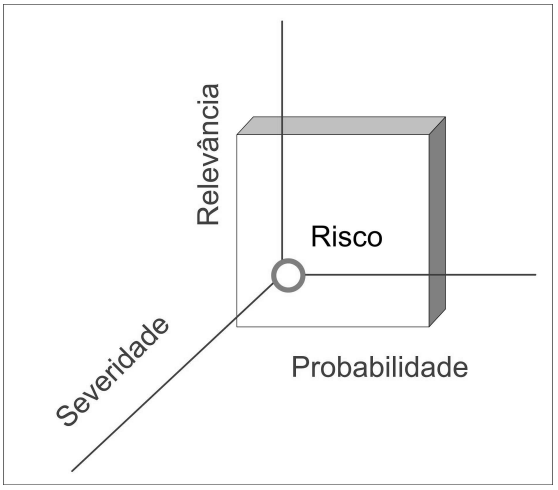

Figura 5.1: Cálculo do risco

A tabela 5.3 mostra a relação do tipo do risco com sua descrição, esclarecendo a ameaça sujeita e sua denominação, que pode ser branda ou desprezível a uma ameaça com um alto grau de risco, podendo causar uma perda catastrófica.

Tabela 5.3: Tabela de severidade do risco

Item	**Denominação**	**Descrição**
1	Desprezível	Sem perdas ou perdas insignificantes
2	Marginal	Perdas controláveis ou de baixo custo
3	Crítica	Perdas expressivas, correções devem ser imediatas
4	Catastrófica	Perdas irreparáveis, correções ineficientes

O modelo de conceituação de risco é importante para se conhecer o escopo do risco para a organização. Quanto maior a probabilidade de um evento ocorrer maior é o risco, enquanto o impacto depende do tipo de incidente determinado, que os riscos são crescentes, Figura 5.2, existe uma área intermediária onde os riscos são considerados moderados, no entanto, busca-se mitigar os riscos, ou mesmo anulá-los, situação difícil de conseguir, mas ao mesmo tempo almejada.

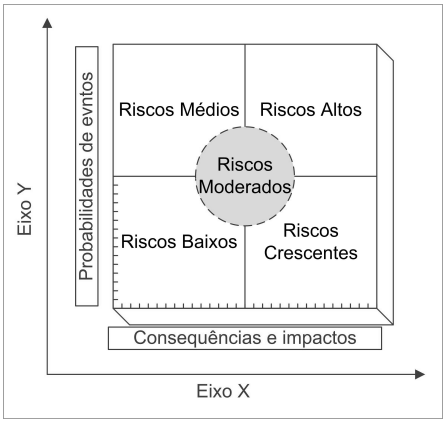

Figura 5.2: Modelo de conceituação do risco

5.2 *CVE - Common Vulnerabilities and Exposures*

CVE é uma lista de informações sobre vulnerabilidades e exposições da segurança da informação, criada em 1999 e que pretende fornecer nomes comuns para problemas publicamente conhecidos. O objetivo de *CVE* é tornar mais fácil o compartilhamento de informações através das potencialidades separadas da vulnerabilidade (ferramentas, repositórios, e os serviços) com esta numeração padrão.

Para demonstrar a grande capacidade de trabalho e a busca pela padronização e aceitação, os desenvolvedores do *CVE* estão catalogando cada vez mais informações sobre vulnerabilidades [12] (ver Figura 5.3, buscando sempre a transparência em suas ações. Desde o início do projeto as informações vêm crescendo em números, devido ao incremento de vulnerabilidades e fatores como maior utilização de tecnologias de redes.

Define-se como um padrão no tratamento e divulgação de informações sobre vulnerabilidades reportadas. O *CVE* é um banco de dados público em que todos interessados podem obter acesso a informações sobre vulnerabilidades.

O conteúdo do banco de dados *CVE* é resultado de esforços colaborativos entre várias entidades ligadas à segurança da informação, entre elas: *Sans Institute*, *Cancert*, *CERT*, entre outras.

O principal gestor do *CVE* é o *MITRE* (*Massachusetts Institute of Technology's Digital Computer Laboratory*). Como o projeto é colaborativo, não é exigida uma contribuição, mas pode ser feita, tanto financeiramente, quanto em relação à divulgação de informações.

A proposta geral do *MITRE* com a utilização do *CVE* não é apenas a divulgação de informações sobre o aspecto de vulnerabilidades e segurança[13], mas principalmente a padronização de como essa informação deve ser encaminhada e tratada. Dessa forma, corrigem-se eventuais duplicações de informação e trata

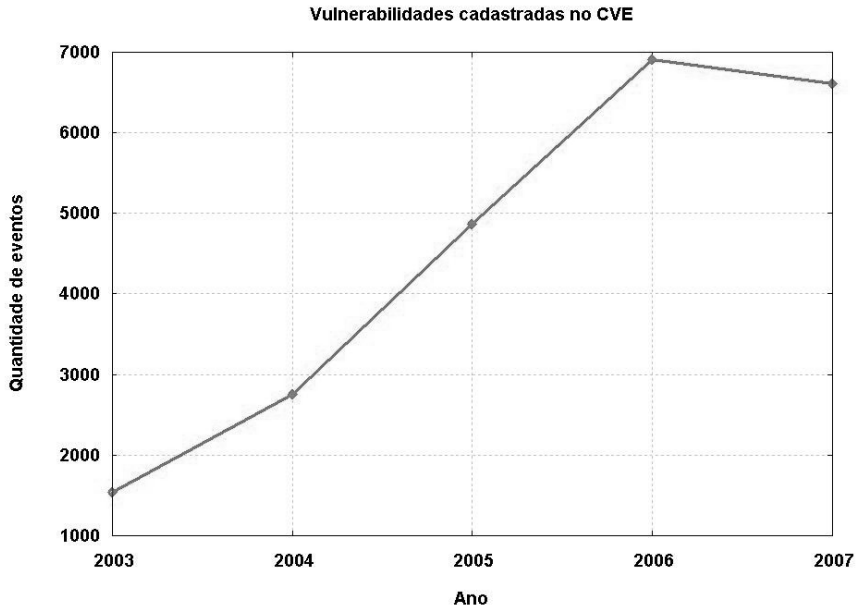

Figura 5.3: Vulnerabilidades cadastradas pelo *CVE*

de maneira eficiente os dados coletados, permitindo uma maior compreensão e, conseqüentemente, a qualidade na obtenção de dados relacionados à segurança.

Usando um identificador comum torna-se mais fácil compartilhar as informações através das bases de dados separadas, ferramentas e serviços.

Um identificador do *CVE* permite uma padronização das informações sobre vulnerabilidades. Conhecendo-se esse identificador é possível obter rapidamente a informação sobre o problema através das fontes de informação múltiplas que são compatíveis com o *CVE*. Por exemplo, possuindo uma ferramenta da segurança cujos relatórios contenham referências aos identificadores de *CVE*, pode-se então obter a informação da correção em uma base de dados.

5.2.1 Definição de nomes no *CVE*

Para facilitar a transferência de informações sobre vulnerabilidades, a equipe de projeto definiu algumas características que a nomenclatura deve conter no *CVE*, são elas:

- Número de identificação *CVE* (i.e., "*CVE*-2006-0125");
- Indicação para o status: Entrada ou candidato;
- Breve descrição da vulnerabilidade;
- Qualquer referência pertinente. Exemplo: vulnerabilidade reportada e relatório formal (*advisories*).

O número de identificação, também chamado de *CVE-ID*, é único, sendo representado pelo ano e número da vulnerabilidade em ordem de entrada.

A indicação do status tem uma regra simples, a entrada é toda a informação que foi aceita e faz parte da base como confirmada, o status candidato refere-se a informações que ainda não foram confirmadas mas está na lista para aceitação. Em breve descrição, toda a vulnerabilidade contém relação de informações pertinentes.

O processo para a criação de uma entrada *CVE* começa quando da descoberta de uma potencial vulnerabilidade. A informação, então, é designada como *CVE Candidate Numbering Authority (CNA)*, publicada no *CVE Web site*, e sugerida à comissão de diretores (*CVE Editor*).

A gestão do *CVE* cabe ao *MITRE* que em conjunto com a comissão de diretores irá discutir a lista de candidatos e votar se será ou não aprovada. Caso a decisão algum candidato seja a de rejeitar, será informado via Web site. Se o candidato for aceito o status será atualizado para entrada na lista *CVE* e também informado via *Website*.

5.2.1.1 Relatório do *CVE* para uma vulnerabilidade

```
Vulnerability Summary CVE-2007-5080
Original release date: 10/31/2007
Last revised: 11/1/2007
Source: US-CERT/NIST


Overview

Integer overflow in RealNetworks RealPlayer 10 and 10.5, RealOne Player 1,
and RealPlayer Enterprise for Windows allows remote attackers to execute
arbitrary code via a crafted Lyrics3 2.00 tag in an MP3 file, resulting in
a heap-based buffer overflow.

Impact

CVSS Severity (version 2.0):
CVSS v2 Base score: 9.3 (High) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

Access Vector: Network exploitable , Victim must voluntarily interact with
attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
```

Impact Type: Allows unauthorized disclosure of information , Allows unauthorized modification , Allows disruption of service

Vendor Statements (disclaimer)

Official Statement from Red Hat (11/1/2007)
Not vulnerable. This issue did not affect the versions of RealPlayer as shipped with Red Hat Enterprise Linux 3 Extras, 4 Extras, or 5 Supplementary.

References to Advisories, Solutions, and Tools

External Source: FRSIRT (disclaimer)
Name: ADV-2007-3628
Type: Advisory , Patch Information
Hyperlink: http://www.frsirt.com/english/advisories/2007/3628

External Source: (disclaimer)
Type: Patch Information
Hyperlink: http://service.real.com/realplayer/security/10252007_player/en/

External Source: SECUNIA (disclaimer)
Name: 27361
Type: Advisory , Patch Information
Hyperlink: http://secunia.com/advisories/27361

External Source: XF (disclaimer)
Name: realplayer-mp3-bo(37434)
Hyperlink: http://xforce.iss.net/xforce/xfdb/37434

External Source: SECTRACK (disclaimer)
Name: 1018866
Hyperlink: http://www.securitytracker.com/id?1018866

External Source: BID (disclaimer)
Name: 26214
Hyperlink: http://www.securityfocus.com/bid/26214

External Source: (disclaimer)
Hyperlink: http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-real-player-id3-tags/

External Source: VIM (disclaimer)
Name: 20071030 RealPlayer Updates of October 25, 2007
Hyperlink: http://www.attrition.org/pipermail/vim/2007-October/001841.html

```
Vulnerable software and versions

Configuration 1

RealNetworks, RealPlayer, 10.0, Unknown, Windows
RealNetworks, RealPlayer, 10.5, 6.0.12.1040, Windows
RealNetworks, RealPlayer, 10.5, 6.0.12.1578, Windows
RealNetworks, RealPlayer, 10.5, 6.0.12.1698, Windows
RealNetworks, RealPlayer, 10.5, 6.0.12.1741, Windows
RealNetworks, RealOne Player, 1.0, Unknown, Windows, En
RealNetworks, RealOne Player, 2.0, Unknown, Windows
RealNetworks, RealPlayer Enterprise, Unknown, Unknown, Windows, En


Technical Details

Vulnerability Type (View All)
Numeric Errors   (CWE-189)

CVE Standard Vulnerability Entry:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5080

Common Platform Enumeration:
http://nvd.nist.gov/cpe.cfm?cvename=CVE-2007-5080
```

5.3 *CVSS - Common Vulnerability Scoring System*

O *CVSS* surgiu como um modelo para cálculo de risco de vulnerabilidades [45], utilizando como base o *CVE*, discutido no capitulo 5.2.

A idéia era que um novo padrão surgisse [36], elevando o nível de controle sobre as vulnerabilidades, já então divulgadas pelo *CVE* através de acordos com empresas desenvolvedoras e *CSIRTs* [8] pelo mundo [34]. Logo que a versão 1 foi disponibilizada começaram os trabalhos em seu aperfeiçoamento e, em julho de 2007, foi lançada a versão 2[51], versão esta adotada neste trabalho.

Vários órgãos e departamentos ligados à segurança da informação como o *NIST* (*National Institute of Standards and Technology*), *FIRST (Forum of Incident Response and Security Teams)* [36], *CERT (Computer Emergency Response Team)* entre outros, se juntaram para criar um padrão para pontuação/mensuração de vulnerabilidades de *software* chamado de *CVSS* [53].

Historicamente, a indústria tem utilizado diversos métodos de *scoring* para

vulnerabilidades de *softwares* [45], geralmente sem detalhamento desses critérios ou processos.

É importante saber que toda vulnerabilidade tem um tempo de vida [30], que deve ser respeitado e seguido para a solução do problema.

O *NIAC* (*National Infrastructure Advisory Council*)[47] escolheu o *FIRST* para liderar o projeto e avaliar um padrão aberto e universal onde deverá ajudar organizações a priorizar a segurança e análise de vulnerabilidades, consolidar esforços do mundo todo e equipes de segurança para resolver o problema permitindo uma resposta mais rápida a riscos provenientes de vulnerabilidades conhecidas.

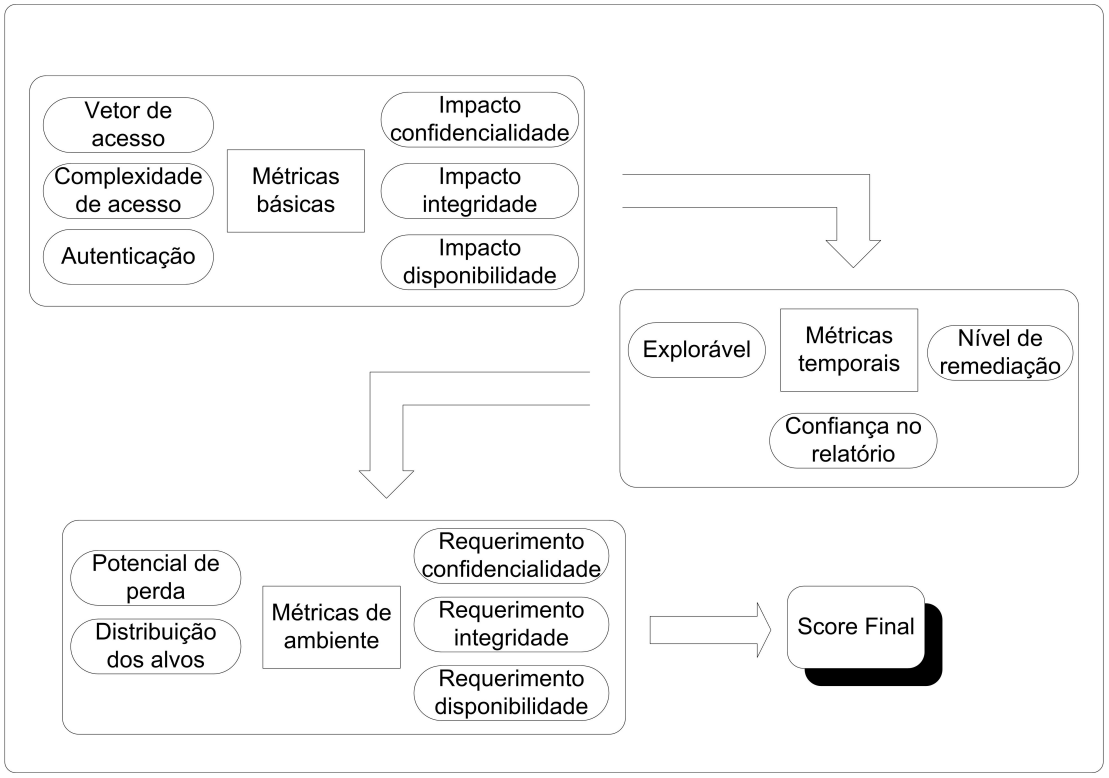

Figura 5.4: Organização do *CVSS*

Para se calcular o escore para uma determinada vulnerabilidade o *CVSS* tem como base três métricas principais:

- Métricas básicas (*Base Metrics*) contêm os atributos que são intrínsecos a toda vulnerabilidade;
- Métricas temporais (*Temporal Metrics*) contêm as características que evoluem de acordo com o ciclo de vida da vulnerabilidade;
- Métricas ambientais (*Environmental Metrics*) representam aquelas características únicas de acordo com o ambiente corporativo onde está sendo implantada.

A base para se conhecer o risco é dada pela tabela 5.4, que mostra o intervalo entre os riscos.

Tabela 5.4: *Ranking* do risco

Risco	**Intervalo *score***
Baixo	0.0 - 3.9
Médio	4.0 - 6.9
Alto	7.0 - 10.0

5.3.1 Métricas Básicas

As métricas básicas capturam as características de uma vulnerabilidade que é constante com tempo e através dos ambientes de usuário. O vetor de acesso à dificuldade e a autenticação capturam como a vulnerabilidade é acessada e as circunstâncias ou não de condições extras que são requeridas para explorá-la. Essas três métricas medem o impacto de como uma vulnerabilidade, se explorada, afetará diretamente um ativo ou recurso de *TI*, onde os impactos são definidos independentemente como o grau de perda da confidencialidade, integridade e da disponibilidade. Por exemplo, uma vulnerabilidade pode causar uma perda parcial da integridade e da disponibilidade, mas nenhuma perda da confidencialidade.

A princípio as métricas básicas são informadas pelo fabricante do produto. São definidas seis métricas para se obter um escore que em conjunto com as métricas temporais e ambientais formarão o cálculo do risco final:

1. Complexidade de acesso: mede a complexidade requerida para que um atacante consiga explorar o sistema alvo;
2. Vetor de acesso: indica se uma vulnerabilidade é explorada localmente ou remotamente;
3. Autenticação: indica se um atacante necessita ou não ser autenticado no sistema para conseguir explorar a vulnerabilidade;
4. Impacto de confidencialidade: mede o impacto na confidencialidade (nenhum / parcial / completo);
5. Impacto de integridade: indica o impacto na integridade;
6. Impacto de disponibilidade: impacto na disponibilidade.

5.3.1.1 Vetor de acesso (AV)

Esta métrica reflete como a vulnerabilidade é explorada. Quanto mais remoto o ataque ao *host* for, maior será o *score* da vulnerabilidade. Os valores possíveis são:

Local (L) : Uma vulnerabilidade explorada com requerimentos apenas de acesso local requer que o atacante tenha o acesso físico ao sistema vulnerável ou uma conta *shell* local. Os exemplos de vulnerabilidades localmente exploradas são ataques a periféricos tais como ataques *Firewire/USB*, e escalada de privilégio;

Adjacent Network (A) : Uma vulnerabilidade explorada com acesso de rede adjacente requer que o atacante tenha o acesso à transmissão ou ao domínio da colisão do *software* vulnerável. Os exemplos de redes locais incluem o *subnet* local do IP, *Bluetooth*, *IEEE 802.11*, e o segmento de ethernet local;

Network (N) : Uma vulnerabilidade explorada com acesso de rede significa que o *software* vulnerável está limitado à pilha da rede e o atacante não precisa ter acesso de rede local ou o acesso local. Esta vulnerabilidade é conhecida por remotamente explorada. Um exemplo de um ataque desse tipo é o *RPC buffer overflow*.

5.3.1.2 Complexidade de acesso (AC)

Esta métrica mede a complexidade do ataque requerido para explorar a vulnerabilidade, uma vez que um atacante ganhou o acesso ao sistema de alvo. Por exemplo: Considere um ataque de *buffer overflow* em um serviço da *Internet*: uma vez que o sistema alvo é encontrado, o atacante pode explorá-lo a vontade.

Outras vulnerabilidades, entretanto, podem precisar de etapas adicionais a fim serem exploradas. Por exemplo, uma vulnerabilidade em um cliente do *e-mail* é explorada somente após os *downloads* de mensagens anexadas. Pode-se dizer então que quanto menor as exigências para o acesso, maior o risco, conseqüentemente maior o cálculo do *score*. Os valores possíveis para essa métrica são:

High (H) : As condições especializadas do acesso existem. Por exemplo: Na maioria das configurações o atacante tenta elevar seus privilégios ou *spoofa* outros sistemas além do sistema atacado, por exemplo, um *DNS hijacking*. Outro exemplo é que o atacante depende dos métodos de engenharia social que seriam detectados facilmente por pessoas mais esclarecidas, por exemplo, a vítima deve executar diversas ações suspeitas ou atividades atípicas;

Medium (M) : As condições de acesso são um tanto especializadas, por exemplo: O ataque é limitado a um grupo de sistemas ou os usuários em algum nível de autorização, possivelmente sem confiança. Alguma informação deve ser recolhida antes que um ataque bem sucedido possa ser iniciado. O ataque requer um pouco de engenharia social para que possa ocasionalmente enganar usuários cautelosos, por exemplo, ataques de *phishing* possibilitando que os ataques modifiquem a barra de status de um web browser para mostrar um link falso;

Low (L) : Condições especializadas de acesso ou circunstâncias não existem. Por exemplo: Um produto afetado tipicamente requer acesso para uma larga escala de sistemas e usuários, possibilitando acesso anônimo ou não confiável.

5.3.1.3 Autenticação (Au)

Esta métrica mede o número de vezes que um atacante deve autenticar a um alvo a fim de explorar uma vulnerabilidade. Esta métrica não calibra a força ou a complexidade do processo de autenticação, somente que as credenciais sejam informadas antes que uma exploração possa ocorrer. Quanto menor o nível da autenticação requerida, maior o *score* da vulnerabilidade. Os valores possíveis para esta métrica são:

Multiple (M) : Explorar uma vulnerabilidade requer que o atacante se autentique duas ou mais vezes, mesmo se as credenciais sejam iguais;

Single (S) : A vulnerabilidade requer que o atacante esteja *logado* no sistema, como uma linha de comando ou via sessão de *desktop* ou interface *Web*;

None (N) : Autenticação não é necessária para explorar uma vulnerabilidade.

Esta métrica deve ser aplicada baseada na autenticação de um atacante antes de iniciar um ataque. Por o exemplo, se um *mail server* for vulnerável a um comando que possa ser emitido antes que um usuário se autentique, a métrica deve ser marcado como *None (N)* porque o atacante pode iniciar um ataque antes que seja solicitada a autenticação. Se o comando vulnerável estiver disponível somente após a autenticação bem sucedida, então deve ser marcado como *Single* (S) ou *Multiple* (M) dependendo de quantas instâncias para autenticação ocorrem antes de possibilitar a execução do comando.

5.3.1.4 Impacto de confidencialidade (C)

Esta métrica mede o impacto na confidencialidade para uma exploração com sucesso de uma vulnerabilidade. A confidencialidade refere-se a limitar o acesso e a divulgação de informação somente aos usuários autorizados. O impacto de confidencialidade alto também aumenta o valor para o cálculo do escore para a vulnerabilidade. Os valores possíveis para esta métrica são:

None (N) : Não existe impacto na confidencialidade para o sistema;

Partial (P) : Há uma considerável divulgação de informação. O acesso a alguns arquivos do sistema é possível, mas o atacante não tem o controle sobre o que é obtido. Um exemplo é uma vulnerabilidade que divulga somente determinadas tabelas em uma base de dados;

Complete (C) : Há uma divulgação total de informação, resultando em todos os arquivos de um sistema que estão disponíveis. O atacante pode ler todos os dados do sistema.

5.3.1.5 Impacto de integridade (I)

Esta métrica mede o impacto em relação a integridade do sucesso na exploração da vulnerabilidade. A integridade garante que a informação não foi alterada. Com o impacto da integridade alto, o valor do escore também aumenta. Os valores possíveis para esta métrica são:

None (N) : Não existe impacto na integridade para o sistema;

Partial (P) : A modificação de alguns arquivos do sistema é possível, mas o atacante não tem o controle sobre o que pode ser modificado. Por exemplo, os arquivos do sistema, ou da aplicação, podem ser sobrescritos ou modificados, mas o atacante não tem controle sobre quais arquivos podem ser afetados ou modificados;

Complete (C) : Há um total comprometimento da integridade do sistema. Há uma perda completa da proteção do sistema, tendo por resultado o sistema inteiro comprometido. O atacante pode modificar todos os arquivos do sistema.

5.3.1.6 Impacto de disponibilidade (A)

Esta métrica mede o impacto em relação disponibilidade do sistema referente a uma exploração com sucesso. A disponibilidade refere-se à acessibilidade de recursos da informação. Ataques que consomem a largura de banda da rede, os ciclos do processador, ou o espaço em disco acabam por afetar a disponibilidade de um sistema. Quanto maior o impacto sobre a disponibilidade, maior o *score* do risco. Os valores possíveis para esta métrica são:

None (N) : Não existe impacto na disponibilidade para o sistema;

Partial (P) : Há uma redução na performance ou interrupção na disponibilidade do recurso. Um exemplo é um ataque de *flood* que permite um número limitado de conexões bem sucedidas a um serviço do Internet;

Complete (C) : Há uma parada total do recurso afetado. O atacante pode tornar o recurso completamente indisponível.

5.3.2 Métricas Temporais

A ameaça causada por uma vulnerabilidade pode mudar o tempo excedente. O *CVSS* captura três valores, a saber: confirmação dos detalhes técnicos de uma vulnerabilidade, o status da correção para a vulnerabilidade, e da disponibilidade do código ou das técnicas do *exploit*. Este valor é usado quando o usuário sente que a métrica particular não se aplica e deseja saltar o excesso.

1. "*Exploitability*": indica se é possível ou não explorar a vulnerabilidade;
2. "*Remediation Level*": informa se há uma solução conhecida;
3. "*Report Confidence*": representa o grau de confiança na existência da vulnerabilidade e na credibilidade de sua divulgação ("*Unconfirmed / Uncorroborated / Confirmed*").

5.3.2.1 Exploitability (E) - Explorável

Esta métrica mede o estado atual de técnicas do *exploit* ou de disponibilidade do código. A disponibilidade pública do código *easy-to-use* do exploit aumenta o número de atacantes potenciais incluindo aqueles que são inábeis, aumentando desse modo a severidade da vulnerabilidade.

Inicialmente, a exploração pode ser somente teórica. A publicação de um código para a prova do conceito (POC), do código funcional do *exploit*, ou dos detalhes técnicos, suficientemente necessário para explorar a vulnerabilidade. Além disso, o código do *exploit* disponível pode progredir de uma demonstração da prova de conceito para um código para se explorar a vulnerabilidade consistentemente. Em casos severos, pode ser entregue com o *payload* de um worm ou vírus. Quanto mais facilmente a vulnerabilidade pode ser explorada, mais elevado é o escore. Valores possíveis são:

Unproven : Nenhum código para o *exploit* está disponível, ou o *exploit* é inteiramente teórico;

Proof of Concept : A prova de conceito do *exploit* ou uma demonstração do ataque que não seja prática para a maioria dos sistemas está disponível. O código ou a técnica não são funcionais em todas as situações e podem requerer a modificação substancial por um atacante hábil;

Functional : O código funcional do *exploit* está disponível. O código trabalha na maioria das situações onde a vulnerabilidade existe;

High : Ou a vulnerabilidade é explorada por um código autônomo móvel funcional, ou nenhuma exploit é requerido (disparador manual) e os

detalhes estão extensamente disponíveis. O código trabalha em cada situação, ou está sendo entregue ativamente através de um agente autônomo móvel como um *worm* ou um vírus.

