Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Claudio Cesar Fraga Cavalcante

SEGURANÇA DA INFORMAÇÃO:

Despesa ou Investimento ?

Rio de Janeiro

2006

Claudio Cesar Fraga Cavalcante

SEGURANÇA DA INFORMAÇÃO: Despesa ou Investimento ?

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Carlos Eduardo Mendes de Azevedo, S.Sc., UFRJ, Brasil

Rio de Janeiro
2006

Claudio Cesar Fraga Cavalcante

SEGURANÇA DA INFORMAÇÃO: Despesa ou Investimento ?

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Setembro de 2006.

Carlos Mendes

Prof. Carlos Eduardo Mendes de Azevedo, S.Sc., UFRJ, Brasil

Dedico este trabalho a minha querida e amada mãe, por ter me ensinado com seus exemplos que na vida por maior que seja o problema que enfrentamos, não devemos nunca desistir, mas sempre olhar pra frente e fazer o nosso melhor para resolvê-lo. Mãe sou feliz por Deus ter me dado esse presente lindo, você.

Dedico este trabalho ao autor da minha vida, Jesus Cristo. Obrigado pela força que o senhor me deu quando pensei em desisir. Obrigado por ter me dado à oportunidade de viver esse momento lindo chamado VIDA.

AGRADECIMENTOS

São muitas pessoas que contribuíram de forma direta ou indireta no período que estive pesquisando sobre esse assunto, sendo assim, agradeço a todos os amigos de trabalho da E/8ªCRE em especial a professora Régia que sempre me deu força e condições para que eu fizesse a pós-graduação.

Agradeço também ao meu amigo Tiago, você sempre me motivou a fazer essa Pós e sempre perguntou: já terminou a monografia? amigo aí está.

Agradeço também a todo o corpo docente e administrativo do MOT, vocês sempre tiveram maior consideração com seus alunos.

Não poderia deixar de agradecer ao Professor Carlos Mendes, que também é responsável pelo sucesso desse trabalho.

Tem duas pessoas pequenininhas que também gostaria de agradecer pela compreensão que elas tiveram, são elas Mariana e Eduarda, elas muitas vezes choraram quando me chamavam para brincar e eu dizia que não podia, pois estava estudando. Minhas sobrinhas lindas vocês são as coisas mais sublimes que Deus plantou em nossa família. O tio agora pode brincar.

Agradeço também a minha irmã por acreditar em minha capacidade.

Novamente agradeço ao autor da minha vida, Jesus Cristo.

RESUMO

CAVALCANTE, Claudio Cesar Fraga. **SEGURANÇA DA INFORMAÇÃO: DESPESA OU INVESTIMENTO?** Monografia (Especialização em Gerência de Redes de Computadores e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

Segurança da Informação é um assunto cada vez mais discutido em reuniões empresarias, já é percebido por todos os executivos a necessidade de implementação de controles para proteger o negócio, contudo, apesar da necessidade de segurança ser comprovada nem sempre os controles necessários são implementados, isto se deve, principalmente na dificuldade que o setor de TI ou Security Office tem em demonstrar que o capital aplicado terá um retorno. São muitas as variáveis que fazem esse assunto ficar obscuro para os executivos, logo torna-se necessário mapear a linguagem técnica do campo de SI, para uma linguagem compreensível por todos os executivos. Através do ROI será possível obter os dados necessários para tirar a conclusão se a solução produz algum retorno ou não.

Palavras-chave: Segurança da Informação; Retorno sobre Investimento; Security Office

ABSTRACT

CAVALCANTE, Claudio Cesar Fraga. **SEGURANÇA DA INFORMAÇÃO: DESPESA OU INVESTIMENTO?** Monografia (Especialização em Gerência de Redes de Computadores e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

Security of Information is a subject more and more discussed in meetings entrepreneurs, it is already noticed by all the executives the need of implementation of controls to protect the business, however, in spite of safety's need to be proven not always the necessary controls are implemented, this is due, mainly in the difficulty that the section of TI or Security Office have in demonstrating that the applied capital will have a return. They are many the variables that make that subject to be obscure for the executives, soon he/she becomes necessary to map the technical language of the field of SI, for a comprehensible language for all the executives. Through I ROI will be it possible to obtain the necessary data to remove the conclusion if the solution produces some return or not.

Keywords: Security of Information; Return on Investiment ; Security Office

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

SIGLA	DESCRIÇÃO
ALE	Annualized Loss Expectancy
ASSET	Asset Map
BIA	Bussiness Impact Analysys
BITMAP	Bussiness and Information Technology Map
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technology
CVM	Comissão de Valores imobiliários
ICP-BRASIL	Infra-Estrutura de Chaves Públicas Brasileiras
ISO	International Standard Organization
ROI	Return on Investment
ROSI	Return on Security Investment
SGSI	Sistema de Gestão da Segurança da Informação
SI	Security Information
SLE	Single Loss Expectancy
TCO	Total Cost of Ownership
TI	Technology Information

SUMÁRIO

1 **INTRODUÇÃO**

O objeto de estudo dessa pesquisa aborda a Segurança da Informação, que consiste em uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Também pode ser considerada como uma prática da gestão de riscos de incidentes que impliquem no comprometimento da confidencialidade, integridade e disponibilidade da informação.

É fato que há muito, as empresas têm sido influenciadas por mudanças e novidades que surgem no mercado a todo o momento e provocam alterações de contexto. Em todas as etapas, a informação é algo de extremo valor para o negócio, porém, é importante observar e analisar todos os aspectos ligados à segurança, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle, e principalmente, os momentos que fazem parte do seu ciclo de vida.

Toda informação é influenciada por três propriedades principais, a saber: confidencialidade, integridade e disponibilidade, além dos aspectos autenticidade, legalidade que complementam esta influência.

Dessa forma, o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa.

Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, quatro momentos do ciclo de vida são merecedores de atenção e, independente da forma como a informação é representada, todos os momentos se aplicam.

Tais momentos podem ser definidos da seguinte forma: a) manuseio, que é o momento em que a informação é criada e manipulada; b) armazenamento, momento em que a informação é armazenada, seja em um banco de dados compartilhado, por exemplo; c) transporte, quando a informação é transportada, seja por correio eletrônico, via fax ou ao telefone e; d) descarte, momento em que a informação é descartada, por exemplo, ao eliminar um arquivo eletrônico do computador ou descartar um CD-ROM usado que apresentou falha na leitura.

Sendo assim, em qualquer iniciativa tomada para a solução de um problema, primeiramente, é necessário identificar a sua origem com requinte de detalhes de forma a permitir maior profundidade na análise de suas características. No que se refere à Segurança da Informação, este desafio cresce exponencialmente, visto a diversidade de fatores associados ao tema.

É preciso ter a visão de que a informação é o alvo, e que esta não se encontra mais confinada em ambientes físicos específicos, ou a processos isolados. A informação circula toda uma empresa, alimentando todos os processos de negócio, e está sujeita as variadas ameaças, furos de segurança ou vulnerabilidades, além de ser sensível a impactos específicos.

A todo instante nos negócios, seus processos e ativos fixos, tecnológicos e humanos são alvo de investida de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada.

Diante dos fundamentos articulados, a Segurança da Informação merece uma análise aprimorada, visto que muitos são os erros comumente praticados no momento de pensar neste tipo de segurança. Tais erros podem ser provocados pela distorção da questão. Existe uma tendência a se perceber os aspectos da segurança de uma forma muito substancial, apenas considerando e enxergando os problemas associados à tecnologia, mais precisamente Internet, redes, computador, e-mail, vírus e hacker. Em função disso, erros são praticados refletindo negativamente no negócio.

Contudo, com vistas aos fundamentos expostos frente à aplicabilidade e eficácia do sistema de segurança da informação de uma empresa, é importante identificar e planejar o tipo de projeto de segurança que a empresa necessita. Para tanto, há necessidade de apresentação do Retorno sobre investimento (ROI) no projeto, para que este seja validado e aprovado pela alta direção, visto que a empresa precisa de dados capazes de demonstrar se o investimento será vantajoso em curto, médio e longo prazo.

Sendo assim, alguns questionamentos norteiam o desenvolvimento do tema exposto no presente estudo. São eles:

De que forma o Corpo Executivo poderá se conscientizar frente aos aspectos da segurança, visto que se trata de um problema generalizado e corporativo, que

envolve os aspectos físicos, tecnológicos e humanos que sustentam a operação do negócio?

Os profissionais executivos e empresários têm administrado corretamente os riscos que suas empresas e negócios estão sujeitos por dependerem da informação?