Not Defined (ND) : Atribuir este valor a métrica não influenciará o score. É um sinal para equação saltar esta métrica.

5.3.2.2 Remediation Level (RL) - Nível de remediação

O nível da remediação de uma vulnerabilidade é um fator importante para priorização. Uma vulnerabilidade típica surge quando uma correção é publicada. As correções que estão sendo desenvolvidas conhecidos como *workarounds* ou os *hotfixes* podem oferecer a correção parcial até uma correção oficial seja lançada. Cada um destes estágios respectivos ajusta o *score* temporal para baixo, refletindo em uma diminuição da urgência enquanto a correção se torna final. Exceto uma correção oficial ou permanente, todos os outros valores elevam o cálculo do *score*. Valores possíveis são:

Official Fix (OF) : Uma solução completa do fabricante está disponível. Ou o fabricante emitiu um *patch* oficial, ou um *upgrade* está disponível.

Temporary Fix (TF) : Há uma correção oficial disponível no entanto é provisória. Isto inclui os exemplos onde o vendedor emite um hotfix temporário, uma ferramenta, ou que está a trabalho;

Workaround (W) : Há uma solução não oficial disponível, que não foi disponibilizada pelo fabricante. Em alguns casos, os usuários da tecnologia afetada criarão uma correção eles mesmos ou fornecerão os passos necessários para se contornar ou mitigar a vulnerabilidade;

Unavailable (U) : Não existe nenhuma solução disponível ou é impossível aplicar a correção;

Not Defined (ND) : Atribuir este valor a métrica não influenciará o score. É um sinal para equação saltar esta métrica.

5.3.2.3 Report Confidence (RC) - Confiança no relatório

Esta métrica mede o grau de confiança na existência da vulnerabilidade e na credibilidade dos detalhes técnicos conhecidos. Às vezes, somente a existência da vulnerabilidade é divulgada, mas sem detalhes específicos. A vulnerabilidade pode mais tarde ser confirmada e reconhecida pelo fabricante da tecnologia afetada. A urgência de uma vulnerabilidade é mais alta quando ela é conhecida e se tem certeza de sua existência. Esta métrica sugere também o nível de conhecimento técnico disponível aos atacantes. Quando a vulnerabilidade é validada pelo fabricante da tecnologia afetada, ou outras fontes de respeito, maior é o risco. Valores possíveis são:

Unconfirmed (UC) : Existe uma única fonte não confirmada ou possivelmente alguns relatórios conflitantes. Há pouca confiança na validade dos relatórios. Um exemplo é um boato *hacker*;

Uncorroborated (UR) : Existem algumas fontes não oficiais, possivelmente empresas independentes de segurança ou organizações de pesquisa. Neste momento pode haver muitos detalhes técnicos conflitantes;

Confirmed (C) : A vulnerabilidade foi reconhecida pelo fabricante ou pelo autor da tecnologia afetada. A vulnerabilidade pode também ser confirmada quando sua existência é confirmada em um evento externo, tal como a publicação do código funcional ou da prova de conceito do exploit;

Not Defined (ND) : Atribuir este valor a métrica não influenciará o score. É um sinal para equação saltar esta métrica.

5.3.3 Métricas Ambientais

As métricas de ambiente têm uma importância muito grande neste trabalho, pois é através desta métrica que o risco medido poderá ser eficaz ou não contra a infra-estrutura da empresa.

A importância se deve ao fato de que uma vulnerabilidade descoberta, afetando um serviço para um sistema operacional, pode ter seu impacto reduzido caso este sistema afetado tenha uma participação inexpressiva, por esse motivo é muito importante que conste, na ferramenta que irá implantar, a metodologia proposta uma maneira de se medir o número total de sistemas operacionais.

5.3.3.1 *Collateral Damage Potential (CDP)*

Esta métrica mede o potencial para a perda de vida ou de recursos físicos com os danos ou o roubo da propriedade ou do equipamento. A métrica pode também medir a perda econômica da produtividade ou do rendimento. Quanto maior o potencial dos danos, mais elevada o escore da vulnerabilidade. Os valores possíveis para esta métrica são:

None (N) : Não há nenhum potencial para a perda de vida, de recursos físicos, de produtividade ou de rendimento;

Low (L) : Um exploit bem sucedido para esta vulnerabilidade pode resultar em danos pequenos. Ou, pode haver uma perda pequena do rendimento ou da produtividade à organização;

Low-Medium (LM) : Um exploit bem sucedido para esta vulnerabilidade pode resultar em danos moderados. Ou, pode haver uma perda moderada do rendimento ou da produtividade à organização;

Medium-High (MH) : Um exploit bem sucedido para esta vulnerabilidade pode resultar em danos ou perdas significativas. Ou, pode haver uma perda significativa do rendimento ou da produtividade;

High (H) : Um exploit bem sucedido para esta vulnerabilidade pode resultar em danos ou perdas catastróficas. Ou, pode haver uma perda catastrófica do rendimento ou da produtividade;

Not Defined (ND) : Atribuir este valor a métrica não influenciará o escore. É um sinal para equação saltar esta métrica.

5.3.3.2 *Target Distribution (TD)*

Indica o tamanho relativo da quantidade de sistemas que são suscetíveis à vulnerabilidade (Nenhum; Baixo até 15%; Médio até 49% ou Alto - se acima de 50% dos sistemas são vulneráveis). Os valores possíveis para esta métrica são:

None (N) : Não existe sistema alvo, ou os alvos são altamente especializados e existem somente em laboratório. Eficazmente 0% do ambiente está no risco;

Low (L) : Os alvos existem dentro do ambiente, mas em uma escala pequena. Entre 1% - 25% do ambiente total está em risco;

Medium (M) : Os alvos existem dentro do ambiente, mas em uma escala média. Entre 26% - 75% do ambiente total está em risco;

High (H) : Os alvos existem dentro do ambiente em uma escala considerável. Entre 76% - 100% do ambiente total são considerados de risco;

Not Defined (ND) : Atribuir este valor a métrica não influenciará o score. É um sinal para equação saltar esta métrica.

5.3.3.3 *Security Requirements (CR, IR, AR)*

Estas métricas permitem ao analista a customização do *CVSS* dependendo da importância para efeito do ativo de *TI* aos usuários da organização, permitindo medir os termos para confidencialidade, integridade, e da disponibilidade, isto é, se recurso de *TI* suporta uma função do negócio onde a disponibilidade é a mais importante, o analista pode atribuir um valor maior à disponibilidade, relativo à confidencialidade e à integridade. Cada exigência da segurança tem três valores possíveis: "baixo", "meio", ou "elevado".

O efeito total para a variável de ambiente é determinado pela correspondência do impacto das métricas básicas, notando que em métricas básicas o valor

dado a *CIA* (confidencialidade, integridade e a disponibilidade), ele mesmo, não é mudado. Isto é, estas métricas modificam o *score* para as métricas de ambiente pelo recálculo da base do impacto das métricas, confidencialidades, integridade e da disponibilidade. Para o exemplo temos: O impacto da confidencialidade (C) aumentou o peso se a exigência da confidencialidade (CR) fosse "alta". Do mesmo modo, o impacto da confidencialidade diminuiu o peso se a exigência da confidencialidade fosse "baixa". O impacto da confidencialidade se torna neutro se a exigência da confidencialidade for "média". Esta mesma lógica é aplicada às exigências da integridade e da disponibilidade.

Note que a exigência da confidencialidade não afetará o *score* da variável de ambiente se a variável básica da confidencialidade for ajustado para nenhum. Também, aumentar a exigência da confidencialidade de médio para alto não mudará o *score* para a variável de ambiente quando as variáveis básicas estiverem ajustadas para completo. Isto é porque o cálculo do *score* parte da métrica básica que já está em um valor máximo de 10.

Maior a exigência da segurança, maior o *score*, por default é médio. Estas métricas modificarão o *score* tanto para mais quanto para menos com um mínimo de 2.5. Os valores possíveis são usados para as três métricas e são:

Low (L) : Perda de confidencialidade, integridade ou disponibilidade, é provável ter somente um efeito adverso limitado na organização ou nos indivíduos, associada com a organização (por exemplo, empregados, clientes).

Medium (M) : Perda de confidencialidade, integridade ou disponibilidade, é provável ter um efeito adverso sério na organização ou nos indivíduos, associada com a organização (por exemplo, empregados, clientes).

High (H) : Perda de confidencialidade, integridade ou disponibilidade, é provável ter um efeito adverso catastrófico na organização ou nos indivíduos, associada com a organização (por exemplo, empregados, clientes).

Not Defined (ND) : Atribuir este valor a métrica não influenciará o escore. É um sinal para equação saltar esta métrica.

5.3.4 Modelo Matemático do *CVSS*

O processo de *score* irá definir o valor final resultante da aplicação de todas as métricas, combinando todos os valores de acordo com fórmulas específicas conforme [53].

Da combinação dos três grupos descritos no projeto *CVSS* obtêm-se o score final. Todo este sistema de métricas pode ser representado sinteticamente através de vetores conforme tabela 5.5.

Tabela 5.5: *CVSS* - Definição dos vetores

Vetores	**Descrição**
Básicos	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N] /C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporais	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND] /RC:[UC,UR,C,ND]
Ambientes	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND] /CR:[L,M,H,ND]/IR:[L,M,H,ND]/AR:[L,M,H,ND]

Desta maneira existe certa facilidade na impostação dos dados ou mesmo no seu tratamento por parte de um programa gerenciador.

A proposta dos idealizadores do *CVSS* é ter um modelo fácil de aplicar e ao mesmo tempo completo. O gerenciamento de *TI* obtém uma ferramenta para análise de vulnerabilidades permitindo uma análise de risco que envolve tanto *software* quanto *hardware*.

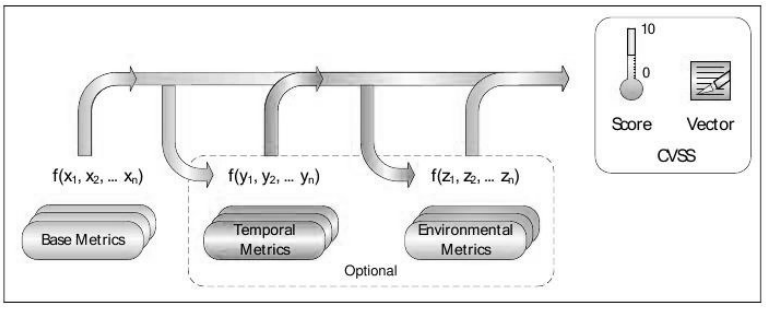

Figura 5.5: Métricas e equações

Atualmente, dezenas de vulnerabilidades são divulgadas diariamente, mas o grande problema é verificar se essas vulnerabilidades afetam ou não o andamento dos serviços de uma empresa.

As equações do modelo *CVSS* são calculadas utilizando *scores* que devem ter seu valor entre 0 e 10. Cada métrica tem seu valor pontuado separadamente, sendo os valores retroalimentados para as duas etapas seguintes, métricas temporárias e de ambiente, no entanto, a última métrica (Ambiente) deve ter seus valores calculados com base nas duas primeiras, métricas básicas e métricas de ambiente, conforme Figura 5.5, sendo essas duas opcionais para o modelo do *CVSS*, mas neste trabalho são tão importantes quanto a primeira, pois permite que o modelo se adeqüe à empresa ou à organização onde se pretenda implementá-lo.

5.3.4.1 Modelo matemático para métricas básicas

As métricas básicas têm seus valores intrínsecos à vulnerabilidade, ou seja, no momento da divulgação da informação pelo menos esta métrica deve estar com seus valores calculados. São utilizadas variáveis como:

- Vetor de acesso;
- Complexidade de acesso;
- Autenticação;
- Impacto sobre a confidencialidade;
- Impacto sobre a integridade;
- Impacto sobre a disponibilidade.

As métricas básicas tem o cálculo elaborado através da equação 5.2. Percebe-se que o impacto tem *score* maior (60%) em relação à possibilidade de exploração (40%), devido ao fato de que uma exploração é ineficiente se não pode causar nenhum tipo de impacto.

$$BaseScore = round\_to\_1\_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f_{impact})) \tag{5.2}$$

Onde o impacto (*Impact*) é calculado pela equação 5.3, e para cada impacto pode ter seu valor obtido através da tabela 5.6. Caso em qualquer dos impactos seja nenhum o valor é assumido como 1, portanto não terá alteração do valor final por ser um produtório. O valor 10.41 do produtório é apenas para que os valores obtenham um escore entre 0 e 10, devendo ter um arredondamento para uma casa decimal.

$$Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact)) \tag{5.3}$$

A equação 5.3 mede o impacto dos pilares relacionados a confidencialidade (*ConfImpact*), integridade (*integImpact*) e disponibilidade (*AvailImpact*) das informações, onde temos os valores para:

Tabela 5.6: Impactos

Impacto	**Nenhum**	**Parcial**	**Total**
Confidencialidade	0.0	0.275	0.660
Integridade	0.0	0.275	0.660
Disponibilidade	0.0	0.275	0.660

A possibilidade de exploração (*Exploitability*) é calculada pela equação 5.4

$$Exploitability = 20 * AccessVector * AccessComplexity * Authentication \quad (5.4)$$

A equação 5.4 que calcula o *exploitability* é elaborada através das variáveis que medem o vetor de acesso ver tabela 5.7, complexidade de acesso ver tabela 5.8 e autenticação ver tabela 5.9.

Tabela 5.7: Vetor de acesso

Vetor de Acesso (*AccessVector*)	**Score**
Requer acesso Local	0.395
Rede adjacente acessível	0.646
Rede acessível	1.0

Tabela 5.8: Complexidade de acesso

Complexidade de acesso (*AccessComplexity*)	**Score**
Alta	0.35
Média	0.61
Baixa	0.71

Tabela 5.9: Autenticação

Autenticação (*Authentication*)	**Score**
Requer Múltiplas instâncias para autenticação	0.45
Requer instâncias simples para autenticação	0.56
Não requer autenticação	0.704

A variável f_{impact} referente a equação 5.2 é determinada pelos valores 0 se não existe impacto e 1.176 se existe impacto.

5.3.4.2 Modelo matemático para métricas temporais

A equação para se obter a métrica temporal (equação 5.5) é uma combinação da equação 5.2 (*basescore*) que deve produzir um valor entre 0 e 10, esta equação poderá produzir um resultado não tão elevado quando a equação 5.2 no entanto não menos que 33% do *basescore*.

$$TemporalScore = round\_to\_1\_decimal(BaseScore * Exploitability * RemediationLevel * ReportConfidence) \quad (5.5)$$

A equação 5.5 que calcula o *score* temporal é elaborada através das variáveis que medem o nível de exploração (*exploitability*) ver a tabela 5.10, o nível de correção (*Remediation Level*) ver tabela 5.11 e o nível de confiança (*Report Confidence*) ver tabela 5.12.

Tabela 5.10: Nível de exploração

Exploitability	**Score**
Não provado	0.85
Prova de conceito	0.9
Funcional	0.95
Alto	1.0
Não definido	1.0

Tabela 5.11: Nível de correção

Nível de correção (*Remediation Level*)	**Score**
Correção oficial	0.87
Correção temporária	0.90
Correção em desenvolvimento	0.95
Não disponível	1.0
Não definido	1.0

O nível de confiança é muito importante, pois aqui será definido o grau de confiança na informação divulgada, não devendo ser descartado nenhum dado, até mesmo os boatos devem ser considerados, não devendo ignorar uma informação, por mais inseguro que seja o canal de divulgação deve-se concentrar pelo excesso e nunca pela omissão.

Tabela 5.12: Nível de confiança

Nível de confiança *(Report Confidence)*	**Score**
Não confirmada	0.90
Não provado	0.95
Confirmado	1.0
Não definido	1.0

5.3.4.3 Modelo matemático para métricas de ambiente

A partir das métricas básicas, os cálculos seguintes sofrem retroalimentação. Neste projeto as métricas de ambiente têm importância extra, pois espelham a real visão do ambiente interno da empresa.

A equação 5.6 para a métrica de ambiente é a soma da métrica básica ajustada (*AdjustedImpact*) com o produto efeito colateral e potência dano e a distribuição do alvo medida em porcentagem.

$$EnvironmentalScore = round\_to\_1\_decimal((AdjustedTemporal + (10 - AdjustedTemporal) * CollateralDamagePotencial) * TargetDistribution) \quad (5.6)$$

Onde o potencial efeito colateral (*CollateralDamagePotencial*) é dado pela tabela 5.13

Tabela 5.13: Potencial Efeito Colateral

Potencial Efeito Colateral *(Collateral Damage Potential)*	**Score**
Nenhum	0.00
Baixo	0.1
Baixo/Médio	0.3
Médio/Alto	0.4
Alto	0.5
Não definido	0

A tabela 5.14 mostra os valores para as variáveis dos alvos (*TargetDistribution*), onde é medido em porcentagem de sistemas que podem ser afetados, este item é demasiado importante, pois uma vulnerabilidade que só afeta um determinado sistema operacional pode ser inútil caso não exista esse sistema em uma rede.

Tabela 5.14: Distribuição dos alvos

Distribuição dos alvos *(Target Distribution)*	**Score**
Nenhum	0.00
Baixo	0.25
Médio	0.75
Alto	1.0
Não definido	1.0

Onde a equação 5.7 (*AdjustedImpact*) é dada por:

$$AdjustedImpact = min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq) * (1 - IntegImpact * IntegReq) * (1 - AvailImpact * AvailReq))) \quad (5.7)$$

A equação 5.7 dada pelo cálculo do *AdjustedImpact* possui variáveis de requerimento de segurança dada pela tabela 5.15

Tabela 5.15: Requerimentos de segurança

Requerimentos	Baixo	Médio	Alto	Não definido
Confidencialidade	0.5	1.0	1.51	1.0
Integridade	0.5	1.0	1.51	1.0
Disponibilidade	0.5	1.0	1.51	1.0

5.4 Estratégias de gerenciamento de Risco

Primeiramente, não existe uma estratégia única para o gerenciamento do risco[48], deve-se utilizar diversas ferramentas que buscam organizar e gerenciar toda a informação. Somente após a informação estar disponível deve-se gerenciar o risco, pois uma estrutura caótica, sem conhecimento do que existe não pode ser gerenciada, conseqüentemente o risco não pode ser medido.

Situações como uma análise intuitiva podem até existir, no entanto o controle dessa situação torna-se inviável em curto prazo, mesmo se se pensar em longo prazo o problema permanece.

Outra situação é saber se a análise de risco irá ou não trazer benefícios para a empresa. Em algumas organizações o tempo e o custo demandado pode ser maior do que o próprio valor da informação. Talvez isso não seja eficiente, por esse motivo a estratégia deve ser bem planejada, levando-se em consideração o negócio, e não o interesse em se implementar algo que não será revertido para o bem da empresa, seja qual for a área de atuação.

Alguns fatores devem ser de conhecimento para o momento do planejamento da estratégia de gerenciamento do risco, a administração da empresa em conjunto com a equipe de *TI* devem levantar os seguintes itens[54]:

- Fatores de riscos que não são conhecidos ou percebidos podem e afetam os lucros da empresa;
- Incidentes de segurança causam perdas, e muitas vezes essas perdas podem levar o negócio a ficar inviável;
- Novos produtos podem alavancar as receitas da empresa, no entanto, pode não ter ligação direta com o aumento das vendas;
- Os riscos derivados da utilização da *TI* existem, esses mesmo riscos podem se propagar para diferentes áreas com características diferentes;
- Os riscos do negócio devem considerar os riscos derivados da *TI*, pois o impacto gerado pela *TI* pode e tem ligação direta com o negócio.

Diante do exposto, os riscos devem ser entendidos. A eficiência e qualidade são determinadas pelo gerenciamento do risco. Neste contexto quatro estratégias podem ser possíveis para se gerenciar o risco [44]:

1. Mitigação de Riscos: Geralmente a estratégia que é a mais utilizada, devendo conter todas as ações que a equipe de segurança definir, visando diminuir as ameaças e aumentar a segurança com a implantação de *firewalls*, IDS, antivírus, e controles de acesso;

2. Aceitação de Riscos: Neste caso se o valor para se eliminar o risco for maior do que o valor da informação, ou se depender de transferir recursos para eliminação de um risco mais grave deve-se aceitar o risco, mesmo que temporariamente;

3. Transferência de Riscos: Em diversas situações, inclusive do cotidiano das pessoas, é bem comum transferir o risco a terceiros[5], como exemplo cita-se a seguradora de carro, que aloca recursos limitados para iniciativas de mitigação.

4. Contenção de Riscos: Podem existir situações graves que o risco é alto assim como o seu custo, não podendo simplesmente ser aceito ou tolerado. Nesta situação a fim de se evitar o risco, pode ser necessária sua contenção, seja retirando um sistema de atendimento, ou mesmo deixando de colocar um novo produto.

A ação mais sensata seria a mitigação de todos os riscos que encontrar, no entanto o custo e demanda de tempo para eliminar as vulnerabilidades pode ser tamanha que seria impraticável [44]. Para isso deve existir uma estratégia combinada de acordo com as necessidades e natureza da empresa e seu departamento de *TI*.

Para um gerenciamento de risco eficiente, deve se utilizar de automatização, o máximo que se puder. Buscando a detecção dos ativos, e conseqüente avaliação do risco a que esses ativos estão sujeitos, inclusive o controle dos processos para correção desses ativos frente às vulnerabilidades e se esses processos foram ou não eficientes.

Pesquisas recentes da *Gartner Group*, afirmam que empresas que implementarem processos para gerenciamento de riscos e novas tecnologias para identificar, gerenciar e eliminar vulnerabilidades podem reduzir em até 90% as chances de um ataque bem-sucedido.

O que se tem acompanhado em empresas despreparadas é que muitas acreditam que simplesmente instalando um sistema de *firewall* estarão seguras, é como colocar uma cerca elétrica, aparentemente pode se estar seguro, no entanto, uma brecha na cerca pode afetar toda a segurança da casa, por esse motivo segundo [44], o nível de conhecimento e gerenciamento de risco, seja em qual estratégia for, deve receber atenção especial e recursos para isso, sempre buscando o maior benefício possível.

Software de gerenciamento tem um ganho excelente em relação ao controle dos ativos e segurança, pois a infra-estrutura passa a conhecer sua rede e seus equipamentos, sabendo qual equipamento está sendo subutilizado e qual seus componentes de *hardware* e *software* estão instalados, uma vez

modificado qualquer um desses componentes o administrador é alertado, podendo tomar ações a fim de corrigir o problema.

Para a segurança esse é um passo importante, pode se dizer que é o primeiro passo que se deve tomar para se implementar corretamente um sistema gerenciador de segurança de *TI*, pois o conhecimento dos equipamentos e ativos torna o trabalho bem mais fácil.

Capítulo 6

Metodologias para análise de risco

Diversas metodologias [33] e interfaces de análise de risco surgiram para tentar reduzir o impacto de vulnerabilidades e conseqüentemente medir o risco atual. Este Capítulo discute os principais métodos [49] e práticas para análise de risco.

6.1 *OCTAVE - The Operationally Critical Threat, Asset, and Vulnerability Evaluation*

O sistema *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)* em português Avaliação de Vulnerabilidades e Ameaças em Ativos Operacionalmente Críticos, é um padrão desenvolvido que atua como *framework* para análise de risco, buscando preencher os requisitos definidos na *ISO 17799*[1].

Desenvolvida em 2003 pelo SEI (*Software Engineering Institute*) da Universidade *Carnegie Mellon* e patrocinado pelo Departamento de Defesa Americano (*DoD*), tem a tarefa de mitigar riscos de *TI* e de negócios.

Em [25], é apresentado um método chamado *OCTAVE*, onde uma equipe, chamada de equipe de análise, gerencia o processo de análise de toda a informação. Organizando ações diretas, tomando decisões de acordo com a situação. A metodologia é direcionada à análise de risco e pela utilização de práticas de segurança.

A sua implementação é fortemente dependente de uma equipe de coordenadores, que é chamada de equipe de análise, tendo a função de:

- Identificar os ativos que deverão ser monitorados e que sejam importantes para a organização;
- A análise de risco deve ter a visão direta para os ativos que são considerados mais críticos;

– Deve haver um relacionamento entre os ativos que são considerados críticos, quais ameaças esses ativos estão sujeitos e quais possíveis vulnerabilidades a que esses ativos estão sujeitos;

– Os riscos devem ser avaliados em decorrência da utilização dos ativos e sua importância para empresa, caso ocorra um comprometimento qual o impacto sobre o negócio;

– Desenvolver uma estratégia de ação visando melhorias da segurança, bem como um plano de controle e mitigação dos riscos.

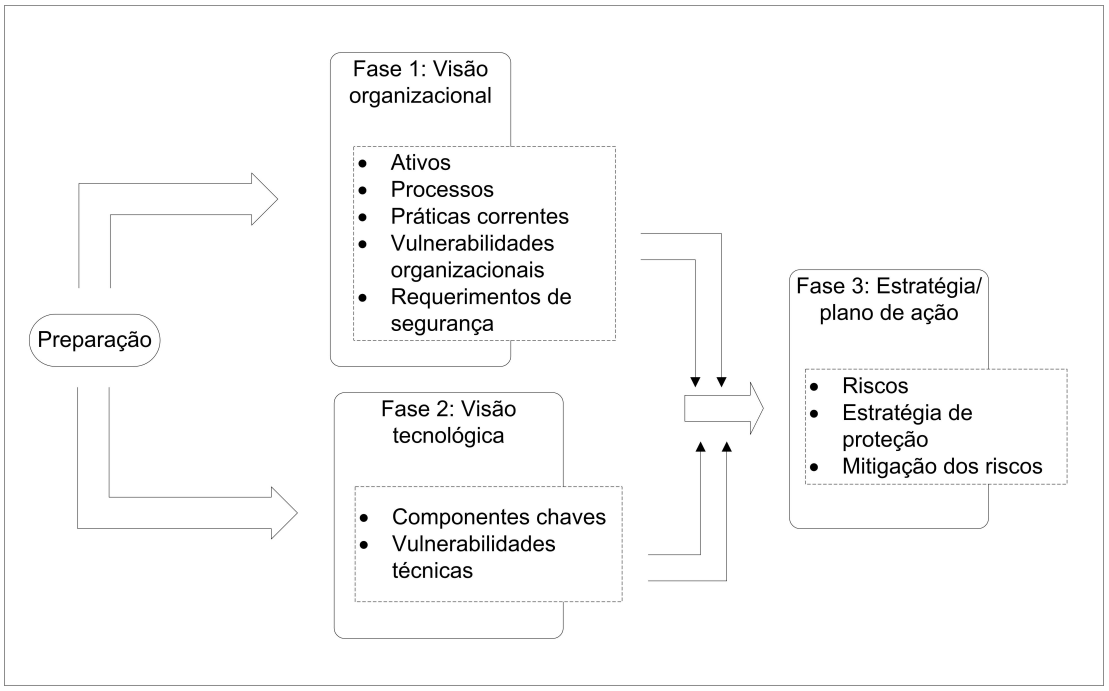

Figura 6.1: Processos do *OCTAVE*

O método tem três fases distintas, conforme Figura 6.1, cada uma definindo a posterior, são elas: Visão organizacional, visão tecnologia e estratégia/plano de ação. As duas primeiras fases servem de base para a terceira e última fase.