De que forma a empresa poderá avaliar se a Segurança da Informação consiste em investimento ou despesa?

Temos como objetivo principal deste trabalho identificar qual seria a melhor concepção no tratamento do tema segurança da informação nas empresas, para tanto reuniremos dados referentes à complexidade do tema, analisando a Segurança da Informação, a fim de traçar um paralelo entre investimento/despesa por parte da empresa.

É importante ressaltar que a segurança é estudada, planejada e aplicada há décadas nas mais diversas atividades e com os mais diversos propósitos. Dentro de um contexto histórico, é possível observar que em épocas distintas os ativos eram os detentores da atenção e, dessa forma eram valorizados pelas empresas em seus negócios, porém, mudavam dinamicamente.

Os ativos mudaram, assim como os valores e a base de sustentação dos processos produtivos e operacionais dos negócios. Toda a forma de representar, manusear, armazenar, transportar e descartar o patrimônio da empresa também mudou e a tendência é continuar mudando dinâmica e rapidamente.

Diante de tantas mudanças, necessitamos de ferramentas que consigam comprovar o retorno sobre o investimento neste novo ambiente.

Muitas são as variáveis que interferem direta e indiretamente nos riscos operacionais de negócio. Mudanças que o fazem oscilar e sair do seu ponto de equilíbrio e, diante do dinamismo dessas diversas variáveis, as empresas necessitarão de algo igualmente dinâmico, que seja capaz de acompanhar com velocidade as variações do ambiente e ajustar os controles para manterem o nível de risco adequado. Porém só conseguiremos implementar estes controles se forem comprovados a necessidade bem como o retorno sobre o investimento.

Esta pesquisa é relevante porque envolve aspectos intimamente relacionados à Gestão da Segurança da Informação, procurando mostrar a importância de se mensurar o ROI com objetivo de conseguir obter os recursos necessários para implementar os controles necessários, e assim proteger o negócio.

O trabalho está dividido da seguinte forma:

No capítulo 1, demonstraremos a relevância do trabalho mostrando as mudanças que ocorreram na forma de representar a informação; neste capitulo convidaremos você a responder a seguinte questão: Segurança da Informação é uma despesa ou investimento.

No capítulo 2, vamos expor todos os conceitos relacionados com Segurança da Informação, mostraremos também técnicas de gerência de riscos e ferramentas para comprovação do ROI em soluções de segurança.

No capítulo 3, demonstraremos através de casos de uso como utilizar as ferramentas apresentadas no capítulo 2.

No capítulo 4, faremos uma análise em cima dos casos de uso apresentado no capítulo 3, neste momento já será possível responder a principal questão apresentada no capítulo1.

No capítulo 5, concluiremos nosso trabalho deixando algumas sugestões para trabalho futuro, bem como expondo a nossa visão sobre tema tratado.

2 **SEGURANÇA DA INFORMAÇÃO**

Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

A Segurança da Informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua disponibilidade (Dias, 2000).

Segundo Benson et al. (2000), segurança computacional significa proteção da informação. Ela trabalha com a prevenção e detecção de ações não-autorizadas por usuários de computador ou por ações da natureza.

De acordo com Sêmola (2003), o Modelo de Gestão Corporativo de Segurança da Informação empresta à expressão um sentido mais amplo, considerando em primeiro plano os desafios do negócio como um todo. Diante desta abrangente orientação, ganham autonomia mais dois conceitos de segurança (autenticidade e legalidade), originalmente extraídos dos três precursores em função de suas importâncias dentro no contexto atual.

A segurança da informação tem a proposta da garantia da confidencialidade, integridade e disponibilidade da informação, a impossibilidade de que agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a continuidade dos negócios.

Esta segurança apenas será alcançada através das práticas e políticas voltadas a uma adequada e eficaz padronização operacional e gerencial dos ativos, e processos que manipulam e exercem a informação.

Sêmola (2003), por sua vez, expõe os seguintes conceitos:

Informação: conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais. A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo chamados ativos, os quais são alvos de proteção da segurança da informação;

Ativo: todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada;

Autenticação: processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos;

Legalidade: característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes;

Autorização: concessão de uma permissão para o acesso às informações e funcionalidades das aplicações aos participantes de um processo de troca das informações, após a correta identificação e autenticação dos mesmos;

Auditoria: processo de coleta de evidências de uso dos recursos existentes, a fim de identificar as entidades envolvidas num processo de troca das informações, ou seja, a origem, destino e meios de tráfego de uma informação;

Disponibilidade: a informação ou sistema de computador deve estar disponível no momento em que a mesma for requisitada;

Autenticidade: garantia de que as entidades identificadas em um processo de comunicação como remetentes e/ou autores sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação. Normalmente, o termo autenticidade é utilizado no contexto da certificação digital, onde os recursos de criptografia e hash são utilizados para atribuir um rótulo de identificação às mensagens ou arquivos enviados entre membros de uma infra-estrutura de chave pública, visando garantir os princípios: irretratabilidade, identidade, autenticidade, autoria, originalidade, integridade e confidencialidade;

Severidade: gravidade do dano que um determinado ativo pode sofrer devido à exploração de uma vulnerabilidade por qualquer ameaça aplicável;

Relevância do Ativo: grau de importância de um ativo para a operacionalização de um processo de negócio;

Relevância do processo de negócio: grau de importância de um processo de negócio para o alcance dos objetivos e sobrevivência de uma organização;

Criticidade: gravidade referente ao impacto ao negócio causado pela ausência de um ativo, pela perda ou redução de suas funcionalidades em um processo de negócio, ou pelo seu uso indevido e não autorizado;

Irretratabilidade: característica de informações que possuem uma identificação do seu emissor que o autentica como o autor de informações por ele enviadas e recebidas.

No ponto de vista de Sêmola (2003), ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração das vulnerabilidades, ocasionando perdas de confiabilidade, integridade e disponibilidade e, conseqüentemente, causando impactos aos negócios de uma organização. O autor classifica as ameaças em três grupos, a saber:

Naturais: são aquelas decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.

Involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, etc.

Voluntárias: ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

2.1 GERENCIAMENTO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

Antes de analisarmos a Segurança da Informação, devemos saber o porquê de protegermos os ativos, quais os ativos devem ser protegidos e quanto custará a implementação dos controles de segurança.

A disciplina de gerenciamento de risco pode nos auxiliar em todo esse processo, pois possui as ferramentas e os modelos necessários que facilitará a análise de um ambiente organizacional. É só a partir da análise e consolidação dos dados obtidos que poderemos verificar se a solução é viável e se ela se enquadra como um investimento ou como uma despesa.

Cabe ressaltar que a segurança da informação não deve ser tratada como uma vaidade empresarial passageira, mas sim como uma necessidade, quer seja para proteger as informações e assim o negócio ou reduzir despesas. Bem sabemos

que a informação é o bem de maior valor que uma organização possui, e muitas vezes o prejuízo gerado por uma invasão ou um acidente qualquer que viole algumas das características da informação poderá gerar prejuízos bem maiores do que o custo de uma solução da segurança.

O risco pode ser compreendido como:

> [...] tudo aquilo que pode afetar nossos negócios e impedir que alcancemos nossos objetivos. Quando se está tratando de segurança da informação, risco corresponde a um grau de perda ou a possibilidade de um impacto negativo para o negócio. (MOREIRA, 2001, p. 20)

Neste contexto, pode-se definir o risco como sendo, a soma de ameaças (os eventos que causam danos), das vulnerabilidades (a abertura de uma brecha para as ameaças e valor dos ativos). O crescimento de qualquer um dos fatores leva a um crescimento do risco (FINNE, 1998).

A disciplina de gerenciamento de risco se divide em 3 fases.

Vejamos as fases:

- **Fase de Avaliação**

Esta é uma fase muito importante que deve ser realizada com o máximo de cuidado e com riqueza de detalhes; é nesta fase que iremos avaliar e atribuir valores aos ativos da empresa, identificar todos os riscos de segurança do ambiente para que possamos depois de uma análise verificar o que deve ser priorizado na solução, também nesta fase criaremos um documento que defina o planejamento e o agendamento dos riscos de segurança. Procuraremos responder nesta fase às perguntas: O que proteger? E por quê?

- **Fase de Desenvolvimento e Implementação**

Nesta fase iremos desenvolver e implementar soluções que resolvam os problemas encontrados na fase de avaliação. Logo se a fase de avaliação não for realizada de forma correta teremos uma falsa sensação de segurança, pois os

controles implementados não serão suficientes para manter o ambiente em um bom nível de segurança.