6.1.1 Visão organizacional

Todas as fases de implantação do *OCTAVE* são importantes e devem ser seguidas sempre com o foco na organização. Nesta fase inicial, devem ser obtidas informações sobre os ativos e identificadas as ameaças que possam vir a ocorrer com esses ativos. Deve ser criada uma equipe que irá levantar as informações necessárias para iniciar o processo, posteriormente esta mesma equipe deverá em relação aos ativos quais são mais importantes para a organização. Finalmente a equipe deverá identificar as ameaças que todos

os ativos, considerado importante, está sujeito, criando um relatório com essas informações, esse documento é chamado de *profile* e cada ativo deve ter um *profile*.

6.1.2 Visão tecnológica

Nesta fase de aplicação da metodologia *OCTAVE* deve se ter conhecimento da infra-estrutura tecnológica existente na organização para ser feita uma identificação das vulnerabilidades, sendo necessárias duas ações:

1. Identificar os componentes críticos: a partir de uma equipe montada para esse fim, devem ser identificados os ativos mais críticos, definindo a abordagem para a avaliação desses ativos.

2. Avaliar os componentes críticos: Devem ser utilizadas ferramentas que irão avaliar os ativos críticos do ponto de vista de vulnerabilidades. Nesta fase os resultados devem conter o relatório *profile* para cada ativo.

6.1.3 Estratégia e plano de ação

O principal objetivo de estratégia e plano de ação é verificar os riscos para os ativos mais críticos e conseqüentemente desenvolver um plano ou estratégia para proteção, neste ponto deve-se ter alguns processos a serem seguidos:

- Análise de risco: Conduzir um plano para análise de risco seguindo o impacto para a empresa, devendo determinar o índice de alto, médio e baixo para as ameaças e vulnerabilidades nos ativos.

- Estratégia de segurança: Desenvolver um plano de ação que vise a mitigar os riscos, buscando proteger os ativos baseados em métodos de melhores práticas, como as descritas em normas de segurança ISO/IEC 17799[1] e ISO 27001[40], por exemplo.

De acordo com o manual técnico do *OCTAVE* [2] em linhas gerais o método pode-se resumir nos seguintes tópicos:

- Construção de um perfil de ameaça: onde se deve conhecer a estrutura da rede e organização das informações;

- Identificação de vulnerabilidades: Nesta fase deve-se avaliar a infra-estrutura e levantar pontos de vulnerabilidades;

- Desenvolvimento de estratégia e plano de segurança: Esta fase pode ser considerada a mais importante, é onde será desenvolvido um plano de ação para a análise de risco.

O método *OCTAVE* relaciona-se tranqüilamente com o proposto pela norma ISO 17799, conforme mostra a Figura 6.2, buscando atuar principalmente na área de gestão, identificando os ativos, analisando as vulnerabilidades e planejando a melhoria da infra-estrutura, sempre considerando o processo e não o projeto, pois a segurança deve ser constantemente reavaliada, buscando-se inconsistências.

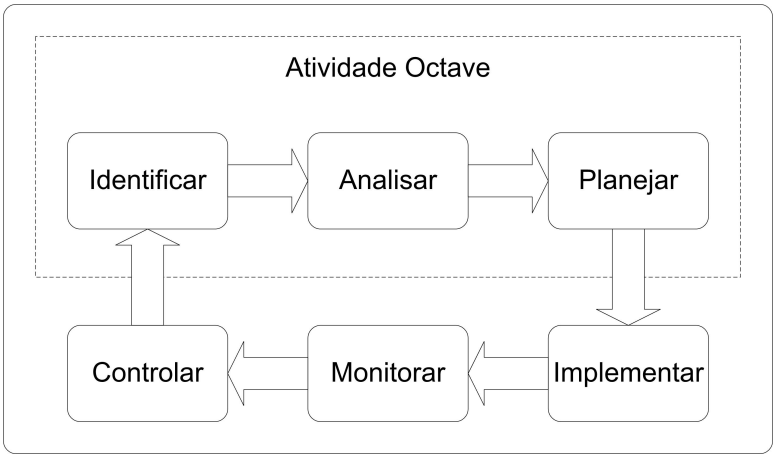

Figura 6.2: Relacionamento do *OCTAVE* com processo de segurança da informação

O ponto que torna o método difícil de aplicar é a necessidade de uma equipe exclusiva para a análise de informações/risco e conseqüente tomada de decisão.

6.2 *CORAS - Risk Assessment of Security Critical Systems*

O projeto *CORAS*[24] *(Risk Assessment of Security Critical Systems)* foi iniciado em janeiro de 2001 e completado em setembro de 2003 por um consórcio de várias empresas em países da Europa. O grupo técnico responsável pelo projeto é o *SINTEF (The Foundation for Scientific and Industrial Research)* do Instituto de Tecnologia da Noruega (*NTH)*, junto com a *Telenor*, responsável pela coordenação administrativa.

A metodologia *CORAS* suporta [42]:

- Uma metodologia para um modelo de análise de risco integrando aspectos complementares aos métodos de análise de risco e uma modelagem considerada *estado da arte*;
- Análise de risco baseada em uma especificação da linguagem *UML*;
- Uma ferramenta computacional que suporta a metodologia e provê dois repositórios: Um repositório de análise e um repositório de reuso das experiências adquiridas na análise;

- Utiliza dados em *XML* para a análise de risco;
- Um relatório de análise das vulnerabilidades.

O *Framework CORAS* é estruturado em quatro partes:

1. Terminologia: Define importantes conceitos e termos para a segurança, análise de risco e documentação do sistema;
2. Biblioteca: É dividida em entidades, estrutura de armazenamento e sistemas de classificação;
3. Metodologia: Consiste em técnicas de análise de risco, processos e linguagens;
4. Ferramenta: Provê suporte para performance na análise de risco de acordo com a metodologia, é uma ferramenta computacional.

6.3 Sistema AGRIS

O Projeto AGRIS [16] (Análise e Gerência de Risco em Segurança) é um trabalho desenvolvido no núcleo de computação da universidade federal do Rio de Janeiro, o objetivo deste projeto é criar uma ferramenta de suporte à segurança da informação sendo capaz de identificar ameaças, vulnerabilidades e impactos ao negócio gerando como respostas relatórios técnicos e gerenciais.

As principais funcionalidades da ferramenta AGRIS são:

- Visualização por ativos: É possível ter uma visão do ativo que está sendo analisado de maneira individual, permitindo a verificação de vulnerabilidades para um item em específico;
- Definição do valor do ativo: Um ativo pode ter um valor alto para uma empresa, mas em outra, mesmo do mesmo segmento, ter um valor menor ou inexpressivo, por isso deve ser possível alterar os valores de maneira individualizados;
- Definição de políticas por ativos: É importante que a ferramenta permita a definição de políticas diferenciadas para cada ativo;
- Uso de *templates*: Visando a facilidade de uso os autores propuseram a criação de *templates* que permitam uma rápida utilização;
- *Benchmarks* e conformidade: Segundo os autores a ferramenta permite uma comparação através de *benchmarks* entre outras empresas, entre o momento atual e o momento anterior, com empresas de setores diferentes ou com algum modelo de prestabelecido.

– Relatórios: Produção de relatórios técnicos para os profissionais de *TI*, produzindo informações sobre os ativos e o nível de exposição ao risco. Relatórios empresariais com informações destinadas aos empresários e administradores com o custo/benefício da implementação de controles e gasto com a segurança/retorno obtido.

– Controle e correção de falhas: Integrar a ferramenta *AGRIS* com ferramentas de análise de vulnerabilidades permitindo uma verificação dos controles e das vulnerabilidades encontradas. Nesta fase a ferramenta deve disponibilizar as informações dos riscos encontrados permitindo um mecanismo associar com documentos informativos sobre o problema e sua correção. É previsto também que se algum risco for identificado e não houver um documento para sua correção, o mesmo deve ser cadastrado. As informações devem estar sendo sincronizadas em um servidor central. Deve existir um plano para a mitigação dos riscos sendo estabelecida uma correlação entre os investimentos e os riscos mitigados.

6.3.1 Estrutura do *AGRIS*

A ferramenta AGRIS é formada por três blocos principais: inicialização, processamento e gerenciamento (Figura 6.3).

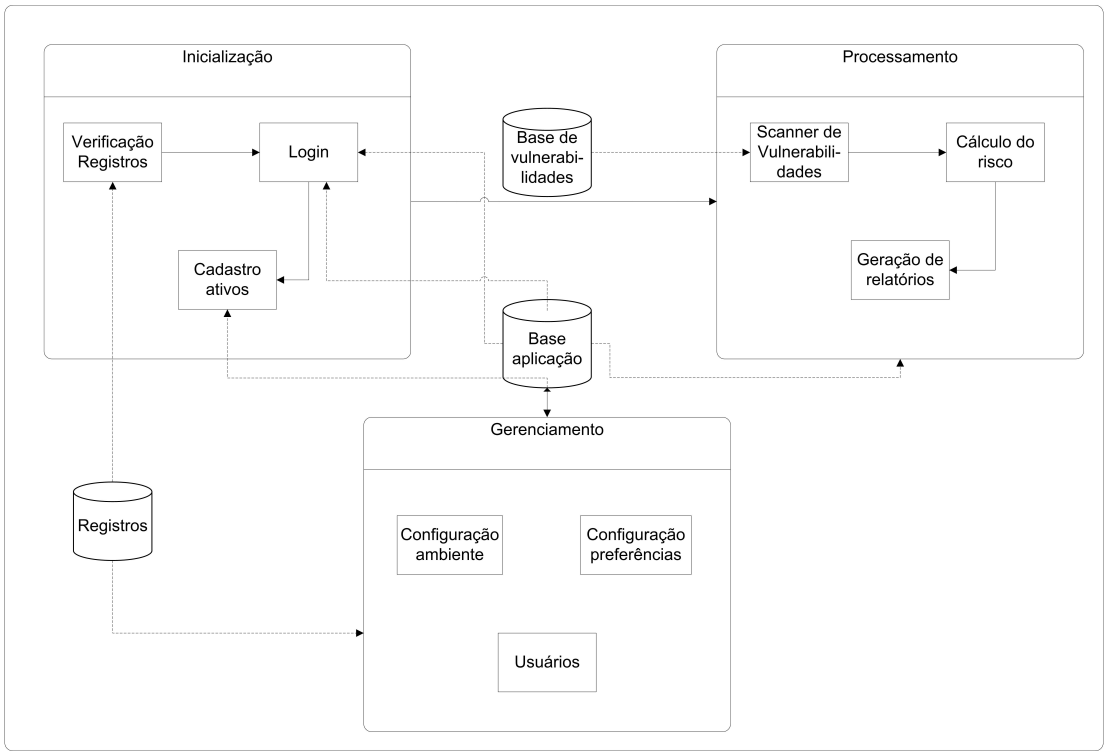

Figura 6.3: Estrutura do *AGRIS*

– Inicialização valida o usuário permitindo a execução da ferramenta, permitindo o cadastramento de novos ativos, permite a verificação da integridade das bases de dados;

– Processamento verifica os controles existentes, bem como carrega as bases de vulnerabilidades, calcula o risco e gera gráficos, permite *compliance* com normas de segurança, realiza os *benchmarks* e gera os relatórios técnicos e gerenciais;

– Gerenciamento, administra as conFigurações, vulnerabilidades, usuários e permissões da ferramenta.

6.3.2 Método para análise de risco utilizado pelo *AGRIS*

O método utilizado é baseado no *CRAMM (Government's Risk Analysis and Management Method)*[14] que é um *framework* desenvolvido pela *CCTA (Central Computer and Telecommunications Agency)*. Originalmente foi desenvolvido nos anos 80 e é um método popular na Inglaterra.

O método trabalha focando na segurança da informação e mitigação dos riscos identificando os ativos e seus valores e requerimento de segurança depois recomendando soluções. No entanto, esse método é geralmente avaliado pela necessidade de qualificação e experiência dos usuários da ferramenta para um bom resultado. Possui dependência entre o risco, ameaças e vulnerabilidades, calculando-se o produto destas variáveis a valores quanto a relevância do ativo e a probabilidade de exploração.

Atualmente está na versão 5.1, que foi lançada em 2005, nesta nova versão foi atualizada buscando implementar recomendações da norma de segurança *BS 7799*[9].

6.4 Estudo comparativo entre metodologias propostas

As metodologias mostradas neste trabalho são as que estão em maior evidência, por diversos motivos como: serem livres e portáveis entre diversas áreas.

O que tem trazido interesse de empresas e acadêmicos neste assunto é a diversidade de problemas a serem resolvidos. No Brasil temos um excelente trabalho desenvolvido pelo Núcleo De Computação Eletrônica da Universidade Federal do Rio De Janeiro, o AGRIS [16].

Sistemas bastante conhecidos como o *CORAS*, desenvolvido por um consórcio de empresas Européias, é distribuído livremente com a licença *LGPL (Library or Lesser General Public License)* através do endereço eletrônico `http://sourceforge.net/projects/coras`.

O sistema *OCTAVE* foi desenvolvido pela *Carnegie Mellon University*, bastante robusto e patrocinado pelo *CERT* Americano, no endereço `http://www.cert.org/octave/`.

Gestão de risco utilizando o *CVSS*, provê uma série de vantagens[46], como cálculo do risco geral da organização, nível de ameaça, priorização de ações, possibilidades de desenvolvimento de aplicações complexas, utilizando a base de conhecimentos de vulnerabilidades e cálculo de risco do CVSS, entre outros.

Tabela 6.1: Tabela comparativa entre metodologias para análise de risco

Descrição	***AGRIS***	***CVSS***	***CORAS***	***OCTAVE***
Local de origem	Brasil	USA	Consórcio Europeu	USA
Método adaptável à realidade de cada organização	Sim	Sim	Sim	Sim
Possui aplicativo ou ferramenta	Sim	Não	Sim	Sim
Possui atualização da base de conhecimento sobre vulnerabilidades	Depende de outros aplicativos	Sim	Não	Não
Método utilizado para cálculo do risco	*CRAMM*	Próprio	*CRAMM*	*OCTAVE criteria*
Busca por vulnerabilidade	Sim	Sim	Sim	Não
Utiliza informações do *CVE*	Não	Sim	Não	Não

A tabela 6.1 traz um estudo comparativo entre as metodologias de análise e gestão de risco, contendo informações consideradas importantes para implementação de um sistema robusto que subsidie a área de gestão de segurança para tomada de decisão e priorização de ações para tratamento do risco.

A existência de aplicativos e ferramentas é prioritária para gestão de risco, pois caso a metodologia necessite de implementação manual pode acabar caindo no esquecimento.

Pode-se dizer que toda organização tem um ambiente de *TI* diferente, atendendo necessidades diferentes, por esse motivo é necessário que a metodologia para gestão de risco possa sofrer mudanças sem a necessidade de alteração de códigos.

O método para elaboração de cálculo de risco é de suma importância para se conhecer o valor do risco que uma organização está sujeita, no entanto,

não é necessário que seja complexo, e sim que permita a visualização do nível de risco da organização.

Vulnerabilidades surgem constantemente, mesmo sistemas exaustivamente testados estão sujeitos a brechas, a metodologia deve prever que isso ocorra e ter ferramentas para atualizações, buscando ser independente de um terceiro, para atualização dessa base.

O *CVE* foi criado em 1996, conforme discutido no Capítulo 5.2, e surgiu como necessidade para se padronizar a divulgação de informações sobre vulnerabilidade, portanto torna-se um item que deve ser considerado em uma metodologia para gestão de risco.

Capítulo 7

Metodologia Proposta

7.1 Descrição

O *framework* para avaliação de risco irá integrar a metodologia com o a ferramenta desenvolvida, permitindo que a informação seja apresentada de maneira clara, facilitando a condução das respostas e controles de risco das vulnerabilidades detectadas, priorizando as respostas.

A proposta deste trabalho é a criação de uma metodologia para gestão de risco, executando os passos de tratamento e apresentação de dados sobre vulnerabilidades, correlacionando os eventos com informações obtidas em uma rede interna, permitindo atuar em tempo real sobre o ambiente de *TI* considerado, calculando um risco para cada vulnerabilidade encontrada. Também faz parte da proposta o desenvolvimento de ferramenta capaz de executar os processos propostos na metodologia.

7.1.1 Modelagem e requisitos considerados

A ferramenta desenvolvida para este projeto deve identificar os componentes de rede e armazenar diversas informações que além de identificar o equipamento, através do agente *CACIC*, deve registrar todos os softwares instalados e suas respectivas versões.

As informações sobre vulnerabilidades são liberadas constantementes por diversos órgãos que tratam a segurança da informação, a base de dados, tanto de vulnerabilidades quanto de inventário, deverá ser atualizada e mantida pelo gestor da aplicação local.

De posse das informações sobre os produtos internos e vulnerabilidades é calculado o *score risk* para cada produto registrado. Os responsáveis pelos ativos que serão monitorados devem, diariamente, acessar listagem atualizada de vulnerabilidades de seu interesse e registrar os históricos relacionados com a condução da regularização da vulnerabilidade.

Para criar a base de produtos da instituição será utilizado uma metodologia de coleta de dados e inventário de rede, onde deverá conter, em cada

equipamento monitorado, um cliente para coleta das informações e conseqüentemente o envio para um servidor. Todo o tráfego das informações será criptografado, garantindo o sigilo das informações em trânsito pela rede.

Todos os requistos considerados fazem parte do anexo D no capítulo 9.4.

7.1.2 Casos de uso

Foi criado um diagrama de caso de uso contendo duas visões: A visão por parte do gestor (Figura 7.1), e a visão por parte do usuário (Figura 7.2).

Todos os casos de uso estão listados no anexo E - Especificação de Caso de Uso no capítulo 9.5.

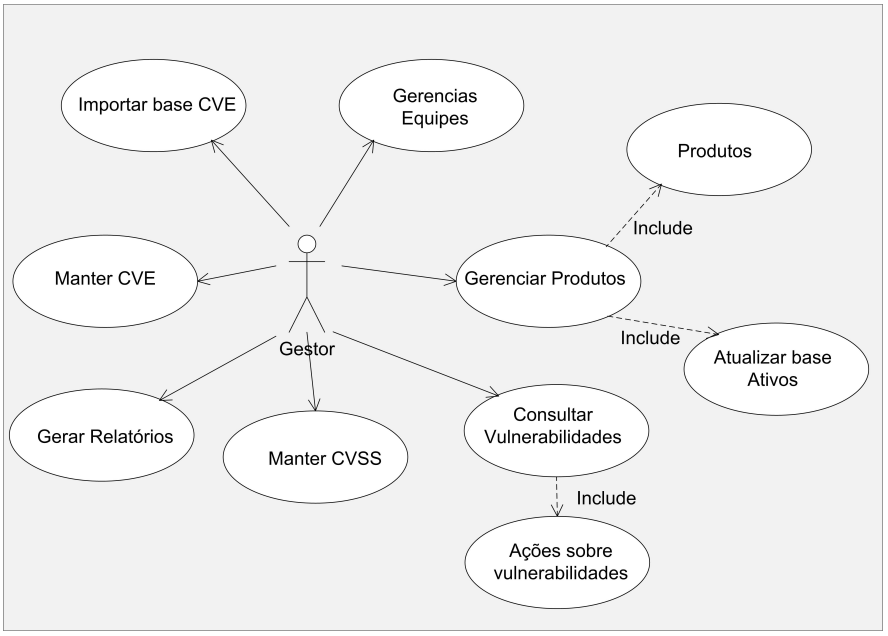

Figura 7.1: Diagrama de caso de uso - Gestor

Não é possível que o usuário veja ou acesse a visão do gestor, no entanto, o gestor tem a visão total do sistema. A idéia é ter várias equipes vinculadas com visões diferentes para cada usuário.

As bases de dados *CVSS* e *CVE* descritas neste trabalho servirão para popular um banco de dados interno, gerando uma base de vulnerabilidades, essas informações serão cruzadas com os dados de *software* e *hardware* coletados em uma rede interna, gerando a base com o conteúdo:

- *IP*[1] da máquina na rede;
- Versão de *softwares* instalados;

[1]Internet Protocol

– Informações sobre usuários logados no domínio;

– Tipo de sistema operacional;

– Informações sobre *hardware* (memória, processador, Hard disk).

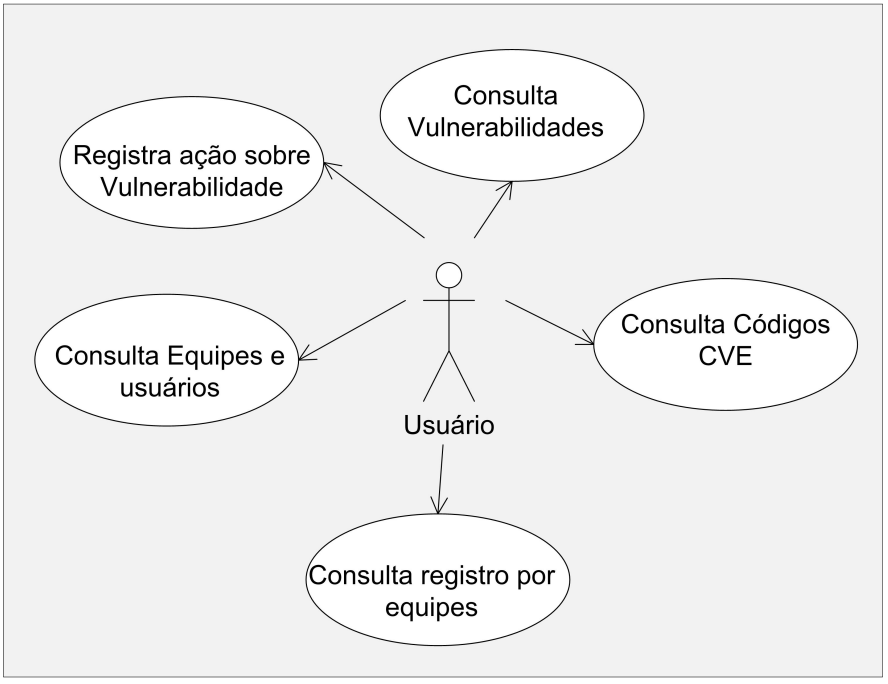

Figura 7.2: Diagrama de caso de uso - Usuário

A base de dados gerada através da coleta de informações internas será denominada inventário.

Conforme a Figura 7.3 o diagrama demonstra a interligação e correlação das informações, sendo que a base *CVSS* e *CVE* é alimentada por organizações externas. A base de inventário é mantida pela entidade interna. Para que o procedimento seja eficiente todas as máquinas que compõem a rede da organização deverão ter instalado o *software* de inventário que irá alimentar a base interna.

É importante que a organização tenha normas de segurança e políticas de utilização de *software* e *hardware*, caso não exista uma política consolidada deverá pelo menos ser criada uma norma de conduta e utilização dos ativos por parte dos usuários.

A princípio a norma deverá conter informações sobre:

– Instalação utilização de *software* não homologados pela instituição, de modo que impeça o usuário a instalar qualquer sistema que não conste no catalogo interno, com isso evitando instalações até mesmo de *software* sem licença;

– Termo de responsabilidade de utilização dos ativos tecnológicos, explicitando sua utilização apenas para fins diretos do negócio;

– Metodologia para utilização de ativos móveis (notebooks, PDA's, etc) sendo vetada a utilização de equipamentos externos, ou seja, que não faça parte dos ativos próprios;

– Criação de métodos para instalação de novos ativos, sendo que qualquer equipamento ligado à rede deverá ter o *software* de inventário instalado.

– Criação de procedimentos de *logins* de usuários na rede, protegendo contra conexões espúrias, de modo que apenas ativos com o *software* de inventário serão permitidos no ambiente local;

– Por fim uma política de divulgação do projeto de modo que o maior número de pessoas possam conhecer e conseqüentemente apoiar.

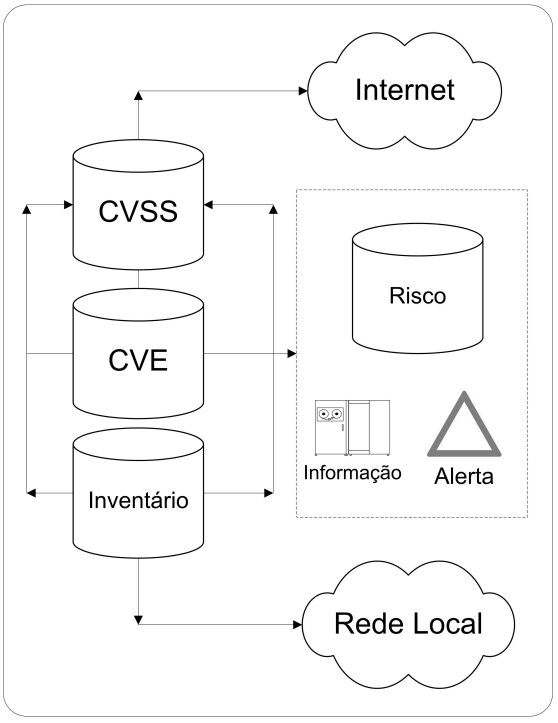

Figura 7.3: Modelagem de infra-estrutura de risco

7.2 Visão integrada do *Framework*

A escolha por uma plataforma livre, simples e ao mesmo tempo robusta, baseou-se na grande aceitação pela comunidade acadêmica e empresarial da padronização proposta pelo *NIST* na metodologia *CVSS* e *CVE*.

Informações são coletadas internamente pela ferramenta *CACIC*, que deve estar rodando na máquina monitorada. Os dados coletados são então enviados para o banco de dados *CACIC*, conforme Figura 7.4.

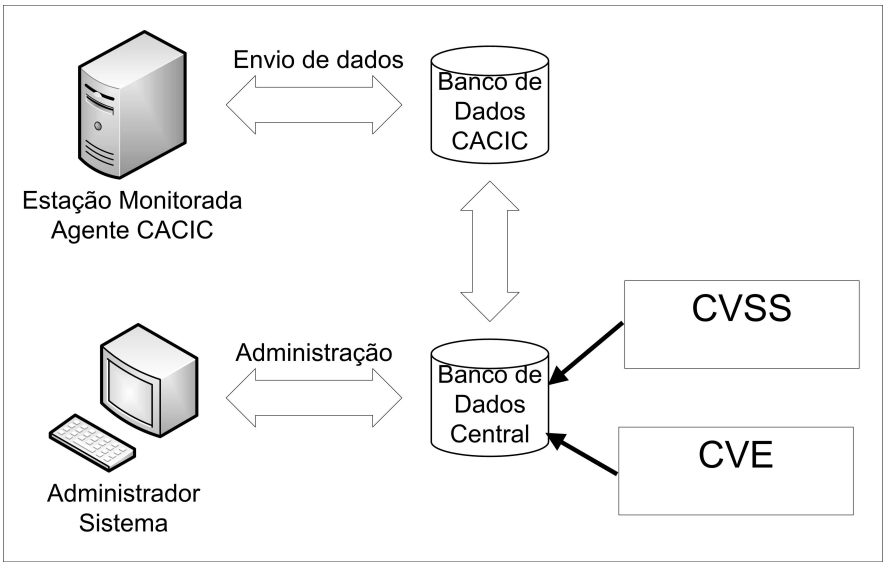

Figura 7.4: Visão conexão e envio de dados

Para facilitar a atualização da ferramenta *CACIC*, tomou-se por base a integração da base de dados central, sem efetuar alterações nas tabelas da base *CACIC*. É nesta base de dados que o *CVSS* e *CVE* deve ser integrado, sendo as informações coletadas externamente e inseridas de maneira semi automatizada, ou mesmo automatizada.

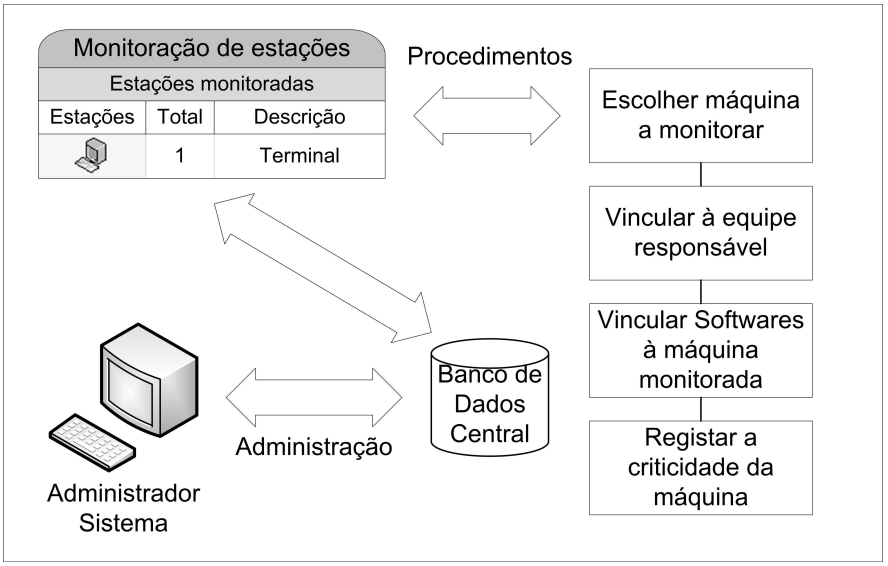

Figura 7.5: Gerenciamento das informações

O administrador poderá controlar todo o sistema podendo intervir na execução das rotinas de importação da base *CVSS* e *CVE*, bem como a monitoração.

Todo o gerenciamento é feito através da estação administrador, conforme Figura 7.5.

Esta etapa é muito importante, pois o administrador deverá seguir os passos:

1. Acessar a ferramenta e escolher a estação que será monitorada;
2. Vincular a estação escolhida a uma equipe, que deverá estar previamente cadastrada, conforme estudo de caso UC05 - Manter equipes;
3. A lista de *softwares* instalados na máquina monitorada será apresentada, para que o administrador marque quais deverão ser monitorados. Essa escolha se deve ao fato de que nem tudo instalado é utilizado;
4. Na interface da ferramenta, será apresentada a lista de criaticidade da máquina monitorada, pois uma máquina idêntica pode ter criticidades e valores diferentes para a organização, para isso deve ser seguida o contido na tabela 7.1.

Tabela 7.1: Nível de criticidade

Criticidade	**Score**
Irrelevante	1.0
Relevante	2.0
Importante	3.0
Crítico	4.0
Vital	5.0

Com todas as informações coletadas deve-se rever a pontuação gerada automaticamente e classificar os ativos considerados críticos, utilizando a Tabela 7.1, dessa maneira obtêm-se informações sobre quais ativos têm maior impacto, caso estes sejam comprometidos, tanto por problemas físicos quanto lógico. Foi criado um fluxo (Figura 7.6), onde são descritos os passos necessários para a coleta e cálculo do risco.

O *Framework* integrado com a metodologia, através da ferramenta proposta, poderá auxiliar com as seguintes informações:

1. Determinar o valor dos ativos de informação bem com a sua criticidade para a corporação;
2. Estimar uma determinada probabilidade de uma ameaça poder ocorrer e possibilitar o cálculo do custo;
3. Identificar pontos vulneráveis e subsidiar decisões para contornar ou diminuir o risco;
4. Permitir a criação de estratégia para mitigar os riscos;
5. Possibilitar a correta identificação dos ativos.

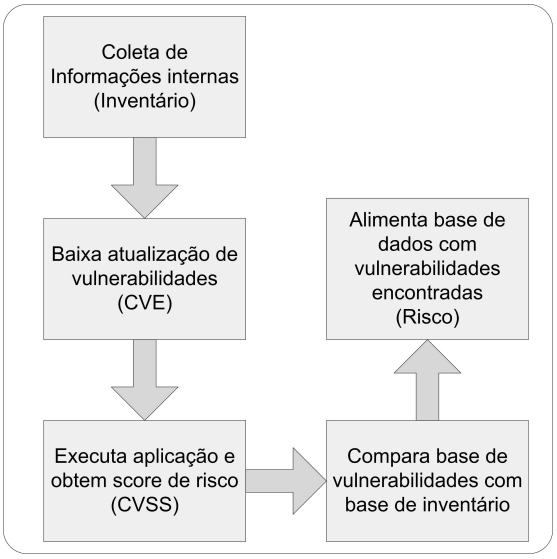

Figura 7.6: Procedimentos de coleta de informações

7.3 Ferramentas para análise e gestão de risco

As ferramentas para análise e gestão de risco não são novidade, já vêm sendo desenvolvidas a pelo menos duas décadas, no entanto, sua utilização vem crescendo, por diversos motivos, como a necessidade, por parte das organizações, em atender requisitos legais como acordo de *Basiléia* [3] e *Sarbanes-Oxley* [43].

7.3.1 *Visual Assurance*

Desenvolvida pela *Kilclare Software*[2], esta ferramenta para gestão de risco tem a função de avaliar, monitorar e informar sobre riscos identificados, armazenando as informações em banco de dados *Oracle* ou *MsSQL*.

Utiliza templates (atualmente mais de 90), como por exemplo o template *SOX*, que possui bibliotecas e *checklists* com informações para atendimento ao *Sarbanes-Oxley*, contendo ações a serem executadas onde busca vincular um ativo analisado a base de conhecimentos que dispõe como manuais, tutoriais ou outros documentos.

7.3.2 *Compliance Guardian*

Desenvolvida pela *Ernest & Young*[3], esta ferramenta tem seu acesso feito via *webserver*. Os objetivos da ferramenta são o desenvolvimento da gestão de risco em *TI* e a verificação de conformidades existentes no mercado.

[2]http://www.kilclare.com/ acessado em 01/01/2008
[3]http://www.eyware.com/ acessado em 01/01/2008

No entanto a ferramenta não permite a classificação dos ativos, o plano de ação é fortemente dependente do conhecimento da equipe, não permite a identificação e inserção de informações sobre vulnerabilidades. Caso ocorra alterações no ambiente de *TI*, a ferramenta peca por não identificar.

7.3.3 *Ecora*

As ferramentas produzidas pela empresa *Ecora*[4] buscam integrar áreas como gestão de mudanças e configuração, gestão de segurança e documentação. divididas em três tipos principais de *software*:

- *Ecora Enterprise Auditor*: Responsável por gestão de configurações;
- *Ecora Patch Manager*: Trata-se de um sistema de atualização de *patch* apenas para equipamentos com o sistema operacional *Windows*;
- *Ecora DeviceLock*: Utiliza-se de políticas de restrição e controle de uso para *drives*.

As ferramentas da *Ecora* permitem a identificação de ativos de *TI* e emitem relatórios sobre vulnerabilidades, também coleta informações sobre ativos, sendo fortemente dependente do sistema operacional Windows. Suas informações sobre vulnerabilidade encontradas restringem apenas para as que possuem o *patch*, não possuindo um plano de ação para a correção dos problemas.

7.3.4 *Risk Manager*

Ferramenta para gestão de risco desenvolvida pela empresa brasileira *Módulo* [5]. Trabalha com o conceito de *checklists* para cada ativo identificado. Não possuem ferramenta para coleta de informações sobre o ativo, no entanto, importa a base de dados de outras ferramentas para gestão de ativos.

Possui diversos módulos para atendimento de *compliance* e gestão de segurança, como *ISO 27001, COBIT, Basiléia*, entre outros.

Emite relatórios tanto gerenciais quanto técnicos.

O acompanhamento da análise é feita através de um *framework* onde cada ativo tem relacionado a si um *checklist* que deve ser atendido.

Mostra a situação anterior à análise e a atual, podendo acompanhar a evolução do tratamento dos riscos.

A ferramenta não efetua identificação de vulnerabilidades em tempo real, sendo fortemente dependente de atualização da base de conhecimento por parte do desenvolvedor da ferramenta *Risk Manager*.

[4]http://www.ecora.com/ acessado em 01/01/2008
[5]http://www.moduloriskmanager.com.br/, acessado em 01/01/2008

7.4 Estudo comparativo com outras ferramentas para análise de risco em *TI*

Para efeito de comparativo, chamamos a ferramenta de *Vulner* proposta por este trabalho, no entanto, a idéia inicial do trabalho era a criação de metodologias, a ferramenta faz parte do amadurecimento e aplicabilidade da metodologia, mostrando-se eficiente em comparação com outras metodologias.

Tabela 7.2: Comparação com principais ferramentas para análise e gestão de risco

Propriedades	**Visual Assurance**	**Compliance Guardian**	**Ecora**	**Risk Manager**	**Vulner**
Visualização por ativos	Sim	Sim	Sim	Sim	Sim
Definição do valor do ativo	Não	Não	Não	Não	Sim
Definição de políticas por ativo	Sim	Não	Não	Sim	Sim
Uso de templates	Não	Não	Sim	Não	Não
Conformidade	Não	Não	Não	Não	Não
Relatórios gerenciais	Sim	Sim	Não	Sim	Sim
Relatórios técnicos	Sim	Sim	Sim	Sim	Sim
Controle de correções	Não	Não	Não	Não	Sim
Suporte a sistemas heterogêneos	Não	Sim	Sim	Não	Sim
Associação do risco a base de conhecimento	Sim	Não	Não	Sim	Sim
Atualização da base de conhecimento	Sim	Indefinido	Não	Sim	Sim

Neste trabalho buscou-se um aperfeiçoamento das metodologias existentes bem como as ferramentas que as aplicam, portanto montou-se um comparativo [16] [59] com as principais ferramentas existentes (ver tabela 7.2) com a proposta deste trabalho.

Nesse comparativo, é claro, há grandes semelhanças entre as ferramentas, buscou-se implementar o que todas as ferramentas tem de melhor. No entanto, o principal foco desse trabalho não é apenas a ferramenta, e sim a metodologia a se seguir.

Na visualização por ativos é possível ter uma visão do ativo que está sendo analisado de maneira individual, permitindo a verificação de vulnerabilidades para um item em específico.

A definição do valor do ativo leva em consideração o impacto e necessidade do ativo para uma empresa, que em alguns casos pode ser alto para um ativo em uma determinada empresa, mas em outra organização, mesmo do

mesmo segmento, ter um valor menor ou inexpressivo, por isso deve ser possível alterar os valores de maneira individualizados.

Uso de *templates* tem como objetivo a facilidade de uso com a criação de *templates* que permitam uma rápida utilização.

A segurança da informação busca a qualidade e atender conformidades de melhores práticas como o caso da *ISO 27001*, discutido no capítulo 3. Neste caso, permite uma comparação através de *benchmarks* entre outras empresas, entre o momento atual e o momento anterior, com empresas de setores diferentes ou com algum modelo prestabelecido.

Os relatórios são ferramentas indispensáveis, tanto para que o processo de segurança seja bem visto pela administração da empresa quanto para o controle e entendimento pelo corpo técnico. A produção de relatórios técnicos para os profissionais de *TI*, produzindo informações sobre os ativos e o nível de exposição ao risco e os relatórios empresariais com informações destinadas aos empresários e administradores com o custo/benefício da implementação de controles e gasto com a segurança/retorno obtido.

7.5 Demonstração da ferramenta

No desenvolvimento da ferramenta utilizou-se como base a linguagem *JAVA*, banco de dados *MySQL* encontrado em `www.mysql.org` na versão 5.0.45 em um sistema *Linux* com distribuição *Slackware 12.0* encontrado em `www.slackware.com`.

Conforme mostrado na Figura 7.1 a visão deve ficar restrita ao gestor, sendo que este tem todo o controle do sistema e conhece o quê todas as equipes estão conduzindo, podendo interferir, repassar, e acompanhar toda a situação (Figura 7.7), descrito no caso de uso UC10 - Gerar relatório principal no Anexo E.

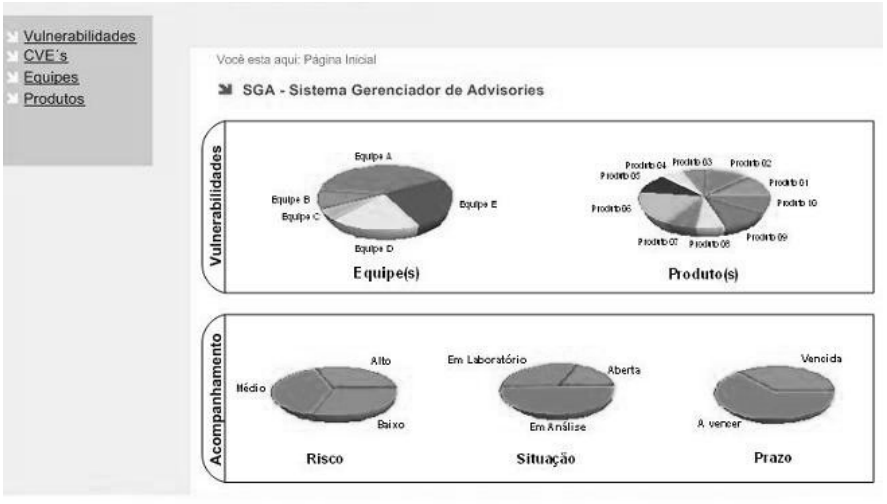

Figura 7.7: Visão do sistema - Gestor

Nesta situação ocorre a necessidade de um controle efetivo, pois em alguns casos a correção de uma vulnerabilidade pode causar mais problemas que a própria ameaça em si. Para este caso sugere-se a inclusão de três situações: Em laboratório, em análise e aberta.

- Aberta: Esta situação envolve a detecção de uma vulnerabilidade, que já foi direcionada a equipe responsável, no entanto, ainda não foi tratada.
- Análise: Uma equipe foi designada para análise, no entanto, nenhuma ação foi tomada, nesta fase ocorre o estudo do problema propriamente dito.
- Laboratório: Neste caso foi identificada uma vulnerabilidade, uma equipe está responsável, o estudo foi efetuado e uma correção sugerida, no entanto, todo o procedimento está em teste antes de ser aplicado em ambiente de produção.

Cada equipe pode ficar responsável por um ou vários *softwares* específicos, assim como equipamentos, chamados aqui de produtos.

No momento do tratamento da vulnerabilidade, deve-se implantar um prazo para correção, por esse motivo um controle sobre prazos deve ser implementado. Quanto mais crítico o ativo ou a vulnerabilidade menor o prazo para sua correção, claro que isso deve ser utilizado com moderação, nem sempre uma ameaça deve ser tratada como prioridade alta, em alguns casos pode ser que uma ameaça com menor risco externamente deva ser tratado como risco alto internamente, pois pode afetar ativos críticos para a organização.

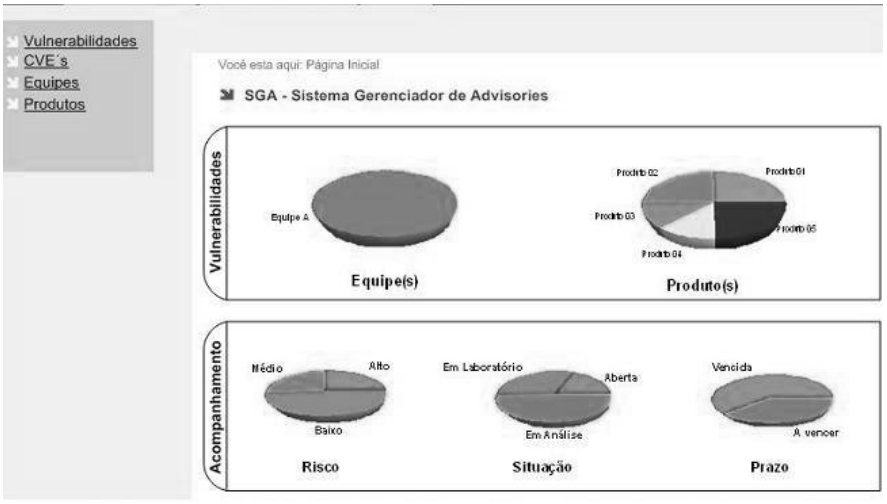

Figura 7.8: Visão do sistema - usuário de equipe

Para a visão da equipe, tem-se todo o controle apenas do que está sob sua condução, não podendo uma equipe ter a visão de outra equipe, mas

pode incorrer de um usuário fazer parte de várias equipes, neste caso terá a visão de mais de uma equipe (Figura 7.8), descrito no caso de uso UC15 - Consultar Relatórios da Equipe no Anexo E.

As Figuras são semelhantes, pois se busca a facilidade na visualização, tanto para o gestor, quanto para as equipes e seus usuários.

As telas mostradas nas Figuras 7.7 e 7.8 constam em seus gráficos sensíveis, podendo chegar às informações detalhadas dos produtos (*softwares* e equipamentos), como: Código *CVE*, cálculo *CVSS*, data da descoberta da vulnerabilidade, data da publicação da vulnerabilidade, descrição da vulnerabilidade, e links sobre a ameaça, e que em alguns casos recomendam os procedimentos para correção, ver Figura 7.9, descrito no caso de uso UC07 - Manter *CVE* no Anexo E.

Figura 7.9: Detalhamento de informações - vulnerabilidades

Após a correção do problema, a ferramenta deve permitir armazenar informações sobre a vulnerabilidade, equipe responsável, *software* afetado, código *CVE*, a descrição obtida pela divulgação do *NIST* pelo *CVE*, assim como os procedimentos adotados para correção do problema no momento do fechamento, ver Figura 7.10, descrito no caso de uso UC09 em Anexo E.

Caso a ocorrência seja fechada de maneira que não seja corrigida a vulnerabilidade, na próxima rodada da ferramenta, irá se detectar que ainda existe a vulnerabilidade, e será aberta uma nova solicitação para a equipe responsável, com isso busca-se que não seja efetuada nenhuma tentativa de *mascarar* o problema por parte das pessoas envolvidas.

Pode acontecer que o gestor busque que toda a rede seja atualizada, neste caso uma solicitação geral deve ser feita, e no caso de uma atualização em massa seja feita na próxima rodada da ferramenta todas as vulnerabilidades não encontradas serão fechadas automaticamente.

Deve-se atentar que, em alguns casos, a correção pode causar mais estragos do que a própria vulnerabilidade, haja vista que é de conhecimento que algumas atualizações podem causar paralisação de *softwares* e *hardware*, e

Figura 7.10: Relatar ação - Acompanhamento de vulnerabilidades

para ativos considerados críticos é recomendado testes em laboratório antes da aplicação da correção em ambiente de produção.

Nesta fase a ferramenta calcula um risco, expõe a vulnerabilidade e em alguns casos, quando disponível, recomenda os procedimentos para correção, sendo bastante eficiente para um controle da infra-estrutura e seus riscos associados.

Capítulo 8

Conclusão e trabalhos futuros

A segurança é uma prioridade dos sistemas, é neste contexto que se deve fazer referência a alguns princípios discutidos neste trabalho, que são: identificar os recursos ou ativos, avaliar os riscos desses ativos e por fim desenvolver possíveis contramedidas buscando mitigar os riscos.

As contramedidas devem ser preventivas e ao mesmo tempo reativa, sendo compostas por regras e respostas baseadas em conhecimento prévio.

As leis em alguns países estão sendo adaptadas buscando dar maior transparência às operações das empresas. Com essa clareza os empresários e pequenos acionistas poderão fazer seus investimentos com maior segurança.

Nos últimos anos foram investidos valores consideráveis para obtenção de equipamentos e soluções de segurança, como sistemas de detecção de intrusos, antivírus, *firewalls*, *anti-spam*. Mas como realmente saber se esses investimentos tiveram o retorno esperado? As informações geradas por essas soluções muitas vezes são ignoradas, ou quando tratadas pouco auxiliam na gestão da informação. É nesse ponto que a gestão de risco vem ao auxílio, consolidando os dados coletados e tornando-os informações utilizáveis.

A metodologia proposta nesse trabalho depende de vários fatores, o principal, e recomendado pelas normas de segurança *ISO 27001* e *ISO 17799*, é a aceitação da idéia por parte dos gestores de que o investimento em segurança da informação é algo que trará retorno.

Outro fator relevante é de que se conhecerá a infra-estrutura geral de *TI*, permitindo que a organização possa elaborar um plano de ação para o tratamento e análise de risco, buscando a conseqüente mitigação ou eliminação dos riscos.

A ferramenta aqui proposta deverá, a princípio, ser de caráter informativo, subsidiando o gestor de informações sobre sua própria base, aplicando-se regras fundamentais da arte da guerra[1]

- Se conheceres a si próprio terás chances de vitória;

[1]Sun Tzu - A arte da Guerra

– Se conheceres a si próprio e a seu inimigo terás a vitória;

– Se não conheceres nem a si e nem o seu inimigo a derrota será certa.

O fato é que não é possível um gerenciamento eficiente de risco se não for possível identificá-lo, pois o risco ocorre tendo como premissa a incerteza, caso não exista incerteza não existe risco. É neste contexto que o trabalho foi desenvolvido, visando reduzir as variáveis de incerteza concomitantemente reduzindo o risco.

Através de agentes coletando as informações em tempo real e alimentando a base de dados sobre os ativos monitorados pretende-se conhecer a infra-estrutura e conseqüentemente suas ameaças e vulnerabilidades.

Uma base de dados centralizada, obtendo as informações sobre vulnerabilidades em centros renomados de segurança, aplicando-se a busca se a vulnerabilidade divulgada afeta ou não a infra-estrutura testada, apresenta-se como um procedimento menos invasivo que os propostos por outras metodologias [25][16][17].

A metodologia proposta se mostrou eficiente no controle dos ativos e levantamento das vulnerabilidades relacionadas a este ativo, no entanto, houve uma preocupação pelo número de vulnerabilidades e ativos podendo chegar a milhares, devido a isso considerou utilizar a vinculação de ativos críticos, diminuindo o número inicial e direcionando o foco a ativos considerados indispensáveis.

Em trabalhos futuros esta metodologia pode ser aplicada em uma infra-estrutura buscando a localização da ameaça e suas vulnerabilidades e correção automática, ou seja, uma determinada vulnerabilidade pode ser corrigida no mesmo momento que é divulgada sua correção. Dependendo de alguns fatores como:

– Uma correção esteja disponível no momento da liberação da informação sobre a vulnerabilidade;

– A infra-estrutura esteja totalmente mapeada;

– Novos equipamentos devem passar pela liberação da equipe de segurança e com o agente coletor instalado;

– A vulnerabilidade seja conhecida;

Na mesma pesquisa pode-se utilizar de co-relacionamentos de *logs* e acessos de usuários, onde o acompanhamento das ações da rede e dos seus usuários seja totalmente monitorada, e caso alguma anomalia seja detectada o *framework* pode registrar uma ação preventiva, alertando os administradores sobre a ocorrência.

Esta ferramenta está em versão *beta*, ou seja, em desenvolvimento, e uma contribuição no sentido de se implementar testes de maior abrangência qualificariam esta pesquisa.

Apesar da metodologia estar fortemente ligada ao *CVE*, em trabalhos futuros é recomendado a diversificação de utilização de bases de informações sobre vulnerabilidades.

Pode-se trabalhar na implantação de controles buscando certificação em normas como *ISO* 27001, adequação a requisitos futuros.

Outro ponto de vista que foi discutido brevemente neste trabalho, mas não foi totalmente desenvolvido e é de grande importância em trabalhos futuros, seria a inclusão em conjunto com a análise de risco, uma metodologia para criação de um plano de continuidade de negócios (PCN). Na implementação da ferramenta, incluiu-se este escopo, no entanto apenas como informativo de que um ativo participa ou não do plano da empresa como sendo motivo de contingência.

Referências Bibliográficas

[1] ABNT. *Norma Brasileira ABNT NBR ISO/IEC 17799:2005-Tecnologia da informação-Técnicas de Segurança-Código de prática para a gestão da segurança da informação*. Rio de Janeiro-RJ, 2a. edition, Agosto 2005.

[2] Christopher Alberts, Audrey Dorofee, James Stevens, and Carol Woody. *Introduction to the OCTAVE Approach*. Carnigie Mellon University - Software Engineering Institute - Pittsburgh - USA, 2003.

[3] Michael J. Andrews, Charles A. e Haubenstock. *Implementação Do Novo Acordo da Basiléia*. Serasa - pages 32-46, São Paulo, 2003.

[4] Marilyn Greestein Arizona and Miklos Vasarhelyi. *Electronic Commerce: Security, risk management and control*. ISBN 0-07-241081-7. McGraw-Hill Higher Education, 2002.