Cada procedimento realizado nesta fase deverá ser testado e documentado com objetivo de gerar registros de conhecimento relacionado aos riscos já conhecidos. Nesta fase iremos responder a seguinte pergunta: Como proteger? Quanto custa proteger?

- **Operação**

Esta fase lida com o processo de reavaliação de ativos e riscos de segurança novos e alterados e monitoração do ambiente, deve fazer parte do cotidiano da empresa, já que a segurança da informação deve ser dinâmica assim como os riscos do negócio são.

Se a fase de operação for executada de forma irresponsável teremos novamente uma falsa sensação de segurança, o que poderá gerar grandes prejuízos empresariais. Nesta fase deverão ser respondidas as mesmas perguntas das fases 1 e 2.

Planejar o gerenciamento de riscos possibilita o controle de possíveis efeitos negativos, além de potencializar os efeitos positivos.

2.1.1 **Resultados esperados após análise de riscos**

Após a análise de riscos teremos todos os dados relacionados à atual situação da empresa. É importante ressaltar que após a análise de risco deverá ser feito um mapeamento dos problemas encontrados para a linguagem do negócio. Em outras palavras queremos dizer que somente com dados monetários conseguiremos atenção do nível estratégico empresarial.

Acreditamos que quando o não investir gera prejuízo podemos dizer que investir traduz retorno, mesmo que não seja fácil identificar esta relação, ela existe e deve ser visualizada por todos os executivos.

Sendo assim esperamos ter os seguintes dados após a análise de riscos:

- Valores monetários atribuídos aos ativos.
- Listagem abrangente de ameaças significativas.
- A probabilidade de ocorrência da ameaça.
- A possível perda para empresa com base em cada ameaça ao longo de 12 meses.
- Salvaguardas, contramedidas e ações recomendadas.

Como pode ser percebido a disciplina de gerenciamento de risco é essencial na hora de avaliarmos se uma solução se encaixara no perfil de uma despesa ou de investimento, portanto se as fases do gerenciamento de risco não forem executada corretamente estaremos avaliando situações que não são as reais.

Quando comprovar o ROI de uma solução é uma exigência empresarial o gerenciamento de risco poderá gerar os dados iniciais para esse processo.

Não esperamos esgotar o assunto gerenciamento de riscos já que este não é objetivo do trabalho, mais informações podem ser obtidas junto à bibliografia desta monografia.

2.2 PANORAMA EMPRESARIAL

Devido ao grande número de ataques e invasões realizados contra empresas de pequeno, médio e grande porte, podemos perceber que houve um amadurecimento sobre assunto “segurança da informação” nas empresas.

Algumas mudanças positivas ocorreram na área de Segurança da Informação, nos dias atuais SI já é tema discutido pelo alto escalão da empresa, como poderá ser visto pela pesquisa abaixo.

As empresas estão começando a reorganizar a área de TI, surge à figura do Security Office, profissional responsável em traduzir as questões técnicas em SI, em uma linguagem que possa ser compreendida por todos os executivos.

Neste momento cabe expor qual é a situação atual das empresas no que se diz respeito a Segurança da Informação, utilizaremos as informações obtidas através de pesquisa pelo a empresa Módulo.

A 9ª Pesquisa Nacional de Segurança da Informação realizada pela empresa Módulo, analisa os dados coletados referentes ao ano de 2003.

Vejamos alguns pontos interessantes:

- As empresas guiam o processo de gestão de segurança da informação de forma normatizada utilizando regulamentações, normas, legislações, as mais utilizadas são: ISO17799, publicações do governo federal (decreto 4553 e outros), publicações do Banco Central (resolução 2554 e outras), Regulamentação da ICP-Brasil, COBIT e publicações da CVM (Resolução 358 e outras).

  Os dados obtidos acima demonstram que os padrões internacionais e nacionais estão sendo implementados, demonstram também que as empresas desejam apresentar a imagem de comprometida com a segurança para seus clientes bem como com a legalidade dos serviços oferecidos.

- As empresas estão conscientes dos riscos associados a sistemas eletrônicos, 78% dos entrevistados relataram isto.
- As empresas estão conscientes que a segurança da informação é necessária, pois 35% reconheceram que tiveram grandes perdas financeiras variando entre

os R$50.000 à R$ 1.000.000; houve um aumento também em relação às empresas que conseguem identificar os prejuízos gerados por um ataque ou invasão.

Os dados expostos acima são de extrema relevância para o nosso trabalho, pois indica que as empresas estão contabilizando o prejuízo gerado, essa contabilização gerará um banco de dados de extrema importância para a comprovação do ROI sobre uma solução de SI.

Os dados acima apesarem de serem positivos ainda demonstram que a maioria das empresas ainda não conseguem nem ao menos contabilizar os prejuízos gerados por falta de controles em SI, acreditamos que essa falta de controle seja o motivo de muitas empresas ainda tratarem a Segurança da Informação sempre como uma despesa.

- Mesmo com a conscientização da necessidade de Segurança da Informação 48% dos entrevistados não possuem nenhum plano de ação formalizado em caso de invasões e ataques.
- 60% das empresas afirmam que os investimentos em Segurança para 2004 vão aumentar.

Acreditamos que este aumento nos investimentos está sendo gerado devido à visualização pelas empresas dos seus prejuízos bem como o aumento de serviços oferecidos por meio de um ambiente eletrônico.

- Muitos obstáculos dificultam a implementação da Segurança nas empresas, falta de consciência dos executivos (23%) ainda continua sendo o maior, seguida pela dificuldade de mostrar o retorno (18%), como o terceiro obstáculo, temos o custo de implementação (16%) que aumentou de forma exponencial devido a complexidade das soluções.

- 51% dos entrevistados acreditam que os executivos consideram a segurança da informação fundamental para a integridade e continuidade de seus negócios, sendo que para 21% é fator vital e para 16% fator crítico.
- A maioria das empresas ainda centralizam a Segurança da Informação na área de TI, porém com 25,5% a figura do Security Office começa ser melhor visualizada como peça fundamental no processo de Gestão de Segurança da Informação.

Os pontos citados acima demonstram um paradoxo relacionado ao nível estratégico empresarial, podemos verificar que apesar dos executivos estarem conscientes com os problemas de Segurança, estes ainda são apontados como o maior obstáculo para implementação da Segurança da informação, acreditamos que este obstáculo diminua a partir do momento que o ROI seja melhor "entendido" e comprovado em SI, mas para isso acontecer deverá ser feita uma reestruturação na área de TI, pois somente com a criação de uma nova área que trate Segurança da Informação como necessidade do negócio e com a visualização na figura do Security Office o profissional responsável por mapear planos técnicos em uma linguagem do negócio será possível vencer as barreiras no momento de aprovar o projeto junto ao alto escalão da empresa.

Será que as empresas sabem o quanto estão vulnerável? Será que as empresas sabem o que proteger? Será que uma vez implementado a solução de segurança a empresa estará para sempre protegida?

As questões citadas acima são de extrema relevância para o nosso trabalho, pois somente conhecendo a situação atual da empresa o alto escalão poderá sensibilizar sobre o problema.

Para respondermos estas perguntas, veremos o que especialistas da área comentam.

Segurança da Informação é uma área dinâmica a certeza de ontem pode não ser a realidade de hoje, são muitas variáveis que devem ser analisadas diariamente e o que mais ocorre é o gap de conhecimento que é provocado essencialmente pela diferença entre a taxa do nível de conhecimento requerido em função da complexidade das soluções, e a taxa do nível de conhecimento da organização, veja na figura abaixo. (Bezerra, 2001)

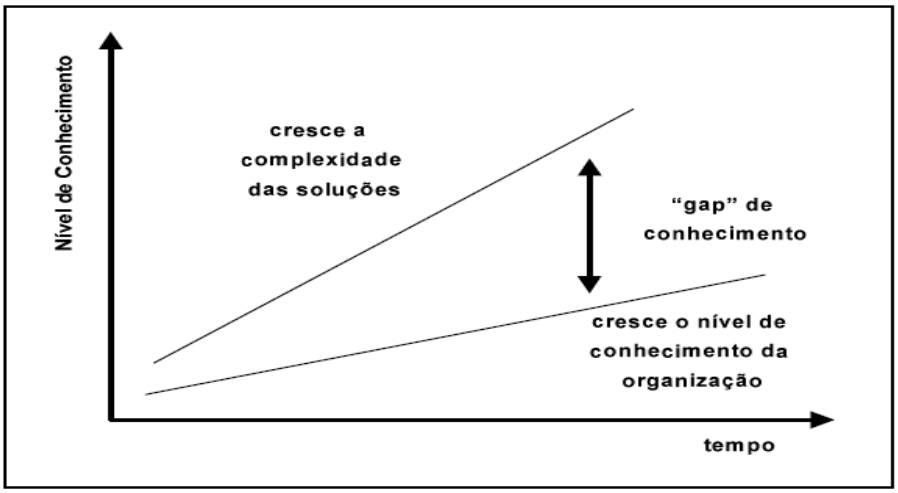

Figura 1 -O gap do conhecimento.