[5] Benoit A. Aubert, Michel Patry, and Suzanne Rivard. *A framework for information technology outsourcing risk management*. SIGMIS Database, New York, NY, USA, 2005.

[6] Standards Australia. *Risk Management, Standard AS/NZS 4360*. Standards Australia, 2004.

[7] Mauro Cesar Bernarde and Edson dos Santos Moreira. *Um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional*. SSI 2005 - 7th Intl Symposium on System and Information Security, São José dos Campos - São Paulo - Brasil, 2005.

[8] N. Brownlee and E. Guttman. *RFC-2350 - Expectations for Computer Security Incident Response*. United States, 1998.

[9] British Standards Institute (BSI). *BS 7799:2001 - Information Security Management - Specification With Guidance for Use*, 2001.

[10] Mark Burgess. *Principles of network and system administration*. ISBN 85-216-1480-2. John Wiley, second edition, 2004.

[11] Hasan Cavusoglu and Huseyin Cavusoglu. *Emerging Issues in Responsible Vulnerability Disclosure*. Workshop on Information Technology and Systems (WITS 2004), Barcelona, Spain, 2004.

[12] Steve Christey. *Unforgivable Vulnerabilities*. The MITRE Corporation, Aug. 2007.

[13] Steve Christey and Robert A. Martin. *Vulnerability Type Distributions in CVE*. The MITRE Corporation, May 2007.

[14] CCTA The UK Central Computer and Telecommunications Agency. *risk analysis and management method (CRAMM) User's Guide (Version 2.0)*. UK, 1991.

[15] Infosec Council. *Formação de Cultura em Segurança da Informação*. Brasil, 2005.

[16] Luiz Fernando Rust da Costa Carmo, Ana Cristina Ribeiro Dutra de Almeida, Gustavo Alberto de Oliveira Alves, Tiago Monteiro do Nascimento, Reinaldo de Barros Correia, and André Henrique Ismael de Azevedo. *Estratégias De Mitigação De Riscos De Segurança Do Ambiente AGRIS (Análise e Gerência de Riscos em Segurança)*. SSI 2005 - 7th Intl Symposium on System and Information Security, Novembro 2005.

[17] Luiz Fernando Rust da Costa Carmo, Ana Cristina Ribeiro Dutra de Almeida, Gustavo Alberto de Oliveira Alves, Tiago Monteiro do Nascimento, and Reinaldo de Barros Correia e André Henrique Ismael de Azevedo. *Programa FRIDA - Relatório Final (v2.0) AGRIS - Análise e Gerência de Riscos em Segurança*. Rio de Janeiro - Brasil, Outubro 2006.

[18] IDC Empresa de consultoria. *Pesquisa segurança da informação*, Dezembro 2005.

[19] IDC Empresa de consultoria. *Worldwide Secure Content Management 2005-2009*, Dezembro 2005.

[20] Laerte Peotta de Melo and Dino Macedo Amaral. *Estudo de taxonomia de ataques e atacantes em um honeypot de alta interação*. The International Conference Of Forensic Computer Science - pages 38-42, Brasília - DF - Brasil, 2006.

[21] Laerte Peotta de Melo and Dino Macedo Amaral. *Honeypot de baixa interação como ferramenta para detecção de tráfego com propagação de Botnets*. The Second International Conference of Forensic Computer Science, Brasília - Brasil, 2007.

[22] Laerte Peotta de Melo and Paulo Roberto de Lira Gondim. *Análise de Risco em Ambientes Corporativos na Área de Tecnologia da Informação*. Simpósio em Excelência em Gestão e Tecnologia - SEGET, Resende - Rio de Janeiro - RJ, 2007.

[23] Laerte Peotta de Melo and Paulo Roberto de Lira Gondim. *A Framework for risk assessment of information technology in the corporate environment*. The international journal of Forensic Computer Science - pages 74-86, São Paulo - Guarujá - Brasil, 2007.

[24] Folker den Braber, Theo Dimitrakos, Bjorn Axel Gran, Mass Soldal Lund, Ketil Stolen, and Jan Oyvind Aagedal. *The CORAS methodology: model-based risk assessment using UML and UP*. Hershey, PA, USA, 2003.

[25] Christopher Alberts e Audrey Dorofee. *An Introduction to the OCTAVE Method*. Carnigie Mellon University - Software Engineering Institute - Pittsburgh - USA, January 2001.

[26] Emilio Tissato Nakamura e Paulo Lício de Geus. *Segurança de redes em ambientes cooperativos*. ISBN 85-7251-609-3. Editora Berkeley, São Paulo - SP - Brasil, 2002.

[27] Fariborz Farahmand, Shamkant B. Navathe, Philip H. Enslow, and Gunter P. Sharp. *Managing vulnerabilities of information systems to security incidents*. ICEC '03: Proceedings of the 5th international conference on Electronic commerce, New York, USA, 2003.

[28] Aguinaldo Aragon Fernandes and Vladimir Ferras de Abreu. *Implantando a Governança de TI: Da estratégia à gestão dos processos e serviços*. ISBN 85-7452-270-8. Editora Brasport, Rio de Janeiro - RJ - Brasil, 2006.

[29] Financial Executives Research Foundation. *What is COSO. Defining the Alliance That Defined Internal Control*. Financial Executives Research Foundation, April 2003.

[30] Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner. *Large-scale vulnerability analysis*. LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, New York, NY, USA, 2006.

[31] Louis Fussell and Scott Field. *The Role of the Risk Management Database in the Risk Management Process*. ICSENG '05: Proceedings of the 18th International Conference on Systems Engineering - pages 364-369, Washington, DC, USA, 2005.

[32] Pedro Galvão. *IBM - Gestão de Riscos Informáticos; Nem tudo é tecnologia*. XIII Semana da Informática, Portugal, 2006.

[33] Chingwoei Gan and Eric Scharf. *Building an Experience Factory for a Model-based Risk Analysis Framework*. Queen Mary University of London, 2003.

[34] Alice Goguen1 e Alexis Feringa1 Gary Stoneburner. *Risk Management Guide for Information Technology Systems*. NIST - National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, nist special publication 800-30 edition, Julho 2002.

[35] Anup K. Ghosh. *E-Commerce Security: Weak Links, Practical Solutions*. ISBN 0471192236. John Wiley Sons, Inc., New York, NY, USA, 1997.

[36] Bernd Grobauer. *CVE, CME, ... CMSI? Standardizing System Information*. FIRST - 17th Annual FIRST Conference on Computer Security Incident Handling, Singapore, Junho 2005.

[37] IBM Corporation Software Group. *Achieve greater efficiency in asset management by managing all your asset types on a single platform*. USA, 2007.

[38] The IT Governance Institute. *COBIT: Framework Control Objectives Management Guidelines Maturity Models*. The IT Governance Institute (ITGITM) (www.itgi.org), USA, 2007.

[39] ISO (International Organization for Standardization). *ISO 31000: General guidelines for principles and implementation of risk management*, 2008.

[40] ISO/IEC. *27001:2006 - Tecnologia da informação, Técnicas de segurança, Sistemas de gestão da segurança da informação - Requisitos*. ISO, Agosto 2006.

[41] M. J. Kenning. *Security Management Standard - ISO 17799/BS 7799*. BT Technology Journal - pages 132-136, Hingham, MA, USA, 2001.

[42] Theo Dimitrakos Rune Fredriksen Bjorn Axel Gran Siv-Hilde Houmb Yannis C. Stamatiou Ketil Stolen, Folker den Braber and Jan Oyvind Aagedal. *Model-based risk assessment in a component-based software engineering process: the CORAS approach to identify security risks*. Kluwer, 2003.

[43] Christian Lahti, Steve Lanza, and Roderick Peterson. *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools*. ISBN-10: 1-59749-036-9, ISBN-13: 978-1-59-749036-8. Syngress, 2005.

[44] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions, Fourth Edition*. ISBN 0072227427. McGraw-Hill, Inc., New York, NY, USA, 2003.

[45] Peter Mell, Karen Scarfone, and Sasha Romanosky. *Common Vulnerability Scoring System*. IEEE Security and Privacy - IEEE Educational Activities Department, Piscataway, NJ, USA, 2006.

[46] Peter Mell, Karen Scarfone, and Sasha Romanosky. *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*. National Institute of Standards and Technology Interagency Report 7435, Gaithersburg, Maryland, United States, Aug. 2007.

[47] David Ahmad Andrew Wright Sasha Romanosky Mike Schiffman, Gerhard Eschelbeck. *CVSS: A Common Vulnerability Scoring System*. National Infrastructure Advisory Council (NIAC), 2004.

[48] Robin Moses. *Corporate risk analysis and management strategies*. Secure Information Systems Limited, UK, Brighton, UK, 16-18 May 1995.

[49] Victor Valeriu Patriciu, Iustin Priescu, and Sebastian Nicolaescu. *Security Metrics for Enterprise Information Systems*. Journal of Applied Quantitative Methods, University of Economics, Bucharest, Romania, Dezembro 2006.

[50] Jeevan Perera and Jerry Holsomback. *An Integrated Risk Management Tool and Process*. Aerospace 2005, IEEE Conference - Pages 129- 136, Março 2005.

[51] Karen Scarfone Peter Mell and Sasha Romanosky. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*, 2007.

[52] Erik Schetina, Ken Green, and Jacob Carlson. *Internet Site Security*. ISBN 85-352-1055-5. Pearson Education, 2002.

[53] Mike Schiffman. *A Complete Guide to the Common Vulnerability Scoring System (CVSS)*, Jun 7 2005.

[54] Leonardo Scudere. *Risco Digital*. ISBN 8535221913. Editora Elsivier, Rio de Janeiro - Brasil, 2006.

[55] R. Shirey. *RFC-2828 - Internet Security Glossary*. United States, 2000.

[56] William Stallings. *Business Data Communications (5th Edition)*. ISBN 0131442570. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2004.

[57] William Stallings. *Cryptography and Network Security (4th Edition)*. ISBN 013-187-316-4. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2005.

[58] William Stallings. *Data and Computer Communications*. ISBN-13: 9780132433105 ou ISBN-10: 0132433109. Prentice Hall, eighth edition, 2007.

[59] Anita Vorster and Les Labuschagne. *A framework for comparing different information security risk analysis methodologies*. SAICSIT '05: Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, Republic of South Africa, 2005.

[60] Álvaro Teófilo. *Segurança sob a perspectiva do ITIL*. Revista IT Web, São Paulo, 2004.

Capítulo 9

Anexos

9.1 Anexo A - Artigos Publicados

Os artigos foram fruto do trabalho de pesquisa desenvolvido na Universidade de Brasília no período de 2006 a 2007 pelo mestrando Laerte Peotta orientado pelo Professor Paulo Gondim.

1 MELO, L. P. ; GONDIM, P. R. L. . *A Framework for risk assessment of information technology in the corporate environment.* The international journal of Forensic Computer Science, v. 2, p. 74-86, 2007.

2 MELO, L. P. ; GONDIM, P. R. L. . *Análise de Risco em Ambientes Corporativos na Área de Tecnologia da Informação.* Simpósio em Excelência em Gestão e Tecnologia - SEGET, 2007, Resende - RJ. http://www.aedb.br/seget, 2007. (poster)

3 MELO, L. P. ; GONDIM, P. R. L. . *Methodology for risk assessment and vulnerabilities identification in environment IT.* Chinacom 2008 Conference on Communications and Networking in China (ICST), (paper submetido, resultado previsto para maio de 2008)

9.2 Anexo B - A Framework for risk assessment of information technology in the corporate environment

Abstract

The growing need for transparency in business negotiations requires greater control of technological risks. However, technological risk assessment tools currently available in the market are imprecise as they are based on the analysis of events that have already passed. The current paper describes a real-time, proactive risk analysis framework. We propose that instead of testing vulnerabilities from an external point of view, agents be incorporated and distributed into "actives"(hardware and software) so as to be able to provide application, configuration and specific localization information. In this manner, changes noted will be divulged by the agent in an immediate and pro-active manner to a central repository. When vulnerabilities are detected, correction processes will be implemented automatically, permitting technological risks to be monitored in real-time.

Keywords: Risk assessment, information security, real time, vulnerability analyst

Introduction

There is currently a growing preoccupation with information security, resulting in the growth of a new field - technology risk analysis. The role of a technological risk analyst is to identify vulnerabilities, calculate a vulnerability score and verify whether or not the identified vulnerability can potentially affect the company business. If so, he or she must correct the problem in the shortest time possible. At first glance the task seems simple, with few steps to follow; however, the number of vulnerabilities has been increasing exponentially to the point that it has become impossible to identify vulnerabilities in a manual or even semi-automatic manner. Another point of note in risk analysis is the increasing need for transparency demanded by the market and by regulatory bodies that require corporations to follow strict information security management norms, such as Sarbanes- Oxley (SOX)[4], Basel Accords I and II[10], ISO 17799[1], ISO 27001[7] and BS-7799[2].

The need to adhere to international norms may result in extra costs and, in some cases, loss of competitiveness, albeit typically only in the short term. Medium and long-term effects resulting from the implementation of such norms are clearly beneficial and demonstrate a certain business "maturity"and preparedness that may even attract new investments and increase the trust of stockholders.

This growing need for transparency in business requires greater control of technological risks. Risk can be defined as the probability of a physical situation to cause damage, at any level, during a specified period of time of a vulnerability, which, in turn, is defined as a weakness in the system, that may involve people or processes or technology that can be exploited to obtain access to information. The existence of a vulnerability creates a risk that results in a threat, here defined as any circumstance or event that has the potential to cause an impact on the confidentiality, integrity or availability of information. As such, the proper classification of information is of critical importance in the cycle of security processes.

Risk analysis may be extremely complex and is directly dependent on the proper planning and prior knowledge of the technological environment in which the analysis will be made, and as such, it is defined as a process that aims to identify, analyze, reduce or transfer risk [13]. The technological risk analysis tools currently available in the market are highly dependent on proprietary operational systems [15][16] that tie the "solution"to a single platform. Additionally, these tools base their assessment on collected information regarding past events and, consequently, are unable to provide a true solution in real time.

Contrary to static models of risk analysis, this paper proposes a pro-active framework that functions in real-time. Instead of testing vulnerabilities from an external point of view, where the information is obtained by simply exploring the "active"(computational system composed of hardware and software), we propose that agents (sensors) capable of providing application, configuration and localization information be incorporated into actives. Any observed changes, such as physical location, software update or installation, hardware modifications, changes in security policy, etc., will be immediately reported by the agent, in a pro-active manner, to a central repository.

The function of the central repository will be to correlate the information provided by the agents with vulnerability information published by the National Institute of Standards and Technology (NIST) through a Common Vulnerability Scoring System (CVSS). Should a vulnerability be identified, a correction process will be immediately requested and the team responsible for that particular active will initiate laboratory analysis in order to make appropriate corrections.

The current paper is structured in the following manner: In Section 2, we present published work that is relevant to the topic. Section 3 will further explore the use of CVSS as an initial methodological base, as well as the metrics used for risk analysis. The model used to register vulnerabilities, known as Common Vulnerabilities and Exposures (CVE) will be discussed in Section 4. Sections 5 and 6 will address means to obtain and classify inventories as well as further detail the methodology of the proposed framework. Finally, Section 7

will present the conclusion and the direction of future work.

Related works

With regards to the development of this paper, we did not identify any previous work that proposed to conduct a risk analysis of information assets in real time, that is to say, at the moment that a vulnerability was identified and reported. In this context, we describe below the publications that contributed to meeting our original objective. The information necessary to define risk and security was established in a recent study by Perera and Holsomback [9]. The study further suggested a matrix for risk analysis following the framework shown in figure 9.1

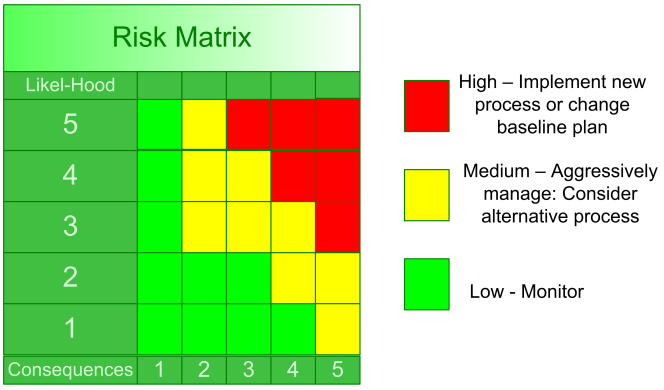

Figura 9.1: Risk analysis matrix

The authors also proposed a risk management system based on IRMA . However, this system is limited in that risk input must always be done manually; consequently there is always the need for a risk analyst for information input.

A study by Fussell and Field [6] identified and described methods for risk analysis management. However, similar to that noted by Perera and Holsomback [9], the described method was limited in that there was no systematic automation for system data collection to be used in risk management. The OCTAVE method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was described in [14], in which a team, known as "analysis team"managed the process and analyzed information, taking direct action when called for, depending on the situation. The method consisted of three distinct phases:

1. The characterization of a threat profile: the network structure and information organization are identified and described;
2. Identification of vulnerabilities: During this phase, the infrastructure is evaluated and vulnerable points are identified;

3. Strategy planning and development of a security plan: This is considered the most important phase, where a risk analysis plan of action is developed.

The difficulty in implementing this method is related to the need for a team of people to work exclusively in the analysis of information and risk, so that decisions can be made.

The objective of this paper is to elaborate a methodology that permits risk analysis calculations for applications and equipment in the area of information technology through the use of sensors that will collect local information and store the data in a central repository. Comparisons between the information provided by the sensors with available vulnerability information in databases will permit the identification of vulnerabilities in real-time, facilitating the initiation of correction processes.

Common Vulnerability Scoring System

Various information security departments such as the NIST (National Institute of Standards and Technology), FIRST (Forum of Incident Response and Security Teams) and CERT (Computer Emergency Response Team), among others, have created a standard to measure and quantify software vulnerabilities, known as CVSS [11]. Historically, the industry has utilized various scoring methods to determine software vulnerability [8]. However, the criteria or processes used were not detailed, which has caused serious problems to users in the management of their systems and applications. It is important to note that all variabilities exist within a limited timeframe, which must be acknowledged in order to solve the problem. The current work utilized CVSS and was based on the assumption that there will be standardization of vulnerability information and reporting of errors. Information divulged by CVSS will be stored internally and immediately compared with inventoried information, identifying actives that may be vulnerable.

FIRST was chosen by the NIAC (National Infrastructure Advisory Council) to head the CVSS project and to establish and open and universal evaluation standard to help organizations prioritize security and vulnerability analysis. The goal was to consolidate the efforts of security teams world-wide to solve the standardization problem and facilitate a quicker response time in addressing risks of known vulnerabilities. CVSS utilizes the following three basic metrics to calculate the score of a given vulnerability:

– Base metrics: contain the attributes that are intrinsic to all vulnerabilities;

- Temporal metrics: contain the vulnerabilities that evolve with the time and are dependent on the lifecycle of the vulnerability;
- Environmental metrics: represent those characteristics that are unique to the corporate environment in which they are being considered.

Base metrics

Base metrics are established by the manufacturer; they are based on the functionality and use of each software, and can be adapted to meet certain criteria. A total of seven impacts (summarized below) are used to obtain a final score that, in conjunction with the Temporal and Environmental metrics, will comprise the final risk score.

1. Access difficulty: measures the complexity required for a hacker to explore the targeted system.
2. Access vector: determines whether or not the vulnerability can be explored locally or remotely.
3. Authentication: determines whether or not the intruder needs to obtain authentication to explore the vulnerability of the system.
4. Confidentiality impact: measures the impact on confidentiality (none/partial/complete).
5. Integrity impact: determines the integrity impact.
6. Availability: determines the availability impact.
7. CIA impact (Confidentiality, Integrity, Availability): permits the evaluator to give greater weight to one of the CIA scores relative to the others.

Temporal metrics

Events may occur that affect the urgency of the threat posed by the vulnerability, that is, during the lifecycle of a vulnerability.

1. Exploitability: This assessment determines whether or not it is possible to exploit the vulnerability, and can be:
   - Unproven: without a known exploit;
   - Proof of Concept: a concept text has been created, suggesting that a threat exists;
   - Functional: when an exploit is available;
   - High: when the vulnerability is being exploited by a malicious code or manually exploited.
2. Remediation level: This assessment provides information as to whether or not a solution has been identified.

- Official Fix: when the manufacturer provides the correction (patch)
- Temporary Fix: when the manufacturer provides a temporary correction
- Walkaround and Unavailable

3. Report confidence: This assessment represents the degree of credibility that a vulnerability exists and the credibility of it dissemination (Unconfirmed/Uncorroborated/Confirmed)

Environmental metrics

Environmental metrics are the only metrics that are defined based on the situation of the specific company and consequently can be manipulated and changed by managers, auditors and consultants to more accurately represent the reality of a given company.

1. Collateral Damage Potential: This assessment measures the potential damage, which can represent the risk of loss of the equipment, with damage to property.
2. Target Distribution: This assessment indicates the percentage of systems, relative to the number of systems, that are susceptible to the vulnerability (None; Low, up to 15%; Medium, up to 40%; High, over 50% of the systems are vulnerable).

Scoring process

The scoring process will define a final value based on the combination of all the metrics used, adding the values utilizing pre-determined formulas [11]. The final score is obtained by combining the three previously described CVSS groups. The metric system can be defined by the vectors listed in table 9.1, facilitating the input of data and its use by a managing program.

Tabela 9.1: CVSS vector definition [11]

Vector	Descrition
Base Vectors	AV:[R,L]/AC:[H,L]/Au:[R,NR]/C:[N,P,C]/I:[N,P,C] /A:[N,P,C]/B:[N,C,I,A]
Temporal Vectors	/E:[U,P,F,H]/RL:[O,T,W,U]/RC:[N,U,C]
Environmental Vectors	/CD[N,L,LM,MH,H]:/TD:[N,L,M,H]

Common Vulnerabilities and Exposures (*CVE*)

The *CVE* (Common Vulnerabilities and Exposures) is a public database in which anyone can obtain information on vulnerabilities. The *CVE* has defined standards relative to the treatment and dissemination of vulnerability information.

The *CVE* database is the result of collaborative efforts between various entities working with information security, such as the Sans Institute, Cancert, CERT, among others. Massachusetts Institute of Technology's Digital Computer Laboratory (MITRE) is the main keeper of *CVE*. Given that this is collaborative project, no pre-specified contributions are expected. However, financial contributions as well as assistance in disseminating information are permitted.

The main objective of the use of *CVE* by the MITRE is not simply to disseminate information regarding vulnerability and security, but to standardize the manner in which this information should be treated. In this manner, the duplication of information is avoided and the data collected is utilized in an optimal manner. As a result, greater comprehension and consequently quality in the security of the data obtained can be achieved.

Management of resources

According to the ISO 27001 normative of 2005, all informational resources of a company must be identified and management, based on determined controls that must be previously established. Ideally, informational resources should be documented and categorized according to importance level. The importance of the resource, in case it is compromised, must also be considered. An effective risk analysis starts from the premise that all technological infrastructures have been identified [3]. There are various manners in which this can be accomplished, such as through manual research through the network, through speaking and interviewing those directly responsible for the infrastructure, through going to the points of connection, and through identifying and recording all of the components of the network.

Risk management is a continuous process that must always be reevaluated to identify inconsistencies. The process of risk analysis itself can be divided into six parts (Figure 9.2).

It is reasonable to assume that it would be viable to implement the above-mentioned points with a small to medium size network (of up to 1000 machines). Unfortunately, as soon as the data collection process has been finished and risk scoring initiated, the analysis would already be outdated- that is, what was assessed would already be in the past. Every passing minute makes risk analysis less efficient. As such, risk analysis may provide a false sense of security. The proposed

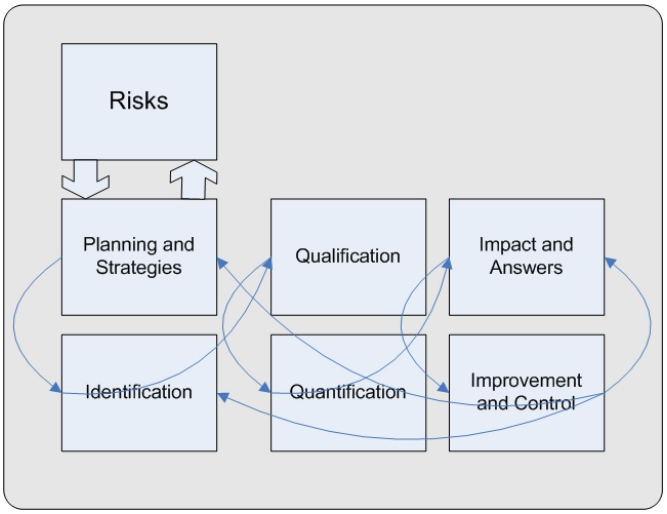

Figura 9.2: Risk management processes [12]

framework addresses this issue by allowing a real time analysis of the known vulnerabilities and the latest inventory changes.

Inventory procedures

The speed, at which information can be collected and updated, as a result of constant changes, is the key to successful risk analysis. Ideally, inventory tools used should meet the following requirements:

- Possess a characteristic client/server support system;
- Be a central database where all the information is stored;
- Be a multiple platform, accessible to diverse systems;
- Be manageable in such a way that information can be requested and obtained at any time;
- Consume a minimum amount necessary of resources to maintain the proper functioning of the client;
- Have the capacity to inform, even if, for whatever reason, the client is disabled;
- Have the ability to be reconfigured at any moment, in a global manner and independent of the will of the user.

Apart from these initial requirements, the tool must also have the capacity to collect diverse information for the inventory; all the information should be sent to the central database. Essential information includes:

- Version of the current operating system
- Any corrections made and the respective version of each

- Information of registered and former users
- List of installed software and respective versions
- Verification of installed antivirus systems and updates
- Information regarding partitions
- Information regarding the physical location of hardware (information provided by the user)
- List of hardware, such as memory, processor, hard drive, and video card specifications

Following data collection to obtain the basic characteristics of the IT infrastructure, qualification of each component must then be done, based on the following categories of importance: 1. Irrelevant; 2. Relevant; 3. Important; 4. Critical; 5. Vital

Proposal Framework

The objective of the article is to create a methodology for the collection, treatment and presentation of data regarding vulnerabilities, correlating events with information obtained form an internal network. To this end, two diagrams have been created, one from the point of view of the manager (Figure 9.3) and the other from the point of view of the user (Figure 9.4).