Moreira (2001, 21) criou um modelo denominado Ciclo da Segurança da Informação, onde é possível avaliar a importância dos riscos para a empresa. O autor inicia a sua análise expondo que todo negócio tem como base a informação e que esta, está sujeita as vulnerabilidades, permitindo ameaças que comprometem a sua integridade, bem como a confidencialidade e disponibilidade. Os riscos, os quais a informação pode estar exposta, podem causar impactos no negócio e, por isso, a importância de se tomar medidas de segurança a fim de minimizar os impactos e proteger a informação.

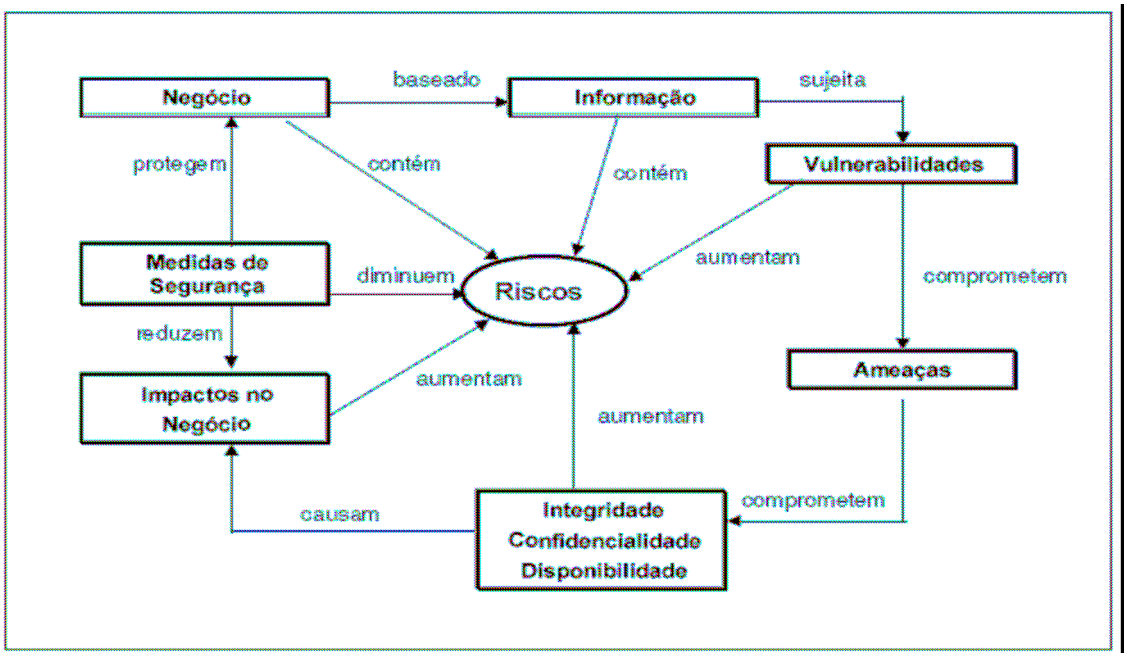

Figura 2 - Modelo do Ciclo de Segurança da Informação.

Diversos motivos podem levar as organizações a não terem Políticas de Segurança implementadas ou ineficazes. De acordo com Nery (2002, 02), é importante que se avalie como a segurança da informação é percebida pelo pessoal da empresa, dividindo a avaliação em duas visões, a saber: a) de que forma a segurança é vista pelos usuários, onde se avalia o ambiente pela sensação de segurança passada ao usuário; b) Aferição da segurança, realizada por especialistas, a fim de verificar se a mesma está adequada ou não.

Segundo Nery (2002), alinhar esta duas visões consiste em um dos maiores desafios da segurança corporativa, visto que nem sempre estas são compatíveis. Em meio a este conflito o ator define quatro cenários possíveis, como pode ser visto na figura 4.

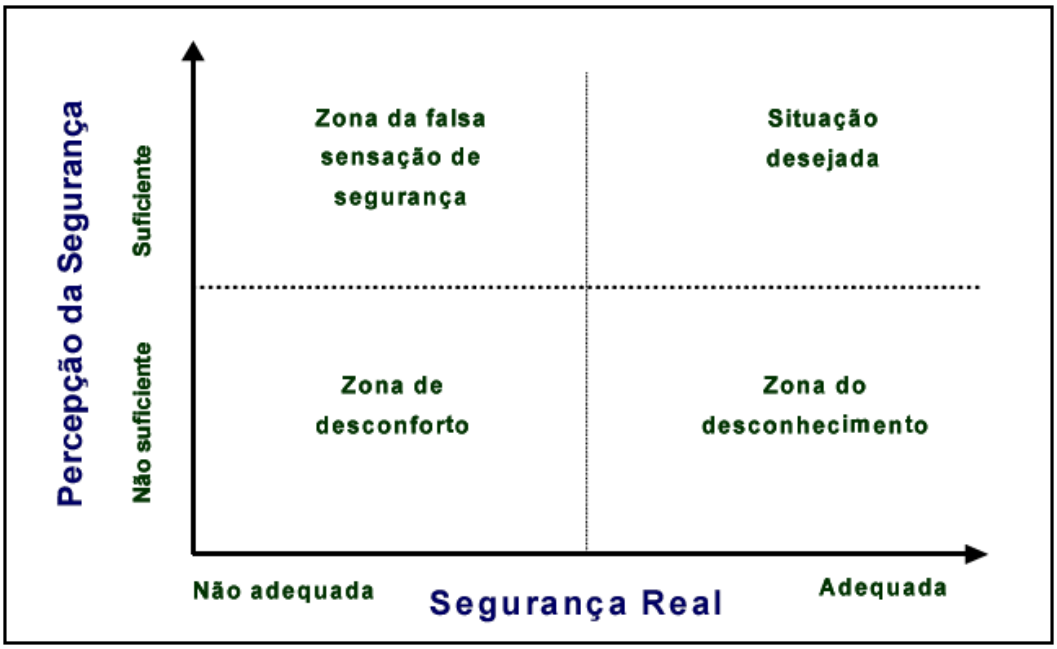

Figura 3 - Quadrantes da segurança, segundo a percepção das pessoas.

Atualmente, grande parte das empresas se encontra na zona da falsa sensação de segurança, onde os usuários consideram a segurança atual satisfatória, e o mesmo não é sentido nas análises técnicas. Isto faz com que haja uma acomodação por parte dos usuários, visto não haver o registro de ocorrências de vulnerabilidade no ambiente. Sendo assim, fraudes podem passar despercebidas e a sensação de ambiente seguro prevalece.

Pode-se considerar que este quadrante consiste em um dos principais motivos da falta de investimento em segurança, porque mesmo que as análises técnicas demonstrem a vulnerabilidade e o risco da segurança no ambiente, o fato dos usuários se acomodarem faz com que não haja investimentos.

Em algumas empresas é verificada a ocorrência da zona do desconhecimento. Em geral, existem sistemas sofisticados de segurança, porém, os usuários se sentem inseguros.

Daí o foco consiste em modificar a cultura do ambiente.

A zona mais adequada para o investimento em segurança é a zona de desconforto, pois existe uma percepção mais clara da realidade e as informações sobre vulnerabilidades são compartilhadas entre os usuários e a equipe técnica. Este é o momento mais adequado ao planejamento da segurança e à tomada de decisões sobre investimentos.

A situação desejada é o momento onde as empresas desejam se enquadrar. Os usuários se sentem seguros e foram implementados pela equipe técnica, os recursos de segurança. Nesta etapa, a segurança se encontra madura e consiste na única situação na qual é justificado o gerenciamento da segurança.

Nery (2002) explica que dificilmente haverá investimento significativo quando a empresa se encontra na zona da falsa sensação de segurança, sendo necessário, na grande parte das vezes, um choque para se chegar à zona de desconforto. No momento em que a empresa se mantém com uma falsa sensação de segurança, está completamente vulnerável aos riscos.

2.3 TÉCNICAS PARA COMPROVAR O RETORNO SOBRE INVESTIMENTO EM SI

Talvez demonstrar o ROI de uma solução de segurança seja a tarefa mais difícil na gestão da Segurança da Informação para o Security Office, porém sem essa demonstração é impossível sensibilizar os executivos para investir, cabe então ao Security Office mapear as soluções técnicas em uma linguagem que seja compreensível aos executivos, ou seja, a solução de segurança deve estar totalmente associada ao plano estratégico empresarial, sempre priorizando os processos de negócios onde danos poderão gerar maiores prejuízos para a empresa.

Mensurar o ROI é traduzir a linguagem técnica de SI para a linguagem estratégica, conhecida por todos os executivos; é demonstrar com fatos a

necessidade do investimento para o bem estar do negócio a pequeno, médio e longo prazo.

Somente a partir de uma análise de riscos e de um banco de dados com o histórico de prejuízos gerados pela falta de implementação de controles de segurança, será possível obter todos os dados para comprovar o ROI da solução.

Veremos então o que é ROI, qual a sua relevância na área de SI .

2.3.1 **ROI (Retorno sobre Investimento)**

Criado em 1977 pelo Gartner, ROI ou Retorno sobre Investimento é uma ferramenta antiga, com base matemática e econômica, construída através do cruzamento de dados reais relacionados a custos diretos, indiretos e intangíveis, e com a projeção de investimentos obtêm-se um excelente instrumento para nortear as ações dos executivos.

Sêmola (2003) explica que projetar o ROI de ações integradas e alinhadas com as diretrizes estratégicas da empresa representará eficaz ferramenta de conscientização e sensibilização do executivo, a fim de ganhar seu investimento.

Avaliar o custo, a rentabilidade, a receita, o lucro, os dividendos, o ganho de market share e valorização das ações, torna-se essencial para apoiar uma tomada de decisão.

Através do exercício do ROI é possível justificar altos investimentos, mudanças de rumo e estratégia, visto que o “retorno do investimento” é projetado.

Não existe um único modelo de ROI, nem tampouco um modelo certo ou errado. O que existe são abordagens e visões diferentes do mesmo objeto. A profundidade da análise interfere diretamente nesse modelo, agregando um número ainda maior de variáveis e refinamentos. Contudo, todas buscam uma resposta mágica para a pergunta: devo realizar este investimento? (SÊMOLA, 2003)

De acordo com Fontes (2003), apresentar o ROI em qualquer projeto aumenta a garantia de aprovação pela alta direção da empresa. Afinal, está sendo demonstrado que se a organização investir um determinado valor em um projeto, após algum tempo esse investimento realizado será pago e, muitas vezes, a organização continuará a ter vantagens por diminuição de perdas.

Hoje o orçamento de segurança de TI é justificado na maior parte das empresas pela necessidade de garantir os negócios e reduzir o risco das operações. É claro que ao reduzir riscos, a empresa acaba reduzindo custos associados e aumentando receitas, mesmo que estas não sejam facilmente mensuráveis. A questão é que isso não elimina a segurança da informação o fato de ser despesa, e despesa, todos sabem, quanto menor, melhor. É por isso que o objetivo de todos os departamentos de segurança da informação é comprovar seu ROI.

É muito mais confortável oferecer soluções à empresa que trazem redução de custos embutida do que simplesmente despesas – mesmo que necessárias ao funcionamento dos negócios.

Investir em tecnologia, principalmente em segurança da informação, consiste em um dos objetivos das organizações, visto que a minimização de riscos e sua sobrevivência também estão atreladas à segurança.

Todavia, as empresas vêm se questionando em relação ao investimento em TI, como demonstra Gurovitz (2001):

Despesa ou investimento? Esse sempre foi o dilema de quem gasta com tecnologia da informação. Pergunte aos diretores de informática e todos garantirão que é impossível viver sem computadores no mundo moderno. E terão razão. Mas, se o computador é um conforto, ele também possui um TCO (Total Cost of Ownership ou Custo Total de Propriedade). Saber quanto se gasta para manter a

estrutura tecnológica é apenas o primeiro passo para avaliar sua eficácia e sua eficiência. Sem isso, fica impossível dimensionar se o computador traz ou não o retorno desejado. (GUROVITZ, 2001, p. 40).

De acordo com Caruso e Steffen (1991), não se deve encarar uma política de segurança como mais um modismo passageiro que, freqüentemente, aparece em todas as áreas de atividades.

> "(...) estudo do ROI, definitivamente, já faz parte do cotidiano dos executivos de tecnologia, e a segurança da informação, em especial, já é pauta certa de reunião e motivo de sobra para ser considerado um investimento. Resta, antes de tudo, gerar e implantar mecanismos de controle que, preliminarmente, reúnam informações que sinalizem os eventos em que há quebra de segurança e registrem os efeitos ao longo do tempo. Com esses números, somados à projeções e simulações, será possível gerar um estudo de ROI capaz de traduzir na linguagem executiva o que ele realmente precisa entender: segurança é um investimento importante, necessário, mensurável e justificável." (SÊMOLA, 2003, p. 26-27)

Segundo Sêmola (2003), todo investimento tem seu ponto de inflexão, ou seja, um ponto na curva onde o retorno já não é proporcional ao esforço empregado, ou seja, seria o mesmo que investir em segurança um montante maior do que o próprio valor do bem protegido, considerando e ponderando, todos os aspectos associados à operação do negócio.

Neste contexto, Fontes (2003) identificou três situações para projetos, a saber:

a) Projetos que podem quantificar um ROI

Em algumas situações o ROI pode ser calculado com um alto grau de certeza. Por exemplo, projetos de implantação de uma nova ferramenta no ambiente computacional que vai diminuir as chamadas ao help desk e a indisponibilidade dos micros utilizados pelos usuários. Transformar as horas de help desk e dos usuários em valores que abaterão o custo da compra da ferramenta é perfeitamente possível.

b) Projetos que identificam um Meta-ROI

Quando é desenvolvido um projeto de plano de continuidade de negócio, uma das etapas é a realização da análise de impacto que pode ser conduzido através da ferramenta BIA (Bussiness Impact Analysys). Em um trabalho bem conduzido, é identificado o possível impacto (financeiro, de imagem e operacional) quando os recursos de informação, que suportam o negócio, ficarem indisponíveis. Utilizar um percentual do valor desse impacto para a aquisição dos recursos necessários para a continuidade do negócio é uma solução adequada.

Afinal, caso não tenha esses recursos, em uma situação de desastre, a organização terá um prejuízo muito maior. Porém, aqui se encontra uma diferença. O ROI somente acontecerá se ocorrer uma situação de indisponibilidade dos recursos. Nessa situação fica evidente que a organização fez um ótimo investimento. Mas, se o desastre ou situação de indisponibilidade não acontecer? Como será comunicado à direção que foi um investimento sem retorno? Nesse caso, pode-se calcular apenas o que o autor identifica como Meta-ROI. Os recursos disponibilizados para a continuidade de negócio somente serão considerados um investimento se acontecer um desastre.

c) Projetos que a segurança é despesa e parte do negócio

Em muitos outros projetos a segurança da informação é parte dos projetos. Por exemplo, em um projeto de e-commerce, alguém de sã consciência profissional vai avaliar qual o ROI para decidir se teremos segurança da informação? A proteção da informação faz parte do projeto. Evidentemente busca-se que a implementação da segurança tenha um custo e qualidade compatível com o negócio. Mas é uma despesa! Será investimento considerando o projeto de negócio como um todo.

Veremos agora os indicadores que são utilizados cálculo do ROI, a saber, são: as análises de custo por incidente (individualizada por evento), e análise de custos acumulados (geralmente mensal ou anual).

2.3.1.1 Indicadores do ROI

No cálculo do ROI utilizaremos alguns indicadores para mensurar em termos financeiros o impacto que determinado incidente poderá gerar para empresa.

O SLE (Single Loss Expectancy) ou expectativa de perda única é o indicador que permite analisar o impacto financeiro de um único incidente. Por exemplo, imagine que worm deixe um servidor WEB indisponível por alguns minutos, podemos calcular este incidente em termos financeiros, é a esta mensuração de um único incidente isolado que chamamos de SLE. Porém se tivermos uma base de dados estatística que nos permita saber qual é a taxa de ocorrência por ano deste incidente, digamos que no período de um ano este incidente ocorra 10 vezes, logo, podemos dizer que ARO (annualized rate of ocurrence) ou taxa anual de ocorrência para este incidente é de 10,0.

De posse dessa taxa podemos utilizar o resultado obtido pelo cálculo de um único incidente e multiplica-lo pela ARO, este novo resultado é o que chamamos de ALE (Annualized Loss Expectancy) ou expectativa de perda anual, e nos permite mensurar o impacto financeiro em um período (anual ou mensal).

Como encontrar o valor a ser utilizado como ARO?