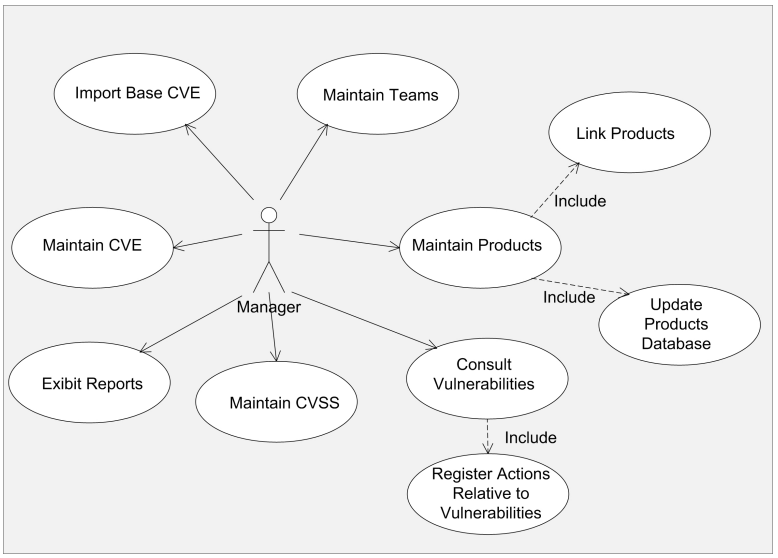

Figura 9.3: Diagram of the Manager's perspective

The user does not have access to the information viewed by the manager, however, the manager has a complete view of the system. The basic idea is to have various teams that are linked, however each user has a different view of the system.

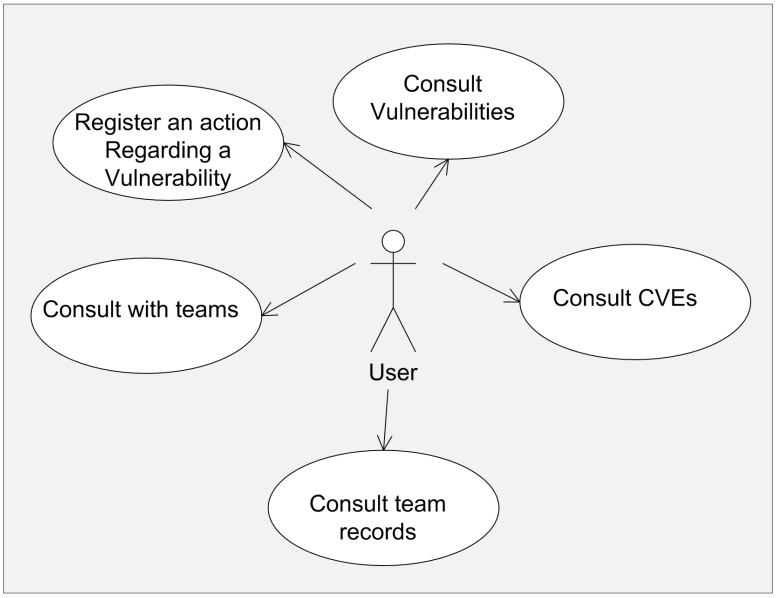

Figura 9.4: Diagram of the user's perspective

Information from the previously mentioned CVCS and *CVE* databases will be used to populate the internal database, creating a base of vulnerabilities referred to here as Risk. This information will be cross-checked with the software and hardware data obtained regarding the internal system, creating the basic contents, which include the IP address of the network machine, installed versions of softwares, information regarding registered users, type of operating system, hardware specifications (memory, processor, hard drive, etc.). The database created from the internal information collected will be referred to as Inventory.

Figure 9.5 demonstrates the correlation/link between the different information obtained, with the update of CVSS and CVS being maintained by external organizations. The base Inventory and Central Repository is maintained by the company. For the system to be efficient, all of the machines within the domain should have the inventory software installed (sensor) so as to continuously feed the internal database.

The company should have an established use policy; if none exists, the company should at minimum draw up "norms of usage of resources"by all users within the company. Normatives should contain the information regarding:

- The installation and downloading of software, prohibiting users to install any software that is not company approved software. This will also avoid the installation of unlicensed software;
- Terms of responsibility of use of company technological resources, explaining that their use must be work-related;

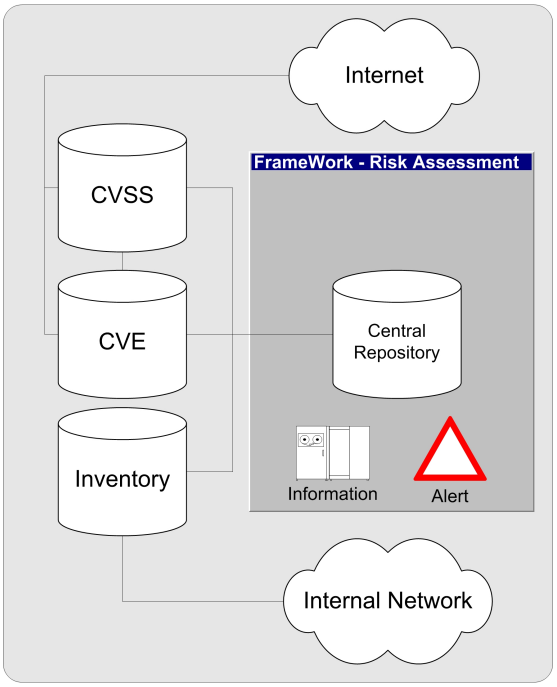

Figura 9.5: Risk infrastructure model

- Definition of limits of use of mobile resources (laptops, PDAs, etc.), prohibiting the use of non-company equipment;
- Installation of new technologic resources such that any new equipment must contain the required software and must be inventoried;
- Creation of a login procedure for network users, so that only technological resources that have been inventoried will have access to the local network;
- The development of a dissemination policy so that all employees will be aware of company policies.

Risk Score Adequation

Once all inventory information has been obtained, it is necessary to qualify each component regarding its importance. This qualification can be obtained by means of a questionnaire that should be responded by managers. In this manner, the company will obtain information regarding the machines/servers that have the greatest impact in case they are compromised, in terms of physical or logical problems. The flow diagram in Figure 9.6 summarizes the necessary steps for data collection for risk analysis from this point forward.

The framework described above will be applicable for the following uses:

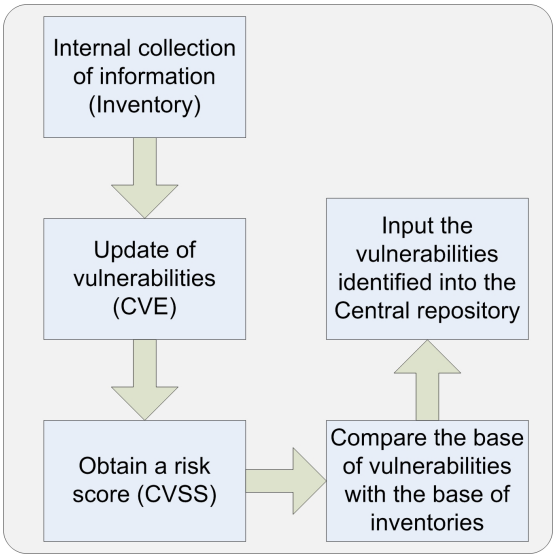

Figura 9.6: Procedures for Risk Analysis in the context of the proposed framework

1. Correctly identify all assets and determine their value as well as how critical they are for the company;
2. Estimate the probability of the occurrence of a threat and calculate the costs it would entail;
3. Identify vulnerable points and establish decisions/protocols to minimize or contain the risk;
4. Permit the creation of a strategy to minimize risks.

Framework demonstration

The proposed tool was developed utilizing JAVA programming language, with client/server support, where the server permits the visualization through a web server HTTP protocol. Initial tests utilized approximately 20 computers, with installed sensor information sent to a central repository.

The information obtained should be displayed or available in a consolidated manner, facilitating the identification of an actual risk resulting from a vulnerability, or permitting the visualization of the entire situation.

The various vulnerabilities that have been identified should be assigned to a specific team, initially responsible only for a specific product.

Each team may be responsible for more than one inventoried product. Figure 9.7 shows a view of the system as seen by the manager. This comprehensive view is only seen by framework managers - framework users have a similar view limited to the products they support (see Figure 9.9).

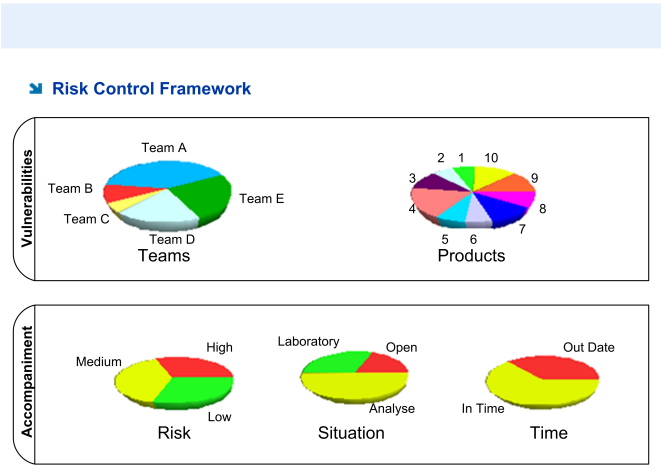

Figura 9.7: Framework manager's perspective of the system

The system is monitored from the point of view of vulnerabilities (the number of vulnerabilities and the number of products affected). The framework provides managers with a high level view of products with vulnerabilities and teams that need more attention. Detailed information from teams and/or products can be obtained by managers by selecting the desired team/product (see Figures 9.8 and 9.9). Risk is measured based on the CVSS score and graphically illustrated in the pie charts by the colors red, yellow and green.

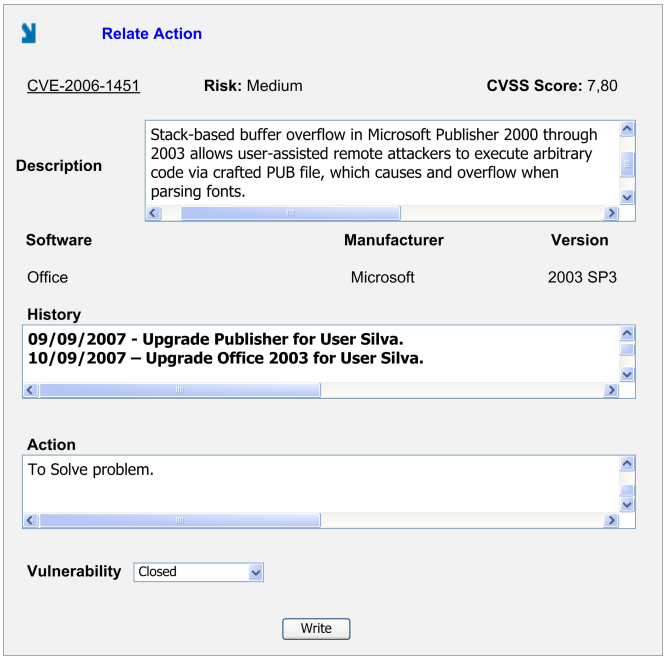

Figura 9.8: Record of an action

At the moment a framework manager or user takes an action, this action is and must be registered (Figure 9.8) as part of the history of actions taken to resolve the problem. This facilitates future work

as it establishes a minimum base of knowledge of procedures already attempted, making it easier to assign and distribute tasks, making the process user independent and auditable.

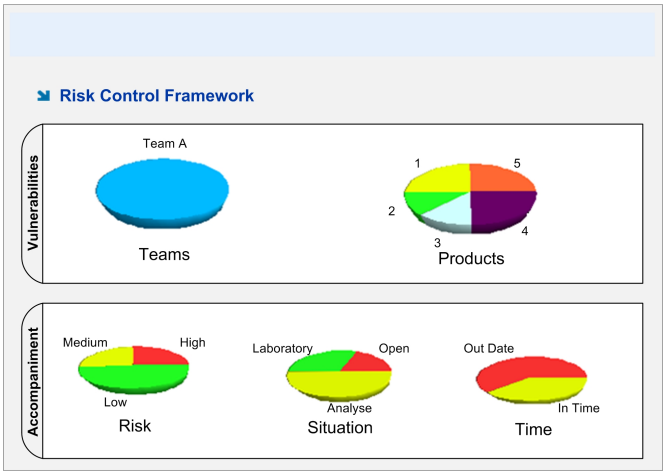

Figura 9.9: General view of the system as seen by the user

The historical record keeps the dates, actions taken and the name of the person executing the actions. This makes it possible to alter or adjust the vulnerability, through analysis or through laboratory work. It is also important to note the various statuses of the vulnerability situation can be "open", "in the laboratory"or "under analysis". Once the vulnerability is addressed in production, it is removed from the view. It has been previously demonstrated that even in empirical situations, the mere use of an available correction may result in even greater problems. For this reason, it is recommended that any changes or alterations be tested first in a laboratory situation and only then implemented in a production environment.

The access to information and view of the system of a specific framework user is limited to the view of his or her team. That is to say, a framework user does not have access to the information of another team (Figure 9.9). For this reason, the vulnerabilities pie graph is continuous, as the user is associated only to his/her own team. On the other hand, the Products graph is associated with all products that may require intervention and that have had their vulnerabilities inventoried.

Additionally, CVSS is used to calculate the risk. The user can find up to date information by simply clicking on the section of interest. All system vulnerabilities that have been inventoried can be seen (Figure 9.10), and can be further listed as "open", "under analysis"or "in laboratory", simplifying the follow-up on pending resolutions. Additionally, deadlines can also be viewed so that, if a correction is made after a given deadline, it is possible to investigate the reason for the delay.

Figura 9.10: Follow-up of vulnerabilities

The *CVE* can also be consulted directly, for information on the CVSS score, the CVSS vector, general risk, brief descriptions, affected products, references, and the date in which the vulnerability was identified, published or modified.

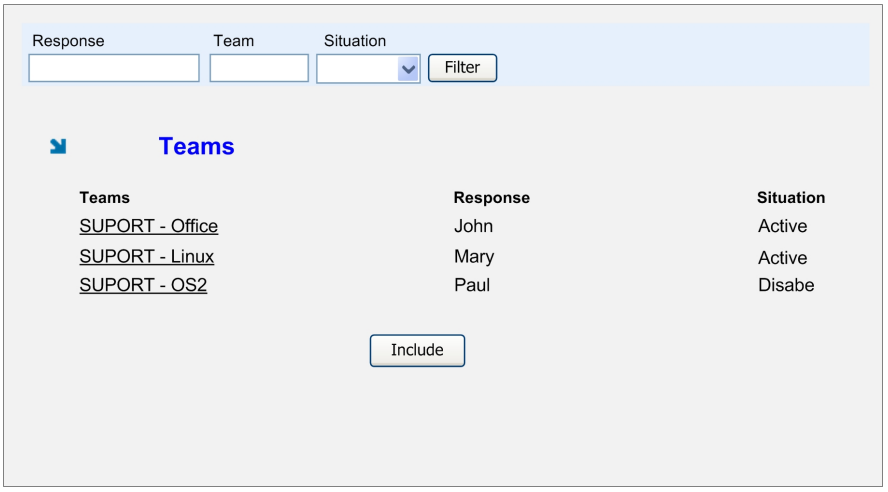

Figura 9.11: Management of teams

In order for the system to function in an automated manner, each team must be defined (Figure 9.11). Additionally, the products under their responsibility must be defined. Filters can also be used to, for example, verify which teams are active.

Conclusions and future work

The laws of various countries are being adapted and modified to increase the transparency of corporate operations so as to increase the trust of investors. Adherence to laws will result in greater gains related to the quality of company processes, increasing their competitiveness and consequently, resulting in greater profits. In recent years, much has been invested in the purchase of security equipment, with the use of systems that detect intrusions, antivirus software, firewalls, and anti-spam, among many others. But in reality, is it possible to evaluate if these investments were worth while? Much of the generated information is ignored or not considered seriously in the process of information management. It is regarding this issue that risk management may be of help, consolidating all available information and, most importantly, making this information useful.

The framework proposed by this article depends on various factors, the first of which is to convince managers that investing in information security is economically worthwhile, understanding that in the corporate environment, all return is of a financial nature. Another relevant factor is that the IT infra-structure will be clearly defined, facilitating a measurement of the return on investment (ROI) and with it, the elaboration of a plan of action for risk analysis, aimed at mitigating risk.

The tools suggested by the current study should initially be of an informative nature, providing basic information to the information manager, and utilizing the basic rules of the art of war : if you know yourself, you will have a chance at victory; if you know yourself and your enemy, you will have victory; if you know neither yourself nor your enemy, defeat is certain. The use of this metaphor relates to the persistent war that is carried out in worldwide networks, where dishonest companies attempt to obtain information illegally to gain a competitive advantage. The "enemy"is any person or company that can use illegally obtained information for their own benefit and to the detriment of the competitors.

The fact is, it is impossible to efficiently manage risk if it has not been initially identified as risk. In other words, risk is based on uncertainty - in the absence of uncertainty, risk does not exist. It is in this context that the present work has been developed, with an aim to reduce the variables associated with uncertainty and consequently reduce risk. In this context we propose a framework to control technological risks based on distributed sensors and a centralized vulnerability repository. As new vulnerabilities are published at the CVSS or any configuration change is communicated in real time by sensors through out the corporate environment, the framework automatically correlates the changes so as to identify new risks. Once identified, the framework assigns the vulnerability to the team responsible for the related pro-

duct, allowing corporations to take immediate actions to eliminate or mitigate the associated risks. As far as it is know to the authors, a framework based on real time analysis of configuration changes and known vulnerabilities has not been published before.

Future work includes the hardening of the tools developed and the full scale deployment in the corporate environment. The authors are also investigating how far automation could go on testing and deploying patches and updates as an alternative to reduce the dependency on human testing. Consideration on how sensors could be used to identify suspicious behavior of end users, based on patterns of configuration changes, is also in the scope of future research.

References

1 ISO/IEC 17799:2005-Information Technology - Code of practice for information security management.

2 (BSI), B. S. I. (2001). BS 7799:2001 - Information Security Management - Specification With Guidance for Use.

3 Chew, E., Clay, A., Hash, J., Bartol, N., and Brown, A. (2006) Guide for developing performance metrics for information security recommendations of the national institute of standards and technology.

4 Christian Lahti, Steve Lanza, R. P. (2005). Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools. ISBN-10: 1-59749-036-9, ISBN-13: 978-1-59-749036-8. Syngress.

5 Frei, S., May, M., Fiedler, U., and Plattner, B. (2006). Large-scale vulnerability analysis. In LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, pages 131-138, NewYork, NY, USA. ACM Press.

6 Fussell, L. and Field, S. (2005). The role of the risk management database in the risk management process. Pages 364-369.

7 ISO/IEC (2005). ISO/IEC 27001:2005 - Information Security Management-Specification With Guidance for Use. ISO

8 Mell, P., Scarfone, K., and Romanosky, S. (2006). Common vulnerability scoring system. IEEE Security and Privacy, 4(6):85-89.

9 Perera, J. and Holsomback, J. (2005). An integrated risk management tool and process. Aerospace 2005, IEEE Conference, (ISBN: 0-7803-8870-4, INSPEC Accession Number: 8939524, Digital Object identifier: 10.1109/AERO.2005.1559306):129-136.

10 Saidenberg, M., Schuermann, T., and May (2003). The new basel capital accord and Questions for research. Technical report.

11 Schiffman, M. (2005). A complete guide to the common vulnerability scoring system (cvss). http://www.first.org/cvss/cvss-guide.html.

12 Scudere, L. (2006). Risco Digital. ISBN: 8535221913. Editora Elsivier, Rio de Janeiro.

13 Stoneburner, G., Goguen, A., and Feringa, A. (July2002). Risk management guide for information technology systems - recommendations of the national institute of standards and technology.

14 Alberts, C. e Dorofee, A. (2001). An introduction to the octave method.

15 ISMS (International Management Systems Experts) - Risk Management Software. http://globalstand.backsite.com.br Access in 07/12/2007

16 Módulo Risk Manager - Risk Management Software. www.modulo.com.br access in 07/12/2007.

9.3 Anexo C - Análise de Risco em Ambientes Corporativos na Área de Tecnologia da Informação

RESUMO

Um tema que vem sendo muito discutido é a governança em TI (Tecnologia da informação), no entanto existem muitos métodos e técnicas de gestão que podem ser adotadas para se implementá-la. Um bom ponto de partida seria elaborar um plano para análise de risco em TI, controlando e conhecendo a infra-estrutura, agilizando a tomada de decisão visando reduzir ou mitigar o risco. Neste artigo será descrito uma metodologia para efetuar uma análise de risco eficiente.

***Palavras-Chave**: Gestão de risco, Segurança da informação, Governança, Compliance.*

Introdução

A premissa básica para uma boa governança em TI é o fato de que deve se conhecer o ambiente interno para uma tomada de decisão acertada, pois o que não se conhece não pode ser gerenciado.

Em uma empresa a área de TI pode ser tratada apenas como commodities, mas essa decisão pode transformar o modo como a empresa opera, sendo pouco acertado em alguns casos tratar a TI como não sendo área fim do negócio. A situação se agrava, pois muitas empresas mantêm negócios na internet e mesmo assim a área de TI fica terceirizada, podendo incorrer diversos riscos que acabam indos além das previsões da empresa e seus controles.

Atualmente as empresas estão bastante preocupadas com o tema segurança da informação, no entanto é necessário encontrar um método que avalie constantemente os ativos internos, auxiliando não somente a análise de risco, mas toda a gestão de TI, pois o conhecimento da infra-estrutura e dos ativos gera conseqüente reflexo na gestão.

A visão de um analista de risco em TI é poder identificar uma vulnerabilidade, calcular um score sobre a vulnerabilidade, verificar se essa falha afeta o negócio da empresa e por fim atuar de maneira a corrigir o problema, devendo o trabalho ser efetuado no menor tempo possível.

Aparentemente o trabalho é simples, pois são poucos passos a seguir, no entanto a quantidades de vulnerabilidades divulgadas vem crescendo exponencialmente, tornando o trabalho cada vez mais complexo a ponto de não ser mais possível controlá-lo de maneira manual ou mesmo semi-automatizado.

Outro aspecto relevante na análise de risco que deve ser observado é a necessidade cada vez mais exigida pelo mercado: a transparência das informações. Isso pode ser confirmado com o número crescente de exigências pelos órgãos reguladores que vem literalmente obrigando a cumprir normas como:

- Sarbanes- Oxley (SOX) [Lahti (2005)];
- Acordos de Basiléia I e II [Saidenberg (2003)];
- ISO 17799 [ABNT (2005)], ISO 27001[ISO/IEC (2005)] ou a BS-7799 [BSI (2001)] para a gestão de segurança da informação.

A adequação a esses padrões internacionais pode gerar custos extras, e em alguns casos, inclusive perda de competitividade, mas isso geralmente é considerado em curto prazo. Quando se avalia a adoção desses padrões e seus resultados a médio/longo prazo pode ter claramente uma visão positiva, demonstrando uma maturidade e preparo que podem, inclusive, atrair novos investimentos e gerar um sentimento elevado de segurança aos acionistas.

O risco pode ser definido como a probabilidade de que uma situação física com potencial de causar danos possa ocorrer, em qualquer nível, em decorrência da exposição durante um determinado espaço de tempo a uma vulnerabilidade, que por sua vez é definida como uma fraqueza em um sistema, que pode envolver pessoas, processos ou tecnologia que pode ser explorada para se obter acesso a informações.

Na existência de uma vulnerabilidade tem-se um risco que decorre do surgimento de uma ameaça que definimos como qualquer circunstância ou evento com o potencial de causar impacto sobre a confidencialidade, integridade ou disponibilidade da informação. Por este motivo a classificação da informação se torna um dos itens mais importantes do ciclo no processo da segurança.

Algumas ferramentas ou mesmo metodologias, tentam explorar as vulnerabilidades diretamente [agris 2004], o que pode levar a perda de informações, comprometimento dos serviços e muitas vezes a sobrecarga da própria rede. Em alguns casos as informações coletadas podem não espelhar a realidade, pois podem existir inconsistências na obtenção dos dados.

A análise de risco pode ser mais complexa que outros temas, mas tudo depende de um bom planejamento e conhecimento prévio do ambiente tecnológico que será aplicado à análise, para tanto definimos como sendo um processo que visa identificar, analisar, reduzir ou transferir o risco [Stoneburner (2002)].

Trabalhos relacionados

Na proposta de elaboração deste artigo não encontramos nenhum trabalho que se propusesse a executar uma análise de risco de ativos da informação e que retornasse as condições atuais em tempo real, ou seja, no momento que uma vulnerabilidade é encontrada e reportada. Neste contexto os trabalhos que contribuíram para o atingimento do foco inicial descrevemos aqui.

Em [Perera (2005)] são colocadas as informações necessárias para se definir termos sobre risco e segurança. Também é sugerida uma matriz para análise de risco, orientando a elaboração de um framework.

Os autores propuseram a criação de um sistema de gestão de risco pela IRMA (Intergovernmental Risk Management Agency). O ponto negativo desta ferramenta é que o risco é colocado sempre de forma manual, ou seja, deve existir a figura de um analista de risco para impostação das informações.

Em [Fussell (2005)] os autores colocam métodos para gestão da informação, descrevendo os processos que envolvem o tema e que tendem para a gerência de risco. O ponto negativo deste trabalho é também o mesmo que o trabalho [Perera (2005)], a falta de um agente que automatize de forma sistêmica a coleta de informações da rede que se pretenda implementar o método para gestão de risco. Em [Dorofee (2001)], é apresentado um método chamado OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), onde uma equipe, chamada de equipe de análise, gerencia o processo e analisa toda a informação. Organizando ações diretas, tomando decisões de acordo com a situação.

O método tem três fases distintas:

1. Construção de um perfil de ameaça: onde se deve conhecer a estrutura da rede e organização das informações;
2. Identificação de vulnerabilidades: Nesta fase deve-se avaliar a infra-estrutura e levantar pontos de vulnerabilidades;
3. Desenvolvimento de estratégia e plano de segurança: Esta fase pode ser considerada a mais importante, é onde será desenvolvido um plano de ação para a análise de risco.

O ponto que torna o método difícil de aplicar é a necessidade de uma equipe exclusiva para a análise de informações/risco e conseqüente tomada de decisão.

Common vulnerability scoring system

Vários órgãos e departamentos ligados a segurança da informação como o NIST (National Institute of Standards and Technology), FIRST

(Forum of Incident Response and Security Teams), CERT (Computer Emergency Response Team) entre outros, se juntaram para criar um padrão para pontuação/mensuração de vulnerabilidades de software chamado de CVSS [Schiffman (2005)].

Historicamente, a indústria tem utilizado diversos métodos de scoring para vulnerabilidades de softwares [Mell (2006)], geralmente sem detalhamento desses critérios ou processos, criando um grande problema para os usuários, que precisam encontrar um meio de gerenciar seus sistemas e aplicações.

É importante saber que toda vulnerabilidade tem um tempo de vida [Frei (2006)], e que deve ser respeitado e seguido para a solução do problema.