Esta é uma pergunta que muitos Security Officers devem se fazer todas as noites, e realmente não é tarefa fácil e nem exata.

Muitos valores a serem considerados como ARO, podem ser obtidos através de consultores da área, tais profissionais têm know-how e já possuem uma boa base de dados estatísticas sobre incidentes. Outras fontes poderão ser utilizadas para

ajudar a estimar o valor da ARO, sites como o do CERT, boletins de segurança da Microsoft entre outros são bons locais para encontrar informações sobre incidentes.

Acreditamos que a melhor base dados sobre incidentes, será aquela gerada na própria empresa ao decorrer dos anos, contabilizando os incidentes e prejuízos a empresa terá um bom valor a ser utilizado como ARO ao longo do tempo.

O grande problema é que segundo pesquisa da empresa Módulo, 65% das empresas não conseguem quantificar o prejuízo gerado pelas invasões, em outras palavras, grande partes dessas empresas não sabem nem quando, nem como foram invadidas. Para essas empresas a melhor solução seria contratar uma consultoria para realizar este trabalho.

Vimos então que a ferramenta ROI possuí indicadores que deverão ser utilizados em conjuntos para que seja possível estimar as reais perdas que um incidente poderá gerar para uma organização. Não faz muito sentido elaborar um relatório que mensure o prejuízo gerado por um incidente isolado, os executivos precisam de dados que mensure os incidentes em um período.

Não há como calcular o ROI de forma correta sem que antes tenhamos feito a analise de risco, pois é na fase de avaliação da análise de risco que identificaremos todos os ativos, ameaças e vulnerabilidades existentes.

Calcular o ROI não é fácil, necessitaremos de dados, informações estatísticas e sempre que necessário auxílio de consultores da área.

Iremos demonstrar no capítulo 3, a utilização da ferramenta ROI em alguns casos.

2.3.2 **Retorno sobre investimento em Segurança da Informação (ROSI)**

Segurança da Informação sempre foi tratada pela área econômica com uma visão qualitativa, os recursos eram aplicados, mas sempre as justificativas eram:

⇒ Segurança representa um custo agregado ao negócio.

⇒ Novos negócios dependem da Segurança da Informação para sua proteção.

⇒ A Internet está se tornando um ambiente muito perigoso, expor as informações sem pensar em segurança das mesmas pode nos trazer grandes prejuízos.

⇒ Nossos sistemas não podem parar.

Todas as justificativas acima são boas, porém nenhuma delas demonstra um ganho quantitativo sobre a utilização da SI, e quando isso acontece, segurança se torna uma despesa necessária. Como bem sabemos, despesas quanto menos, melhor.

Já algum tempo grupos de pesquisas têm estudado este assunto: “como demonstrar o ROI em Segurança da Informação?”.

Pois quando tivermos ferramentas que possibilitem mensurar o ROI em SI, teremos mais chances de aprovar os projetos de segurança, junto ao alto escalão da empresa.

Um dos grandes problemas é que nesse campo a relação custo benefício não pode ser medida nos mesmos termos, ou seja, não é fácil demonstrar que a implementação de um controle de segurança irá gerar no período “x” o valor “y” em reais.

Algumas soluções surgiram para resolver este problema, a saber, o ROSI que significa Retorno sobre Investimento em Segurança da Informação (ROSI), esta ferramenta é uma adaptação do ROI que já é utilizado a muito tempo nos mais diversos campos, e tem como objetivo mensurar o ROI feito em SI.

A partir desta ferramenta será possível justificar os controles implementados e planejar investimentos futuros, já que agora teremos a possibilidade de mensurar de forma quantitativa o retorno sobre o investimento feito nos projetos de segurança.

Vejamos então a fórmula criada pela Universidade de Idaho para cálculo do ROSI em um cenário específico (Segurança do Perímetro):

(R-E)+T = ALE, e R – ALE = ROSI

A variável “R”, dessa fórmula representa o custo anual que uma empresa gastaria para recuperar-se de uma intrusão. O Security Officer necessitará de apoio dos demais departamentos da empresa para calcular esse valor, por exemplo, imagine que a indisponibilidade por 20 minutos de um sistema de e-commerce gere para a empresa o prejuízo de R$ 50.000,00, isto sem contar com o perda de market share, reputação, perda de cliente para concorrentes, etc. Estes valores só podem ser estimados pelas pessoas ligadas ao negócio da organização, pois estão relacionados com os processos de negócio, valor das informações, etc.

A variável “E”, representa a economia gerada por se interromper uma intrusão. Se a empresa sabe qual é o prejuízo que uma intrusão gera, é bem fácil descobrir qual seria o ganho caso consiga interromper essa intrusão.

A variável “T” representa o custo da ferramenta de detecção de intrusão. È importante acrescentar nesta variável os custo de manutenção, pessoal, licenças e outros custos indiretos, para que assim possamos ter um valor real do custo da ferramenta.

A variável ALE, representa a Expectativa de Perda Anual e como já foi dito, somente teremos uma boa estimativa se os departamentos envolvidos com o negócio da empresa estimarem este valor em conjunto com o Security Officer.

Se a empresa conseguir calcular essas variáveis poderá utilizar está fórmula com um bom ponto de apoio nas suas estimativas quantitativas do retorno sobre investimento.

2.3.2.1 Quando o ROSI não pode ser calculado

Como pôde ser visto no capítulo anterior, calcular o ROSI não é tarefa fácil. Somente empresas que conheçam muito bem do seu negócio, e que possuam dados contábeis que permitam gerar os valores a serem utilizados pelas variáveis da fórmula do ROSI, terão sucesso, e é por isso que muitas empresas não conseguirão calcular o ROSI, e tratarão de forma errada a SI como uma despesa do negócio.

O fato de uma empresa não conseguir calcular o ROSI, não quer dizer que SI é uma despesa, o que acontece, é que tal empresa ainda não atingiu um grau de maturidade sobre seus processos de negócio, sendo assim não sabem o quantificar seus prejuízos quando são invadidas.

Empresas que não conseguem quantificar os prejuízos gerados pela falta de SI, irão pelo caminho errado e tratarão a SI como uma despesa, utilizando ferramentas como o TCO (Total Cost of OnwerShip) para quantificar os custos com SI.

O TCO, ou custo total de propriedade como é conhecido permite calcular todos os custos associados com hardware, software ou até mesmo serviços, itens como: manutenção, licenças, upgrade, suporte técnico, treinamentos entre outros são somados e permitem calcular o custo total de propriedade.

Quando incluirmos a SI no cálculo do TCO, ela é vista como uma despesa, sendo assim na maioria dos casos a solução de segurança dimensionada, pode ser a incorreta, muitas empresas irão por este caminho por ser mais fácil, e

principalmente devido a imaturidade empresarial relacionada aos processos de negócio e também por não conhecerem o valor da informação gerada na empresa.

O caminho do TCO não possibilita a visão de retorno sobre investimento em Segurança da Informação pois o cálculo não trabalha com variáveis que medem a expectativa de perda anual (ALE) ocasionada por invasões. O cálculo do TCO somente permite calcular o quanto custará para a empresa manter este ou aquele controle de segurança.

Veja no capítulo 3 um exemplo de cálculo de TCO associado com a SI.

3 VISUALIZAÇÃO DO ROI ATRAVÉS DE CASOS DE USO

Veremos através de alguns casos de uso como comprovar que SI é um investimento que pode ser mensurado, aplicaremos as técnicas comentadas no capítulo 2, desta forma será possível comprovar suas utilidades.

Cabe ressaltar que a tarefa de estimar o retorno em SI não é uma tarefa simples, são muitas variáveis e muitos destas não possuímos o controle total, de forma que trabalhamos no campo da probabilidade e da incerteza, porém embasado com dados estatísticos.

Não temos como objetivo demonstrar normas ou técnicas de gestão de riscos, nem como elaborar uma política de segurança. Cabe ao leitor procurar informações sobre esses assuntos e depois de ter uma política de segurança adequada aos riscos do negócio utilizar os casos de uso aqui demonstrados para inferir sua realidade.

Como ROI em SI é também uma questão de sensibilidade, a afirmação feita em nossos exemplos pode estar em discordância com a sua, pois tudo depende do ambiente, negócio e das variáveis envolvidas.

Segundo Linda McCarthy, autora de “IT Security: Risking the Corporation, o grande números ataques cibernéticos continua crescendo dia-a-dia. Razão mais do que suficiente para tornar segurança parte do processo empresarial.