O NIAC (National Infrastructure Advisory Council) escolheu o FIRST para liderar o projeto e avaliar um padrão aberto e universal onde deverá ajudar organizações a priorizar a segurança e análise de vulnerabilidades, consolidarem esforços do mundo todo e equipes de segurança para resolver o problema permitindo uma resposta mais rápida a riscos provenientes de vulnerabilidades conhecidas.

Para se calcular o score para uma determinada vulnerabilidade o CVSS tem como base três métricas principais:

- Métricas básicas (Base Metrics) contêm os atributos que são intrínsecos a toda vulnerabilidade.
- Métricas temporais (Temporal Metrics) contêm as características que evoluem de acordo com o ciclo de vida da vulnerabilidade.
- Métricas ambientais (Environmental Metrics) representam aquelas características únicas de acordo com o ambiente corporativo de onde está sendo implantada.

Métricas básicas

As métricas básicas são impostadas pelo fabricante, são compostas de acordo com a funcionalidade e utilização implícita em cada software, podendo ser adaptada com critérios. São definidos sete impactos para se obter um score que em conjunto com as métricas temporais e ambientais comporão o risco final:

- Dificuldade para acesso: mede a complexidade requerida para que um atacante consiga explorar o sistema alvo
- Vetor de acesso: indica se uma vulnerabilidade é explorada localmente ou remotamente
- Autenticação: indica se um atacante necessita ou não ser autenticado no sistema para conseguir explorar a vulnerabilidade

- Impacto confidencialidade: mede o impacto na confidencialidade (nenhum / parcial / completo)
- Impacto Integridade: indica o impacto na integridade
- Impacto Disponibilidade: impacto na disponibilidade
- Impacto CIA (Confidencialidade, Integridade, Disponibilidade): permite atribuir maior impacto em um dos pilares da CIA sobre os demais.

Métricas temporais

As métricas temporais são determinadas de acordo com o tempo de vida de uma vulnerabilidade.

Exploitability: indica se é possível ou não explorar a vulnerabilidade, podendo ser:

- Unproven: (não há um exploit conhecido);
- Proof of Concept: (foi criada uma prova de conceito indicando que a ameaça existe);
- Functional: (quando um exploit está disponibilizado);
- High: (quando a vulnerabilidade está sendo explorada por um código malicioso ou mesmo manualmente).

Remediation Level: informa se há uma solução conhecida:

- Official Fix: quando o fabricante disponibilizou uma correção/patch;
- Temporary Fix: (fornecida uma correção temporária pelo fabricante);
- Workaround e Unavailable: Trabalhando e indisponível.

Report Confidence: Representa o grau de confiança na existência da vulnerabilidade e na credibilidade de sua divulgação (Unconfirmed / Uncorroborated / Confirmed).

Métricas de ambientes

São as únicas que são definidas de acordo com a realidade de cada empresa e, portanto podem ser manipuladas pelos gestores, consultores e auditores para representar a realidade em sua corporação:

- Collateral Damage Potential: mede o potencial de dano, podendo representar o risco de perda do equipamento físico, os danos de propriedade.
- Target Distribution: indica o tamanho relativo da quantidade de sistemas que são suscetíveis à vulnerabilidade (Nenhum; Baixo até 15%; Médio até 49% ou Alto - se acima de 50% dos sistemas são vulneráveis).

Processo de *scoring*

O processo de Scoring irá definir o valor final resultante da aplicação de todas as métricas, combinando todos os valores de acordo com fórmulas específicas conforme [Schiffman (2005)].

Da combinação dos três grupos descritos no projeto CVSS obtêm-se o score final.

Desta maneira existe certa facilidade na impostação dos dados ou mesmo no seu tratamento por parte de um programa gerenciador.

Common vulnerabilities and exposures (cve)

Define-se como um padrão no tratamento e divulgação de informações sobre vulnerabilidades reportadas. O *CVE* (Common Vulnerabilities and Exposures) é um banco de dados público em que todos interessados possam obter acesso a informações sobre vulnerabilidades.

O conteúdo do banco de dados *CVE* é resultado de esforços colaborativos entre várias entidades ligadas a segurança da informação, entre elas: Sans Institute, Cancert, CERT, entre outras.

O principal gestor do *CVE* é o MITRE (Massachusetts Institute of Technology's Digital Computer Laboratory). Como o projeto é colaborativo, não é exigida uma contribuição, mas pode ser feita, tanto financeiramente quanto em relação à divulgação de informações.

A proposta geral do MITRE com a utilização do *CVE* não é apenas a divulgação de informações sobre o aspecto de vulnerabilidades e segurança, mas principalmente a padronização de como essa informação deve ser encaminhada e tratada. Dessa forma corrigem-se eventuais duplicações de informação e trata de maneira eficiente os dados coletados, permitindo uma maior compreensão e conseqüentemente qualidade na obtenção de dados relacionados à segurança.

Gestão de ativos

Segundo a norma ABNT NBR ISO/IEV 17799 de 2005, o item gestão de ativos foca a responsabilidade pelos mesmos, ou seja, todos os ativos da empresa devem ser identificados e atribuído uma responsabilidade sobre a sua manutenção baseada em controles. É conveniente que os ativos identificados sejam documentados e a eles atribuído uma importância. Também se deve considerar a importância sobre o ativo, caso este seja comprometido.

Para uma eficiência em uma análise de risco deve-se partir do principio de que se conhece toda a infra-estrutura tecnologia [Chew (2006)]. Existem diversas maneiras conhecidas para se obter essa informação:

- Através de pesquisas manuais de descoberta na rede;
- Utilizando-se de entrevistas com responsáveis diretos pela infra-estrutura;
- Visitando todos os pontos de conexão
- Catalogando por inventário todos os componentes da rede.

O processo de gestão de risco é continuo e deve ser sempre reavaliado em busca de inconsistências. Podemos dividir o processo de condução de uma análise de risco em seis partes:

- Planejamento e estratégia: planejar ações e criar estratégias de avaliação
- Identificação: Criar procedimentos para uma correta identificação dos riscos;
- Qualificação: Introduzir uma qualificação decorrente de uma vulnerabilidade;
- Quantificação: Possibilitar uma pontuação do nível de risco;
- Impactos e respostas: Criar procedimentos para se determinar o impacto sujeito e qual resposta deverá ser utilizada;
- Monitoramento e Controle: Determinar procedimentos para um constante acompanhamento para ações.

Nos pontos aqui descritos, pode-se ter uma idéia que em redes de pequeno/médio porte (até 1000 máquinas) seria viável efetuar um dos itens acima. Infelizmente no momento que terminar de se coletar a ultima informação e conseqüentemente iniciar o processo de scoring de risco, toda a análise estará baseado no passado, ou seja, a análise de risco não terá a mesma eficiência, e a cada minuto que se passa menos eficiente estará. Com isso pode ocorrer uma falsa sensação de segurança.

Procedimentos de inventário

A velocidade na coleta da informação e sua constante atualização decorrido das mudanças que ocorrem a todo instante é a chave de sucesso para uma análise de risco eficaz.

Desta maneira é proposta uma ferramenta que deve atender aos seguintes requisitos:

- Possuir suporte característico cliente/servidor;
- Ter um banco de dados central, onde todas as informações serão armazenadas;
- Ser multi plataforma, de modo a rodar em diversos sistemas;

- Ser gerenciável para que se possam solicitar informações a qualquer momento que se faça necessário;
- Consumir o mínimo de recursos necessários para o funcionamento do cliente;
- Ser capaz de informar caso o cliente por algum motivo seja desabilitado;
- Poder ser reconfigurado a qualquer instante, de forma global, independente da vontade do usuário.

Desses requisitos iniciais, a ferramenta também deverá ser capaz de coletar diversas informações de inventário, sendo toda a informação enviada diretamente ao banco de dados central. Informações essenciais:

- Versão do sistema operacional corrente;
- Correções aplicadas e suas respectivas versões;
- Informações de usuários cadastrados e logados;
- Lista de softwares instalados e suas versões;
- Checagem de instalação de sistemas antivírus e suas atualizações;
- Informações sobre compartilhamentos;
- Informações de localização física do hardware (neste caso a informação deverá ser solicitada ao usuário);
- Lista de hardwares.

Após a coleta das informações para a geração de uma base de conhecimento da infra-estrutura de TI deve se proceder à qualificação quanto à importância do ativo. Para tanto um pequeno questionário pode ser adotado considerando cinco itens: Irrelevante, Relevante, Importante, Crítico e Vital.

Proposta do *Framework*

A proposta deste artigo é a criação de uma metodologia para coleta, tratamento e apresentação de dados sobre vulnerabilidades, correlacionando os eventos com informações obtidas em uma rede interna.

Não é possível que o usuário veja ou acesse a visão do gestor, no entanto o gestor tem a visão total do sistema. A idéia é ter várias equipes vinculadas com visões diferentes para cada usuário.

As bases de dados CVSS e *CVE* descritas neste artigo servirão para popular um banco de dados interno, gerando uma base de vulnerabilidades chamada aqui de Risco, essas informações serão cruzadas com os dados de software e hardware coletados em uma rede interna, gerando a base com o conteúdo:

- IP (Internet Protocol) da máquina na rede;
- Versão de softwares instalados;
- Informações sobre usuários logados no domínio;
- Tipo do sistema operacional;
- Informações sobre hardware (memória, processador, Hard disk).

A base de dados gerada através da coleta de informações internas será denominada inventário.

O diagrama demonstra a interligação/correlação das informações, sendo que a base CVSS e CVS é alimentada por organizações externas. A base Inventário e Risco são mantidos pela entidade interna. Para que o procedimento seja eficiente todas as máquinas do domínio deverão ter instalado o software de inventário que irá alimentar a base interna. Neste caso deverá constar, caso exista, na política de segurança da empresa, caso não exista uma política consolidada deverá pelo menos ser criada uma norma de conduta e utilização dos ativos por parte dos usuários.

A princípio a norma deverá conter informações sobre:

- Instalação e utilização de software não homologado pela instituição, de modo que impeça o usuário a instalar qualquer sistema que não conste no catalogo interno, com isso evitando instalações até mesmo de software sem licença;
- Termo de responsabilidade de utilização dos ativos tecnológicos, explicitando sua utilização apenas para fins diretos do negócio;
- Metodologia para utilização de ativos móveis (notebooks, PDA‘s, etc.) sendo vetada a utilização de equipamentos externos, ou seja, que não faça parte dos ativos próprios;
- Criação de métodos para instalação de novos ativos, sendo que qualquer equipamento ligado na rede deverá ter em seu enxoval de instalação o software de inventário.
- Criação de procedimentos de logins de usuários na rede, protegendo contra conexões espúrias, de modo que apenas ativos com o software de inventário serão permitidos no ambiente local;
- Por fim uma política de divulgação do projeto de modo que o maior número de pessoas possa conhecer e conseqüentemente apoiar.

Adequação do risco

Com todas as informações coletadas deve-se rever a pontuação gerada automaticamente e verificar através de um questionário a avaliação de servidores considerados críticos, dessa maneira terá informações

sobre quais máquinas/servidores tem maior impacto caso esta seja comprometida tanto por problemas físicos quanto lógico. Foi criado um fluxo (figura 9.12), onde é descrito os passos necessários para a coleta e cálculo do risco.

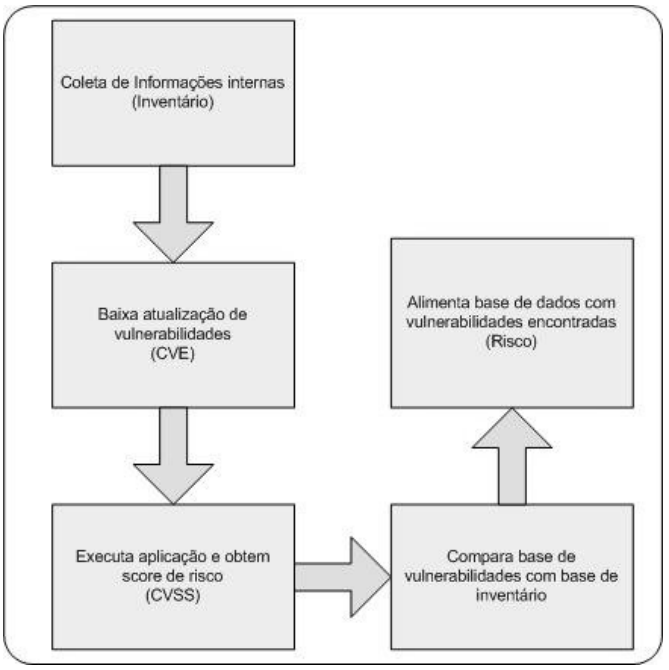

Figura 9.12: Procedimentos de coleta de informações

O Framework poderá auxiliar com as seguintes informações:

- Determinar o valor dos ativos de informação bem com sua criticidade para a corporação;
- Estimar uma determinada probabilidade de uma ameaça poder ocorrer e possibilitar o cálculo do custo;
- Identificar pontos vulneráveis e subsidiar decisões para contornar ou diminuir o risco;
- Permitir a criação de estratégia para mitigar os riscos;
- Possibilitar a correta identificação dos ativos.

Conclusões e trabalhos futuros

As leis de vários países estão sendo adaptadas visando dar maior transparência às operações das empresas. Com essa clareza os investidores poderão fazer seus investimentos com maior segurança. Por parte da empresa ocorrerá ganhos relacionados à qualidade de seus processos, tornando-a mais competitiva e, conseqüentemente, podendo aumentar seus ganhos financeiros.

Nos últimos anos foram investidos valores consideráveis para obtenção de equipamentos e soluções de segurança, como sistemas de detecção de intrusos, antivírus, firewalls, anti-spam, e uma infinidade de outras soluções. Mas como realmente saber se esses investimentos tiveram o retorno esperado? As informações geradas muitas vezes são ignoradas, ou quando tratadas pouco auxiliam na gestão da informação. É nesse ponto que a gestão de risco vem ao auxilio, consolidando os dados coletados e transformando em informações utilizáveis.

O framework proposto neste artigo depende de vários fatores, o principal é a aceitação da idéia por parte dos gestores de que o investimento em segurança da informação é algo que lhes trará retorno, e no mundo corporativo o retorno tem que ser de caráter financeiro.

Outro fator relevante é de que se conhecerá a infra-estrutura geral de TI, podendo mensurar os investimentos e retorno (ROI), com isso elaborar um plano de ação para o tratamento e análise de risco, visando à conseqüente mitigação dos riscos.

A ferramenta aqui proposta deverá, a principio, ser de caráter informativo, subsidiando o gestor de informações sobre sua própria base, aplicando-se regras fundamentais da arte da guerra: Se conheceres a si próprio terás chances de vitória;Se conheceres a si próprio e a seu inimigo terás a vitória; Se não conheceres nem a si e nem o seu inimigo a derrota serás certa.

Esta metáfora é devido à constante guerra que está sendo travada na rede mundial de computadores, onde empresas desonestas podem querer obter informações de maneira ilícita para que assim tenham vantagens sobre suas concorrentes. Conseqüentemente o inimigo é qualquer pessoa/empresa que se utilize de conhecimentos e informações obtidos de maneira não legal e os utilize para si, podendo gerar prejuízos para seus concorrentes.

O fato é que não é possível um gerenciamento eficiente de risco se não for possível identificá-lo, pois o risco ocorre tendo como premissa a incerteza, caso não exista incerteza não existe risco. É neste contexto que o trabalho está sendo desenvolvido, visando reduzir as variáveis de incerteza concomitantemente reduzindo o risco.

Em trabalhos futuros pretende-se desenvolver uma metodologia ativa em relação às vulnerabilidades, tornando-as inócuas à medida que forem detectadas, de maneira totalmente automatizada e transparente para o usuário.

O framework deverá permitir que vulnerabilidades sejam localizadas e corrigidas, identificando aspectos inclusive de comportamento do usuário.

Referências

ABNT (2005). NORMA BRASILEIRA ABNT NBR ISO/IEC 17799:2005-Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. ABNT, Rio de Janeiro - RJ, segunda edição.

Alberts, C. e Dorofee, A. (2001). An introduction to the octave method.

(BSI), B. S. I. (2001). BS 7799:2001 - Information Security Management - Specification With Guidance for Use. Chew, E., Clay, A., Hash, J., Bartol, N., and Brown, A. (2006) Guide for developing performance metrics for information security recommendations of the national institute of standards and technology.

Christian Lahti, Steve Lanza, R. P. (2005). Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools. ISBN-10: 1-59749-036-9, ISBN-13: 978-1-59-749036-8. Syngress.

Frei, S., May, M., Fiedler, U., and Plattner, B. (2006). Large-scale vulnerability analysis. In LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, pages 131-138, NewYork, NY, USA. ACM Press.

Fussell, L. and Field, S. (2005). The role of the risk management database in the risk management process. Pages 364-369. ISO/IEC (2005). ISO/IEC 27001:2005 - Information Security Management-Specification With Guidance for Use. ISO

Mell, P., Scarfone, K., and Romanosky, S. (2006). Common vulnerability scoring system. IEEE Security and Privacy, 4(6):85-89. Perera, J. and Holsomback, J. (2005). An integrated risk management tool and process. Aerospace 2005, IEEE Conference, (ISBN: 0-7803-8870-4, INSPEC Accession Number: 8939524, Digital Object identifier: 10.1109/AERO.2005.1559306):129-136.

Saidenberg, M., Schuermann, T., and May (2003). The new basel capital accord and Questions for research. Technical report. Schiffman, M. (2005). A complete guide to the common vulnerability scoring system (cvss). `www.first.org/cvss/cvss-guide.html`

Scudere, L. (2006). Risco Digital. ISBN: 8535221913. Editora Elsivier, Rio de Janeiro.

Stoneburner, G., Goguen, A., and Feringa, A. (July2002). Risk management guide for information technology systems - recommendations of the national institute of standards and technology.

Carmo, Luiz Fernando. Costa, Ricardo de Barros e Reis, Carlos Augusto. Alves, Gustavo Alberto de Oliveira. Nascimento , Tiago Monteiro.

(2004) . Estratégias De Mitigação De Riscos De Segurança Do Ambiente AGRIS - Núcleo de Computação Eletrônica Universidade Federal do Rio de Janeiro, Brasil

9.4 Anexo D - Documento de Requisitos de Sistema

Sistema: Sistema Gestão de Risco TI

Descrição geral do sistema

O Projeto deve identificar os componentes de rede e confrontar as informações sobre vulnerabilidades divulgadas e calcular um risco para esse componente. Também deve gerar relatórios sobre vulnerabilidades encontradas e criar um acompanhamento para efetivação das correções, bem como um histórico e base de conhecimentos das ações realizadas.

Características de usuários

Nome do usuário: GESTOR
Descrição do usuário: Gestor de segurança

Nome do usuário: USUÁRIO
Descrição do usuário: Responsável pelo software ou hardware

Premissas e dependências

A base atualizada de *CVE* será baixada diariamente da internet, do site `http://nvd.nist.fov/download.cfm`. O sistema utilizará a base de informações (hardwares, softwares e suas respectivas versões). O sistema funcionará no ambiente da intranet corporativa.

Requisitos futuros

Possibilidade de correlações de logs gerados por dispositivos de rede como firewalls, IDS (Sistemas de detecção de intrusão), etc, baseado em módulos permitindo uma maior integração da ferramenta.

Requisitos funcionais

- Download base *CVE*;
- Manter base *CVE* atualizada;
- Importar base de Produtos;
- Consultar *CVE*;
- Consultar produtos com vulnerabilidades;

- Incluir histórico de Produto com Vulnerabilidade;
- Consultar histórico de Produto com Vulnerabilidade;
- Manutenção de equipes (incluir, alterar, consultar, excluir)
- Manutenção de produtos (incluir, alterar, consultar, excluir);
- Manutenção de vulnerabilidades (incluir, alterar, consultar, excluir);
- Vincular usuários a Equipes;
- Vincular produtos a Equipes.

Requisitos de desempenho

- Número de acessos simultâneos: 10 usuários;
- Transações de consulta/dia: 100 consultas;
- Transações de atualizações/dia: 50 atualizações;
- Volume de dados - média diária: 15 Mb;
- Tempo de resposta em condições normais: 3 a 10 segundos.

Requisitos de segurança

O controle de acesso seguirá os padrões de segurança adotados pela instituição no acesso a rede interna.

Requisitos de confiabilidade

As cópias de segurança das tabelas deverão ser efetuadas semanalmente.

Requisitos de disponibilidade

Em condições normais da *intranet*, o sistema deverá estar disponível 24h/dia, respeitando a janela de manutenção da rede, conforme acordos de níveis de serviços previamente informados.

Requisitos operacionais

Utiliza as mesmas características de arquitetura e restrições da rede interna.

Requisitos de qualidade

- Portabilidade: não há necessidade de instalar a aplicação em mais de uma plataforma;
- Usabilidade: deverá possuir pesquisas diversas para localização de informações. Quando a quantidade de itens dificultar a visualização, deve possuir opções de pesquisa ou combos para buscar informações disponíveis na base de dados. A navegação entre campos deve manter o padrão em todas as telas para facilitar o aprendizado do sistema. Deve fornecer informações sobre a realização ou não das ações solicitadas;
- Escalabilidade - o sistema deverá ser robusto para comportar todos os dados previstos;
- Facilidade de manutenção: será utilizado projeto orientado a objetos para facilitar a evolução do *software*.

9.5 Anexo E - Especificação de Caso de Uso

9.5.1 UC01 - Importar Arquivos *NIST*

Este caso de uso ocorre diariamente, deve ser inicializado pelo gestor por questões de segurança. Ele é responsável por fazer o *download* dos arquivos do *NIST* para a máquina do usuário.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O gestor acessa um aplicativo, preenche os campos com sua chave e senha;
2. O sistema verifica se a chave e a senha do usuário possuem 8 caracteres. [E1]
3. O sistema acessa a internet com os dados fornecidos pelo usuário;
4. O sistema efetua o download dos arquivos [nvd_dictionary.txt], [nvdcve-recent.xml] e [nvdcve-modified.xml] para a máquina o usuário;
5. O sistema apresenta uma tela com a descrição do resultado da operação de *download*;
6. Fim do caso de uso.

Fluxo de Exceção

1. E1: verificação de chave e senha;
2. Caso a chave ou a senha não possuam 8 caracteres, o sistema apresenta uma mensagem de erro informando que a chave ou a senha são inválidos;
3. O sistema retorna ao passo 1 do Fluxo Básico.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização : O usuário deve ter acesso à internet.

Regras de negócio

- Os arquivos não serão armazenados para histórico.
- O sistema deve sobrescrever os arquivos caso já estejam na máquina do usuário.

Procedimentos de contingência

Caso ocorra insucesso no *download* dos arquivos [nvd_dictionary.txt], [nvdcve-recent.xml] e [nvdcve-modified.xml] via programa sgaDownload.jar, os mesmos deverão serem baixados do site do *NIST* manualmente.

- *NIST*: `http://nvd.nist.gov/download.cfm`
- arquivo [nvd_dictionary.txt] : `http://nvd.nist.gov/download/nvd\_dictionary.txt`
- arquivo [nvdcve-recent.xml] : `http://nvd.nist.gov/download/nvdcve-recent.xml`
- arquivo [nvdcve-modified.xml] : `http://nvd.nist.gov/download/nvdcve-modified.xml`

9.5.2 UC02 - Importar Base de Produtos

Este caso de uso ocorre diariamente, deve ser inicializado pelo gestor por questões de segurança. Ele é responsável por processar os arquivos do *NIST* e fazer a carga e atualização da base de fabricantes, produtos e versões do sistema.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O gestor acessa um aplicativo via linha de comandos;
2. O sistema processa o arquivo com o dicionário de dados do *NIST* ["nvd_dictionary.txt"];
3. O sistema insere ou atualiza os dados conforme a necessidade;
4. O sistema apresenta na tela uma mensagem de "OPERAÇÃO REALIZADA COM SUCESSO";
5. Fim do caso de uso.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O usuário deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.

Caso de uso Importar Arquivos *NIST*: O caso de uso Importar Arquivos *NIST* deve ter sido executado anteriormente .

Regras de negócio

- Os arquivos não serão guardados em um histórico.
- O sistema deve processar linha a linha buscando verificar o surgimento de novos produtos.
- Produtos não serão excluídos em hipótese alguma.

9.5.3 UC03 - Importar Base *CVE*s

Este caso de uso ocorre diariamente, deve ser inicializado pelo gestor por questões de segurança. Ele é responsável por processar os arquivos do *NIST* e fazer a carga e atualização da base de *CVE's* do sistema.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O gestor acessa um aplicativo via linha de comandos, e passa como parâmetro sua chave;
2. O sistema verifica se a chave do usuário possui 8 caracteres. [E1]
3. O sistema processa o arquivo com os *CVEs* do dia. *NIST* ["nvdcve-recent.xml"];
4. O sistema insere ou atualiza os dados conforme a necessidade.
5. O sistema processa o arquivo com os *CVEs* modificados vindos do *NIST* ["nvdcve-modified.xml"];
6. O sistema insere ou atualiza os dados conforme a necessidade.
7. O sistema apresenta na tela uma mensagem de "OPERAÇÃO REALIZADA COM SUCESSO".
8. Fim do caso de uso.

Fluxo de Exceção

9.5.3.1 E1: Verificação de chave

1. Caso a chave não possua 8 caracteres, o sistema apresenta uma mensagem de erro informando que a chave é inválida.
2. O sistema retorna ao Passo 1 do Fluxo Básico.

Requisitos Especiais

Não há.

Condições Prévias

- Autenticação e autorização: O usuário deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.
- O caso de uso Importar Base de Produtos deve ter sido executado posteriormente.

Regras de negócio

- Os arquivos não serão armazenados em histórico, o histórico é a própria base de *CVE*;
- Um *CVE* existente no sistema é apenas atualizado;
- Um *CVE* com o campo *type="CAN"* (candidato) não é incluído na base;
- Um *CVE* com o campo *reject="1"* faz com que o sistema gere uma ação de cancelamento do mesmo com uma mensagem padrão do sistema;
- Se o *CVE* for cancelado o sistema deverá finalizar todas as ocorrências de vulnerabilidades vinculadas ao *CVE*, incluindo uma ação com o texto "*CVE* CANCELADO - Vulnerabilidade Cancelada pelo Sistema".