3.1 UTILIZAÇÃO DA FERRAMENTA ROI

Consideremos uma hipotética empresa que possui um sistema proprietário para administração do departamento financeiro. Este sistema foi desenvolvido ao longo de um ano por uma equipe de cinco pessoas que utilizavam cento e sessenta horas por mês. Com um salário de R$3.000,00 para cada um, estimamos um custo/hora na casa de 20,00 (acrescido encargos, benefícios e outros).

Uma vulnerabilidade no servidor principal deste sistema explorada por uma ameaça - funcionário insatisfeito, crackers através da Internet, sabotagem – causaria danos que na melhor das hipóteses dispenderiam o esforço de revisão de todo o código fonte da aplicação.

O prejuízo deste sistema pode ser calculado da seguinte forma:

8(horas/dia) x 240 (dias/ano) x 5 (número de pessoas) = 9.600 horas

R$ 20,00 (custo/hora) x 9.600 (horas) = R$ 192.000,00

Prejuízo total de R$ 192.000,00 – 100%. Destruição total dos arquivos, inexistência ou indisponibilização das cópias de segurança (backup). Isto é quanto custa o ativo do exemplo supracitado.

Agora só resta decidir o quanto vale a pena investir em segurança, pois já possuímos uma métrica para a definição de um prejuízo total.

O exemplo acima citado demonstra com clareza que o investimento em segurança traria um retorno, porém desde que fosse implementado o controle correto, levando em consideração a probabilidade da invasão acontecer; alguns pessoas podem dizer mas só haveria retorno caso o servidor fosse invadido. Como já foi dito é possível através de dados históricos de invasões que aconteceram na empresa, através de consultorias, através de institutos como o CERT (Computer Emergency Response Team) conseguir um bom valor para ser utilizado como probabilidade.

No caso acima fica a cargo do executivo correr o risco ou não, já foi mostrado que o investido trará um retorno.

Vejamos outro exemplo em que o ROI poderia ser mensurado.

Este exemplo demonstra os prejuízos gerados e que geralmente não são contabilizados.

Nos dias atuais a maiorias das organizações utilizam a Internet como meio de comunicação entre funcionários ou como plataformas de novos negócios.

Quando os recursos de conectividade para o desempenho de atividades são utilizados para outros motivos sem relação alguma com o negócio da organização, é sem dúvida motivo de preocupação. Salas de bate-papo e páginas de mulheres nuas lideram o ranking das “atrações” que mais tomam tempo dos funcionários (diminuindo a produtividade) e banda da organização (tornando a conexão com o mundo insuportavelmente lenta).

Imaginemos o seguinte cenário:

Uma empresa com 500 funcionários, onde 75% possuem acesso à rede.

Cada um destes 375 funcionários utiliza uma hora por semana para “brincar na rede”. Com um valor/hora na faixa de R$10,00 ficamos com um prejuízo acumulado de:

375 (funcionários) x 1 (hora por semana) x 44 (semanas) = 16.500 horas

R$ 10,00 (custo/hora) x 16.500 (horas) = R$ 165.000,00

São 165.000,00 reais perdidos anualmente. Sem contar a utilização da banda contratada pela sua organização, com os riscos de baixar um worm, spywares em sites maliciosos.

Muitas vezes a reclamação de um link lento pelos os funcionários deve-se a falta de controle no acesso dos mesmos, uma política de segurança poderia resolver este problema através de controles no acesso.

Muitas vezes a questão acima passa despercebida pelos responsáveis da área de TI e os executivos não enxergam o prejuízo gerado, cabe ao Security Office estar atento a todos os detalhes.

Seria quase impossível conseguir recursos para implementar uma solução de Proxy para resolver o problema acima, se não demonstrássemos a expectativa de perda anual através da má utilização dos recursos de informática.

Uma coisa é dizer para os executivos que temos que instalar um servidor Proxy para controlar o acesso dos usuários com a Internet, outra coisa totalmente diferente é mostrar para os executivos que com a instalação de um Proxy podemos estar ganhando 165.000,00 por ano e uma melhor qualidade no acesso para fins comerciais. A quem diga que a empresa não ganhará 165.000,00 simplesmente estará utilizando de forma melhorada seus recursos humanos e tecnológicos.

Essa é uma questão de visão, acredito que quando reduzimos custos com a utilização da segurança da informação, provocamos o ROI em SI, mesmo que seja um META ROI, ele existe, e os cálculos demonstram isso.

3.2 UTILIZAÇÃO DA FERRAMENTA ROSI

Vejamos um caso específico da utilização da ferramenta ROSI. A simulação foi realizada por um grupo de pesquisa da Universidade de Idaho para comprovar que o custo-benefício em cima da utilização de um sistema de detecção de intrusão (IDS) criado pelo mesmo grupo, seria a melhor solução em relação ao qualquer outro método.

Vejamos suas conclusões:

Após várias análises, concluíram que um IDS que custa 40 mil e têm uma eficiência de 85% gera um ROSI de 45 mil em uma rede na qual se espera que se perca anualmente 100 mil, como resultado de uma intrusão.

Vejamos o cálculo:

(R - E) + T = ALE	**R – ALE = ROSI**
(100.000 – 85.000) + 40.000 =ALE	100.000 – 55.000 = ROSI
15.000 + 40.000 =ALE	ROSI = 45.000
ALE = 55.000	

Onde temos:

R = custo anual para recuperação de uma intrusão

E = economia gerada por interromper-se uma intrusão

T = custo da ferramenta IDS

ALE = Expectativa de perda anual

ROSI = Retorno sobre investimento em segurança da informação

O grupo da Universidade Idaho, concluiu empiricamente que o IDS criado permitiria bloquear 85% das tentativas de invasões. A variável “R” foi estimada pela organização levando em consideração seus ativos e serviços.

A variável “E” foi estimada levando em consideração a eficiência da ferramenta de detecção de intrusos, logo, se a ferramenta tem uma eficiência de 85% e o custo anual para recuperar-se de uma intrusão é de R$ 100.000,00, inferimos o valor de “E” em R$85.000,00.

A variável “T” representa os custos da ferramenta de IDS, neste caso não acrescentamos custos indiretos.

A variável ROSI demonstrou o retorno que este controle traria para uma hipotética empresa. O ROSI poderá aumentar ou diminuir, tudo dependerá da expectativa de perda anual (ALE), em pequenas empresas o custo desta ferramenta poderá não ser viável dado a expectativa de perda anual.

O exemplo acima demonstra somente uma situação, cada empresa deve verificar seus problemas através da análise de risco, escolher os controles que melhores se enquadram aos seus problemas e calcular o ROSI em cima destes.

Após todo esse trabalho poderá ser gerado um relatório para ser analisado pelo alto escalão da empresa. A probabilidade de conseguir os recursos utilizando esse método é bem maior, pois estamos demonstrando se a empresa investir "x" terá um retorno estimado de "y".

3.2.1 **Analisando a SI no cálculo do TCO**

Vamos aproveitar esse momento para analisar a mesma situação acima, porém agora iremos supor que a empresa não conseguiu calcular o ROSI por que faltavam informações sobre seus processos de negócio, faltava conhecimento sobre o valor da informação e faltava a visão de SI associada ao plano estratégico empresarial. Sendo assim a empresa utilizou a ferramenta TCO para verificar o quanto custaria a solução de segurança.

As premissas para se avaliar o custo de um Sistema de Detecção de Intrusos, foram:

- Necessitamos de proteger nossa informação.
- Não podemos ficar com nossos sistemas indisponíveis.

O grande problema das justificativas acima que elas não mensuram o prejuízo gerado por uma invasão que violem a integridade, confidencialidade ou disponibilidade das informações.

Vejamos então tudo que deve ser adicionados no cálculo do TCO:

- Custo de aquisição do IDS (CA) – este custo está ligado ao appliance (Hardware e Software) comprado. Vamos assumir que compramos este equipamento por R$ 40.000.

- Custo de Licenciamento (CL) – custo anual de licenciamento do IDS. Vamos assumir que este custo seja de R$ 2.000.
- Custo com Pessoal Qualificado (CPQ) – este custo está relacionado com os técnicos e operadores do IDS, no nosso exemplo, vamos assumir que 2 técnicos e 1 operador são os responsáveis. Cada técnico recebe 3.000 mensalmente e operador 2.000. Totalizando um total anual de aproximadamente R$ 96.000.
- Custo com treinamento (CT) – este custo está associado com o treinamento de todos os envolvidos com o IDS. Vamos assumir que por ano a empresa gasta R$ 5.000 com treinamento.
- Custo com Suporte (CS) – este custo é relativo ao valor anual pago ao fabricante do IDS em relação ao suporte e consultoria prestado. Vamos assumir que este valor seja de R$ 12.000.
- Custo com Manutenção (CM) – este custo é inerente a manutenções preventivas e corretivas do appliance. Vamos assumir que este valor seja de R$ 6.000 anualmente.
- Custo de Upgrade (CU) – este custo é inerente a atualizações tanto de software do IDS quanto de Hardware. Vamos utilizar o valor de R$ 5.000 anualmente.