9.5.4 UC04 - Vincular Produtos *NIST* x *CACIC*

Este caso de uso ocorre quando o gestor necessita vincular produtos do software *CACIC* e produtos da base *NIST*.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O Gestor seleciona o item "vincular produtos";
2. O sistema exibe uma tela de filtro solicitando a entrada do nome de uma fabricante específico
3. O usuário preenche este campo clica no botão "filtrar";
4. Após esta filtragem, o sistema apresenta uma tela com uma lista com os produtos encontrados com o valor passado no filtro de fabricante;
5. O usuário seleciona um produto e clica no botão "filtrar";
6. O sistema apresenta uma tela com uma lista com o padrão(fabricante-produto-versão) referente a base *NIST* e outra lista referente aos produtos do software *CACIC* com o padrão(fabricante-produto-versão). O resultado destas listas se baseia nos dados repassados nos filtros anteriores; [A1], [A2];
7. O gestor seleciona um produto da lista referente à base *NIST* e seleciona um ou N produtos referentes a lista do *CACIC*;
8. O gestor clica no botão "vincular";
9. O sistema exibe uma tela de confirmação;
10. O usuário clica no botão confirmar;
11. Fim do caso de uso.

Fluxo alternativo

A1: Filtrar produtos na tela de vinculação com campo "filtro *NIST*"

1. O gestor fornece entrada com campo "filtro *NIST*";
2. O gestor clica em filtrar;
3. O sistema realiza o filtro dos produtos do *NIST* e atualiza a lista de produtos *NIST*;
4. O sistema exibe a tela de vinculação com a lista atualizada;
5. Fim do caso de uso;
6. Retorno ao fluxo básico.

A2: Filtrar produtos na tela de vinculação com campo "filtro *CACIC*"

1. O gestor fornece entrada com campo "filtro *CACIC*";
2. O gestor clica em filtrar;
3. O sistema realiza o filtro dos produtos do *CACIC* e atualiza a lista de produtos *CACIC*;
4. O sistema exibe a tela de vinculação com a lista atualizada;
5. Fim do caso de uso;
6. Retorno ao fluxo básico.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O usuário deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

- Um produto do *NIST* pode ser vinculado a N produtos do *CACIC*;
- Um produto *CACIC* só pode ser vinculado a um produto *NIST*.

9.5.5 UC05 - Manter equipes

Este caso de uso ocorre quando um gestor precisa atualizar informações referentes a equipes.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O usuário seleciona a opção "Equipes";
2. O sistema exibe um botão "incluir",um botão "alterar", um botão "excluir"e uma lista de equipes com os seguintes dados: Nome da equipe, Responsável, Situação;
3. O usuário seleciona a opção incluir; [A1]
4. O usuário seleciona uma equipe a opção alterar; [A2]
5. O usuário seleciona uma equipe a opção excluir; [A3]
6. O usuário a opção filtrar; [A4]
7. Fim do caso de uso.

Fluxo alternativo

A1: Incluir Equipe

1. O usuário clica no botão "incluir"no fluxo básico;
2. O sistema solicita a entrada dos seguintes dados:
   (a) Nome da equipe;
   (b) Funcionário responsável pela equipe;
   (c) Funcionário responsável.
   (d) Funcionários membros da equipes;
   (e) Produtos sob a responsabilidade da equipe.
3. O usuário informa com os dados solicitados;
4. O usuário seleciona a opção incluir;
5. O sistema solicita confirmação
6. O usuário confirma;
7. O sistema inclui a equipe e informa que a operação foi executada com sucesso;
8. Fim do caso de uso.

A2: Alterar equipe

1. O sistema carrega entradas com os seguintes dados;
   (a) Nome da equipe;
   (b) Funcionário responsável;
   (c) Descrição da equipe;
   (d) Lista de funcionários membros da equipe;
   (e) Lista de produtos sob a responsabilidade da equipe.
2. O usuário altera um ou mais itens de dados;
3. O usuário seleciona a opção alterar;
4. O sistema solicita confirmação da operação;
5. O usuário confirma;
6. O sistema registra as alterações e informa que a operação foi executada com sucesso;
7. Fim do caso de uso.

A3: Excluir equipe

1. O sistema solicita confirmação da operação;
2. O usuário confirma;
3. O sistema exclui a equipe;
4. O sistema exibe a lista de equipes e informa que a operação foi executada com sucesso;
5. Fim do caso de Uso;

A4: Filtrar Equipes

1. O usuário fornece uma entrada ou várias entradas de filtro:
   (a) Responsável;
   (b) Equipe;
   (c) Situação.
2. O usuário aciona o comando filtrar;
3. O sistema exibe uma lista com as equipes que atendam os critérios fornecidos;
4. Fim do caso de uso

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O O usuário deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

- Um usuário pode fazer parte de mais de uma equipe.
- Um produto pode estar vinculado a mais de uma equipe.
- Uma equipe só pode ser excluída caso não possua vulnerabilidades associadas.
- A Equipe de segurança nunca poderá ser excluída, só os integrantes da mesma podem mudar.Nome e demais atributos não mudam.
- uma equipe deve ter no mínimo um líder. o líder também pode ser o funcionário.
- quando uma equipe for associada a um produto o sistema deverá gerar todas as vulnerabilidades anteriores para a equipe, sendo que as vulnerabilidades com risco alto deverão estar com o estado em aberto e as demais com o estado inativo, com opção para o usuário abrir a vulnerabilidade.
- um usuário pode estar vinculado a mais de uma equipe.
- se a equipe for desativada o sistema deverá alterar o estado das vulnerabilidades vinculadas à equipe para inativo, incluindo uma ação com o texto "equipe cancelada - vulnerabilidade suspensa pelo sistema".
- se uma for equipe desativada, todas as vulnerabilidades serão notificadas/visualizadas pela equipe de segurança. a vulnerabilidade passa a ser inativa. o status da equipe também passa a ser inativa, todas as vulneravilidades relacionadas à equipe terão o status de inativas.

9.5.6 UC06 - Manter produtos

Este caso de uso ocorre quando um gestor precisa atualizar informações referentes a produtos não identificados pelo sistema *CACIC*.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O Gestor seleciona a opção produtos;
2. O sistema exibe uma lista de produtos com os seguintes dados:
   (a) Fabricante;
   (b) Produto;
   (c) Origem.
3. O usuário seleciona um produto;
4. O sistema exibe os seguintes dados:
   (a) Fabricante;
   (b) Produto;
   (c) Origem;
   (d) Equipes responsáveis;
   (e) *CVE´*s.
5. O Gestor seleciona a opção incluir; [A1]
6. O Gestor seleciona a opção alterar; [A2]
7. O Gestor seleciona a opção excluir; [A3]
8. Fim do caso de uso.

Fluxo alternativo

Filtrar Produtos

1. O usuário fornece uma entrada ou várias entradas de filtro:
   (a) Fabricante;
   (b) Produto;
   (c) Origem.
2. O usuário aciona o comando filtrar;
3. O sistema exibe uma lista com os Produtos que atendam os critérios fornecidos;
4. Fim do caso de uso.

A1: Incluir produto

1. O sistema solicita a entrada dos seguintes dados:
   (a) Fabricante;
   (b) Produto;
   (c) Equipes responsáveis (preenchimento opcional).
2. O gestor entra com os dados;
3. O gestor seleciona incluir;
4. O sistema solicita confirmação;
5. O gestor confirma;
6. O sistema inclui o produto e informa que a operação foi executada com sucesso;
7. Fim do caso de uso.

A2: Alterar produto

1. O sistema carrega entradas com os seguintes dados;
   (a) Fabricante;
   (b) Produto;
   (c) Equipes responsáveis (preenchimento opcional).
2. O gestor altera um ou mais itens de dados;
3. O gestor seleciona a opção alterar;
4. O sistema solicita confirmação da operação;
5. O gestor confirma;
6. O sistema registra alterações e informa que a operação foi executada com sucesso;

A3: Excluir produto

Este fluxo só está disponível para produtos que não estão associados a equipes ou *CVE*s.

1. O sistema solicita confirmação;
2. O gestor confirma;
3. O sistema exclui produto;
4. O sistema exibe a lista de produtos e informa que a operação foi executada com sucesso;
5. Fim do caso de Uso;

Requisitos Especiais

Não há.

Condições Prévias

O gestor deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

- Um produto NÃO pode ser excluído em hipótese alguma.
- Um PRODUTO pode estar vinculado a mais de uma EQUIPE, neste caso gerando umaVULNERABILIDADE, independente, para cada EQUIPE.

9.5.7 UC07 - Manter *CVE*

Este caso de uso ocorre quando um gestor precisa gerenciar informações referentes a *CVE*s.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O usuário seleciona a opção *CVEs*;
2. O sistema sistema exibe a lista de *CVEs* registrados no sistema, com os seguintes dados:
   (a) Código *CVE*;
   (b) Data Publicação;
   (c) Produtos;
   (d) Risco;
   (e) Situação.
3. O usuário seleciona um *CVE*;
4. O sistema exibe os seguintes dados:
   (a) Tipo;
   (b) Nome;
   (c) Sequencial;
   (d) Risco;
   (e) Data de descoberta;
   (f) Data de publicação;
   (g) Data de modificação;
   (h) Pontuação CVSS;
   (i) Vetor CVSS;
   (j) Descrição *CVE*;
   (k) Lista de produtos afetados
   (l) Lista de referências.
5. O usuário seleciona a opção incluir; [A1]
6. O usuário seleciona um *CVE* e a opção alterar; [A2]
7. O usuário seleciona um *CVE* e a opção excluir; [A3]
8. Fim do caso de uso.

Fluxo alternativo

Filtrar *CVE*s

1. O usuário fornece entrada para um ou várias entradas de filtro:
   (a) *CVE*;
   (b) Data;
   (c) Produto;
   (d) Situação.
2. O usuário aciona o comando filtrar;
3. O sistema exibe uma lista com os *CVE*s que atendam os critérios fornecidos;
4. Fim do caso de uso.

A1: Incluir *CVE*

1. O sistema solicita a entrada dos seguintes dados:
   (a) Nome *CVE*;
   (b) Risco;
   (c) Data descoberta;
   (d) Data publicação;
   (e) Descrição;
   (f) Referências;
   (g) Softwares afetados.
2. O usuário informa os dados solicitados;
3. O usuário seleciona a opção incluir;
4. O sistema solicita confirmação
5. O usuário confirma;
6. O sistema inclui o *CVE* e informa que a operação foi executada com sucesso;
7. Fim do caso de uso.

A2: Alterar *CVE*

1. O sistema carrega entradas com os seguintes dados;
   (a) Nome *CVE*;
   (b) Risco;
   (c) Data descoberta;
   (d) Data publicação;
   (e) Descrição;

(f) Referências;
(g) Softwares afetados.

2. O usuário altera um ou mais itens de dados;
3. O usuário seleciona a opção alterar;
4. O sistema solicita confirmação da operação;
5. O usuário confirma;
6. O sistema registra as alterações e informa que a operação foi executada com sucesso;
7. Fim do caso de uso.

A3: Excluir *CVE*

Este fluxo só estará disponível para *CVE´*s que ainda não tenham ações associadas.

1. O sistema solicita confirmação;
2. O usuário confirma;
3. O sistema exclui o *CVE*;
4. O sistema exibe a lista de *CVE´*s e informa que a operação foi executada com sucesso;
5. Fim do caso de Uso;

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: o usuário deve ter autenticado o usuário pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

- A Gerência de segurança só pode cancelar um *CVE* gerado por ela mesma.
- Somen te a Gerência de segurança (gestor) pode incluir *CVE*.
- Se o *CVE* for cancelado o sistema deverá finalizar todas as ocorrências de vulnerabilidades vinculadas ao *CVE*, incluindo uma ação com o texto "*CVE* CANCELADO - Vulnerabilidade Cancelada pelo Sistema".

9.5.8 UC08 - Consultar Vulnerabilidades

Este caso de uso ocorre quando o gestor deseja consultar as vulnerabilidades registradas no sistema.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O gestor seleciona a opção vulnerabilidades;
2. O sistema exibe uma lista com as 20 últimas vulnerabilidades detectadas. São exibidos os seguintes dados para cada Vulnerabilidade:
   (a) Código do *CVE*;
   (b) Equipe;
   (c) Produto;
   (d) Risco;
   (e) Situação;
   (f) Prazo.
3. O usuário seleciona uma vulnerabilidade e clica no botão consultar
4. O sistema exibe os detalhes do *CVE* associado e o histórico de ações referentes vulnerabilidade selecionada.
5. Fim do caso de uso. [A1]

Fluxo alternativo

Filtrar *CVE*s

1. O usuário fornece entrada para um ou várias entradas de filtro:
   (a) *CVE*;
   (b) Data;
   (c) Produto;
   (d) Situação.
2. O usuário aciona o comando filtrar;
3. O sistema exibe uma lista com os *CVE*s que atendam os critérios fornecidos;
4. Fim do caso de uso.

A1: Filtrar vulnerabilidades

1. O usuário fornece entrada para um ou vários campos de filtro:
   (a) Equipe;
   (b) Produto;
   (c) Código do *CVE*;
   (d) Prazo;
   (e) Risco;
   (f) Situação.
2. O usuário aciona o botão filtrar;
3. O sistema exibe uma lista com as vulnerabilidades que atendam aos critérios fornecidos;
4. Fim do caso de uso.

Requisitos Especiais

Não há.

Condições Prévias

O usuário deve ser autenticado pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

– O gestor pode consultar todas as vulnerabilidades.
– O gestor pode encerrar ou reabrir uma vulnerabilidade, gerando uma ação para qualquer uma destas opções.

9.5.9 UC09 - Registrar ação referente a vulnerabilidade

Este caso de uso ocorre quando o gestor necessita registrar uma ação para encerrar ou reabrir uma vulnerabilidade.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O gestor clica no botão encerrar ou no botão reabrir, a partir da tela de consulta de vulnerabilidades, para registrar a ação;
2. O sistema exibe uma tela com um campo para o gestor inserir o motivo da ação.
3. O gestor preenche o campo e clica no botão confirmar;
4. O sistema exibe uma mensagem de confirmação;

Fluxo alternativo

Não há.

Requisitos Especiais

Não há.

Condições Prévias

- Caso de Uso Consultar Vulnerabilidades.
- Autenticação e autorização: o usuário deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

- As únicas ações permitidas ao gestor são encerrar ou reabrir.
- Uma ação não pode ser editada após ter sido incluída pelo usuário.
- Uma ação não pode ser editada em hipótese alguma.
- Uma ação não pode ser excluída em hipótese alguma.
- Só a Gerência de segurança pode reabrir uma vulnerabilidade finalizada.

9.5.10 UC10 - Exibir Relatórios

Este caso de uso ocorre quando o gestor acessa o aplicativo.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O gestor acessa o sistema;
2. O sistema exibe os gráficos sob a ótica de dois domínios: Vulnerabilidades e Acompanhamento. Para este são apresentados os gráficos de Vulnerabilidades por Equipe(s) e por Produto(s), e para aquele os gráficos de Risco, Situação e Prazo.
3. O gestor clica no gráfico Equipe(s) do domínio Vulnerabilidades;[A1]
4. O gestor clica no gráfico Produto(s) do domínio Vulnerabilidades;[A2]
5. O gestor clica no gráfico Risco do domínio Acompanhamento;[A3]
6. O gestor clica no gráfico Situação do domínio Acompanhamento;[A4]
7. O gestor clica no gráfico Prazo do domínio Acompanhamento;[A5]
8. Fim do caso de uso.

Fluxo alternativo

A1: Listar vulnerabilidades por equipes

1. O sistema verifica o nível hierárquico da informação (Gerencial ou Equipe). Se o nível for Gerencial, os gráficos serão novamente carregados, porém, apenas com as informações da equipe selecionada. Se o nível for Equipe, será apresentada uma lista com as seguintes informações:
   (a) Nome da equipe (informação deve constar apenas como título e cabeçalho);
   (b) Código *CVE* (com link para consulta detalhada da *CVE*);
   (c) Data Descoberta;
   (d) Produto(s);
   (e) Risco;
   (f) Prazo.
2. Fim do caso de uso.

A2: Listar vulnerabilidades por produto

1. O sistema verifica quais vulnerabilidades estão associadas com o produto selecionado e apresenta uma lista com as seguintes informações:
   (a) Nome do produto (informação deve constar apenas como título e cabeçalho);
   (b) Código *CVE* (com link para consulta detalhada da *CVE*);
   (c) Data Descoberta;
   (d) Equipe(s);
   (e) Risco;
   (f) Prazo.
2. Fim do caso de uso.

A3: Listar vulnerabilidades por risco

1. O sistema verifica quais vulnerabilidades estão associadas com o risco selecionado e apresenta uma lista com as seguintes informações:
   (a) Risco (informação deve constar apenas como título e cabeçalho);
   (b) Código *CVE* (com link para consulta detalhada da *CVE*);
   (c) Data Descoberta;
   (d) Equipe(s);
   (e) Produto(s);
   (f) Risco;
   (g) Prazo.
2. Fim do caso de uso.

A4: Listar vulnerabilidades por situação

1. O sistema verifica quais vulnerabilidades estão associadas com a situação selecionada e apresenta uma lista com as seguintes informações:
   (a) Situação (informação deve constar apenas como título e cabeçalho);
   (b) Código *CVE* (com link para consulta detalhada da *CVE*);
   (c) Data Descoberta;
   (d) Equipe(s);
   (e) Produto(s);
   (f) Risco;
   (g) Prazo.
2. Fim do caso de uso.

A5: Listar vulnerabilidades por prazo

A vencer : Vulnerabilidades sem providências em até 15 dias da data de descoberta;

Vencidas : Vulnerabilidades sem providências após 15 dias da data de descoberta.

1. O sistema verifica quais vulnerabilidades estão associadas com o prazo selecionado e apresenta uma lista com as seguintes informações:
   (a) Prazo [A vencer ou Vencida] (informação deve constar apenas como título e cabeçalho);
   (b) Código *CVE* (com link para consulta detalhada da *CVE*);
   (c) Data Descoberta;
   (d) Equipe(s);
   (e) Produto(s);
   (f) Risco;
   (g) Prazo.
2. Fim do caso de uso.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O gestor deve ter autenticado o usuário pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

– Somente o gestor tem visão sobre TODAS as Vulnerabilidades e TODAS as equipes.

9.5.11 UC11 - Consultar Equipes

Este caso de uso ocorre quando um usuário necessita consultar as informações referentes a(s) equipe(s) da(s) qual(is) é integrante.

Atores : Usuário

Fluxo de Eventos

Fluxo Básico

1. O usuário seleciona a opção Equipes;
2. O sistema exibe a lista das equipes das quais o usuário é integrante, com os seguintes dados:
   (a) Nome da Equipe;
   (b) Responsável
3. O usuário clica no nome da equipe que deseja consultar;
4. O sistema exibe os detalhes da equipe do usuário com os seguintes dados:
   (a) Nome da equipe;
   (b) Responsável pela equipe;
   (c) Todos os usuários integrantes da equipe com as respectivas chaves e seus nomes;
   (d) Todos os produtos pelos quais a equipe é responsável.
5. Fim do caso de uso.

Fluxo alternativo

Não há.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: usuário deve ter sido autenticado e possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

– O usuário só tem a visão das equipes das quais é integrante.

9.5.12 UC12 - Consultar *CVE*s

Este caso de uso ocorre quando um usuário necessita consultar os dados de um ou mais *CVE's*.

Atores : Usuário

Fluxo de Eventos

Fluxo Básico

1. O usuário seleciona a opção *CVE's*;
2. O sistema sistema exibe a lista de *CVE's* registrados no sistema, com os seguintes dados:
   (a) Código *CVE*;
   (b) Data Publicação;
   (c) Produtos;
   (d) Risco;
   (e) Situação.
3. O usuário seleciona um *CVE*;
4. O sistema exibe os seguintes dados:
   (a) Nome;
   (b) Sequencial;
   (c) Risco;
   (d) Data de descoberta;
   (e) Data de publicação;
   (f) Data de modificação;
   (g) Pontuação CVSS;
   (h) Vetor CVSS;
   (i) Descrição *CVE*;
   (j) Lista de produtos afetados
   (k) Lista de referências;
5. Fim do caso de uso.

Fluxo alternativo

Filtrar *CVE*s

1. O usuário fornece entrada para um ou várias entradas de filtro:
   (a) *CVE*;
   (b) Data;
   (c) Produto;

(d) Situação

2. O usuário aciona o comando filtrar;
3. O sistema exibe uma lista com os *CVE*s que atendam os critérios fornecidos;
4. Fim do caso de uso;

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O usuário deve ter autenticado o usuário pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.

9.5.13 UC13 - Consultar Vulnerabilidades

Este caso de uso ocorre quando um usuário deseja consultar uma vulnerabilidade.

Atores : Usuário

Fluxo de Eventos

Fluxo Básico

1. O usuário seleciona a opção vulnerabilidades;
2. O sistema exibe a lista de vulnerabilidades relacionadas a produtos sob responsabilidade de equipes a qual o usuário esta vinculado. São exibidos os seguintes dados para cada notificação;
   (a) Código do *CVE*;
   (b) Data de notificação;
   (c) Produto;
   (d) Situação;
   (e) Risco;
   (f) Prazo.
3. O usuário seleciona uma vulnerabilidade e clica no botão detalhar;
4. O sistema exibe os detalhes do *CVE* associado e o histórico de ações referentes a equipe do usuário;
5. Fim do caso de uso. [A1]

Fluxo alternativo

A1: Filtrar vulnerabilidades

1. O usuário fornece entrada para um ou vários campos de filtro:
   (a) *CVE*;
   (b) Data;
   (c) Produtos;
   (d) Situação;
   (e) Risco.
2. O usuário aciona o botão filtrar;
3. O sistema exibe uma lista com notificações que atendam os critérios fornecidos;
4. Fim do caso de uso.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O usuário deve ser autenticado pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

– Um usuário só poderá consultar as vulnerabilidades vinculadas a sua equipe.

9.5.14 UC14 - Registrar ação referente a vulnerabilidade

Este caso de uso ocorre quando um usuário necessita registrar uma ação executada para solucionar uma vulnerabilidade.

Atores : Usuário

Fluxo de Eventos

Fluxo Básico

1. O usuário seleciona a opção registrar ação, a partir da tela de consulta de vulnerabilidades;
2. O sistema exibe os detalhes da Vulnerabilidade, *CVE* associado e ações anteriores, da equipe do usuário, um campo para inclusão da nova ação e outro para indicar o novo status da vulnerabilidade;
3. O usuário entra com a o texto descritivo da ação e situação da vulnerabilidade e solicita sua inclusão;
4. O sistema solicita confirmação;
5. O usuário confirma a operação;
6. O sistema registra a ação (texto, timestamp de criação, situação da vulnerabilidade e chave do usuário) e notifica que a operação foi executada com sucesso;
7. Fim do caso de uso.

Fluxo alternativo

Não há

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O usuário deve ser autenticado pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.

Regras de negócio

- Os usuários só podem visualizar as ações de suas respectivas equipes.
- Uma ação não pode ser editada após ter sido incluída pelo usuário.
- Uma ação não pode ser editada em hipótese alguma.
- Uma ação não pode ser excluída em hipótese alguma.
- Os usuários só podem visualizar as ações de suas respectivas equipes.

9.5.15 UC15 - Gerar relatório principal

Este caso de uso ocorre quando o usuário acessa o aplicativo ou quando o usuário clica em relatórios.

Atores : Gerência de segurança

Fluxo de Eventos

Fluxo Básico

1. O usuário acessa o sistema;
2. O sistema exibe os gráficos sob a ótica de dois domínios: Vulnerabilidades e Acompanhamento. Para este são apresentados os gráficos de Vulnerabilidades da Equipe e vulnerabilidades por Produto(s) gerenciado(s) pela equipe, além dos gráficos de Risco, Situação e Prazo.
3. O usuário clica no gráfico Equipe do domínio Vulnerabilidades;[A1]
4. O usuário clica no gráfico Produto(s) do domínio Vulnerabilidades;[A2]
5. O usuário clica no gráfico Risco do domínio Acompanhamento;[A3]
6. O usuário clica no gráfico Situação do domínio Acompanhamento;[A4]
7. O usuário clica no gráfico Prazo do domínio Acompanhamento;[A5]
8. Fim do caso de uso.

Fluxo alternativo

A1: Listar vulnerabilidades por equipes

1. O sistema exibe apenas as vulnerabilidades da equipe do usuário com as seguintes informações:
   (a))Código *CVE* (com link para consulta detalhada da *CVE*);
   (b) Data Descoberta/Detecção da vulnerabilidade;
   (c) Situação;
   (d) Risco;
   (e) Prazo.
2. O usuário deve selecionar uma vulnerabilidade e clicar no botão detalhar.
3. Fim do caso de uso.

A2: Listar vulnerabilidades por produto

1. O sistema verifica quais vulnerabilidades estão associadas com o produto selecionado e apresenta uma lista com as seguintes informações:
   (a) Código *CVE* (com link para consulta detalhada da *CVE*);
   (b) Data Descoberta;
   (c) Equipe(s);
   (d) Risco;
   (e) Prazo.
2. Fim do caso de uso.

A3: Listar vulnerabilidades por risco

1. O sistema verifica quais vulnerabilidades estão associadas com o risco selecionado e apresenta uma lista com as seguintes informações:
   (a) Código *CVE* (com link para consulta detalhada da *CVE*);
   (b) Data Descoberta;
   (c) Equipe(s);
   (d) Produto(s);
   (e) Risco;
   (f) Prazo.
2. O usuário seleciona uma vulnerabilidade e clica no botão detalhar;
3. Fim do caso de uso.

A4: Listar vulnerabilidades por situação

1. O sistema verifica quais vulnerabilidades estão associadas com a situação selecionada e apresenta uma lista com as seguintes informações:
   (a) Código *CVE* (com link para consulta detalhada da *CVE*);
   (b) Data Descoberta;
   (c) Equipe(s);
   (d) Produto(s);
   (e) Risco;
   (f) Prazo.
2. O usuário deve selecionar uma vulnerabilidade e clicar no botão detalhar;
3. Fim do caso de uso.

A5: Listar vulnerabilidades por prazo

A vencer: Vulnerabilidades sem providências em até 15 dias da data de descoberta;
Vencidas: Vulnerabilidades sem providências após 15 dias da data de descoberta.

1. O sistema verifica quais vulnerabilidades estão associadas com o prazo selecionado e apresenta uma lista com as seguintes informações:
   (a) Código *CVE* (com link para consulta detalhada da *CVE*);
   (b) Data Descoberta;
   (c) Equipe(s);
   (d) Produto(s);
   (e) Risco;
   (f) Prazo.
2. O usuário deve selecionar uma vulnerabilidade e clicar no botão detalhar;
3. Fim do caso de uso.

Requisitos Especiais

Não há.

Condições Prévias

Autenticação e autorização: O gestor deve ter autenticado o usuário pelo sistema de login da intranet e este deve possuir as permissões necessárias para utilizar o sistema.
O usuário só poderá acessar as informações das equipes nas quais estiver vinculado.

Regras de negócio

– Somente o gestor tem visão sobre todas as vulnerabilidades e todas as equipes.