TCO (IDS) = CA + CL + CPQ + CT + CS + CM + CU

Os valores que serão utilizados na fórmula são fictícios, e tem como objetivo nos dar uma base de referência.

TCO (IDS) = 40.000 + 2.000 + 96.000 + 5.000 + 12.000 + 6.000 + 5.000

TCO (IDS) = R$ 166.000,00

O Custo Total de Propriedade nesse cenário específico é de R$ 166.000, um valor alto. Um dos problemas do TCO é que ele não analisa a vantagem sobre a aplicação realizada. Neste exemplo 166.000,00 parece um valor muito alto, porém isso depende do valor da informação da empresa, do valor dos processos de negócios. Muitas empresas perdem milhões quando seus processos de negócio ficam indisponíveis, tudo depende do cenário, e isso o TCO não calcula, o ROSI é que nos permite verificar os ganhos sobre o investimento feito em SI.

4 **ANÁLISE DO ROI**

Antes de analisarmos o ROI fica a reflexão abaixo para todos os executivos.

"*Se a sua empresa gasta mais em café do que em segurança de TI, você será invadido. Aliás, falando francamente, você merece ser invadido*", quem disse isso foi Richard Clarke, assessor de segurança de TI da Casa Branca em uma coluna da revista Time no ano de 2003. Mais do que ninguém, ele sabe o quão importante essa questão se apresenta nos dias de hoje.

Como foi visto através dos exemplos no capítulo anterior o ROI em segurança da informação existe e pode ser mensurado, cabe ao Security Office adequar cada ferramenta a sua realidade. Contudo é impossível demonstrar ROI em segurança da informação sem uma base de dados sólida sobre prejuízos gerados por invasões, análise de impacto do negócio, análise de riscos e sensibilidade dos executivos.

Outra questão muito importante a ser levada em consideração é que o ROI em SI, pode ser melhor compreendido se for visto como um META ROI ou valor agregado ao negócio, ou seja, é necessário o investimento por que dada a probabilidade de uma invasão ou evento acontecer, o prejuízo gerado será bem maior do que o custo do controle.

As pesquisas indicam que a indisponibilidade de processos de negócios com mais intensidade aqueles que são unicamente realizados de forma eletrônica, é o fator que mais gera prejuízos para as empresas. Analistas industriais da Enterprise Management Associates estimam que grandes casas de comércio internacional, podem sofrer perdas acima de 5 milhões de dólares por hora quando as operações são afetadas. E esse valor assustador somente leva em consideração custos diretos, como por exemplo, infra-estrutura fora do ar e transações perdidas. Quando custos

indiretos como, reputação, perdas de mercado e vendas são incluídos, as perdas podem disparar, chegando às vezes a bilhões.

A sexta edição da Global Information Security Survey, depois de ouvir executivos da área de TI de 1400 empresas em 66 países, constatou que mais 60% dos entrevistados não utilizam nenhuma ferramenta para mensurar o ROSI. Essa constatação talvez explique por que o investimento em segurança ainda não se tornou concreto em todas as organizações.

A constatação acima demonstra por que muitas vezes segurança da informação é vista como uma despesa pelo alto escalão da empresa, e como qualquer despesa, quanto menos, melhor.

É necessário mostrar aos executivos que os investimentos em segurança trarão benefícios e reduzirão despesas futuras e problemas voltados ao controle e alteração de informações.

Dito tudo isto temos certeza que segurança da informação é um investimento, pode ser comprovado, poder ser compreendido pelos executivos através de números, e sempre deve caminhar junto ao plano estratégico empresarial.

Quando a empresa não conseguir contabilizar o valor da suas informações ela escolherá o caminho mais fácil porém errado que é tratar SI como uma despesa e serão utilizadas ferramentas que mensuram o custo total de propriedade.

5 **CONCLUSÕES**

Nos dias atuais todas as empresas sabem que devem proteger seus ativos e com isso a informação, essa constatação pode ser verificada através das diversas pesquisas consultadas. A pesquisa realizada pela empresa Módulo no ano de 2004 verificou que 60% dos entrevistados indicaram que os investimentos iriam aumentar nos próximos anos. Porém a pesquisa não respondia o maior problema da SI: como justificar os recursos aplicados para proteger este bem tão valioso chamado informação ?

A resposta a essa pergunta, pode mudar um dos maiores problemas da área de Segurança da Informação, que é a reprovação pelo o alto escalão da empresa de grande parte dos projetos de segurança. Os executivos sabem da importância da SI para empresa, mais daí aprovar o projeto é outra coisa.

Fomos buscar o motivo da Segurança da Informação ser tão mal compreendida por alguns executivos, vimos que o maior problema está relacionado com a visão dada a SI pela empresa. Algumas acreditam que SI é uma despesa já outras defendem que SI é um investimento.

Após analisarmos essa questão cuidadosamente, vimos que a resposta não é simples por ser tratar de uma questão complexa. No entanto essa resposta existe, e está embasada por ferramentas que calculam o Retorno sobre Investimento em Segurança da Informação.

Concluímos utilizando o ROI e posteriormente a ferramenta ROSI que a SI traz um retorno para as empresas, um retorno quantificável em valores monetários, que poderá ser utilizado para justificar o projeto junto ao alto escalão da empresa. Contudo essas ferramentas não são mágicas precisam de dados que somente as empresas organizadas possuirão, e é só a partir dos dados contábeis e estatísticos

da empresa que será possível estimar os valores para serem utilizados na fórmula do ROSI.

Foi possível verificar através de exemplos no capítulo 3, que a não adoção de um IDS provocaria grandes prejuízos para a empresa, e se implementássemos o IDS a empresa teria um retorno sobre o investimento, o que mais uma vez demonstra que SI é um investimento.

Cabe ressaltar, que para o calcularmos o Retorno sobre Investimento em Segurança da Informação, teremos que ter feito antes: análise de risco, análise de impacto do negócio e também possuir uma base de dados sobre prejuízos gerados por invasões.

Como já foi dito Segurança da Informação é um investimento, e se a sua empresa não consegue calcular é por que você não possui informações sobre seus processos de negócios, os riscos do seu ambiente e o valor das informações da empresa.

O que acontece é que em empresas desorganizadas, a SI é tratada de forma totalmente errada, como uma despesa, e é incluída somente nos cálculo do TCO, sendo assim não é dada a devida importância ao assunto, o que irá gerar grandes prejuízos no futuro para a empresa. O que deve ficar claro, é que a visão da empresa neste caso esta errada.

Sugerimos que as empresas calculem também o TCO dos projetos de SI, mas que depois utilizem este valor na variável do ROSI que trata do custo de aquisição da ferramenta, pois dessa forma o valor colocado na variável assumirá todos os custos diretos e indiretos. Quando o TCO é analisado isoladamente na maioria das vezes os controles de segurança não serão implementados, pois não existirá uma correlação com a vantagem obtida em valores monetários sobre a

implementação dos controles, o que faria a SI ser tratada de forma errada e vista pelos executivos como uma despesa, o que justificaria muitas vezes a reprovação do projeto de segurança.

Sabemos que medir o ROI em Segurança da Informação é uma questão complexa, e por isso muitas vezes é mal entendida, esperamos que as ferramentas disponíveis sejam melhores estudadas por cada empresa e adaptada ao seu negócio, para que assim seja possível produzir o ROSI no seu ambiente. Saiba, o ROSI existe e pode ser quantificado.

Acreditamos que no momento que o Security Office possuir os dados, que provém para o alto escalão da empresa, que implementar o controle de segurança, trará um retorno, será mais fácil obter a aprovação do projeto, porém só obteremos esta mensuração do retorno utilizando ferramentas como o ROSI.

Acreditamos que a palavra de ordem em SI deve ser moderação, ou seja, analisar o ambiente, quantificar o ROSI, implementar controles para os riscos que causam grande impacto e trabalhar com algum risco residual. Mas uma vez fica claro que tudo depende da análise do negócio, pois o que para algumas empresas causam grande impacto para outras não.

Em relação às ferramentas disponíveis concluímos que são eficazes, são originárias da área econômica, muitas empresas já as utilizam com sucesso. No decorrer do trabalho podemos perceber que muitos grupos de pesquisas estão estudando o assunto para melhorar essas ferramentas, no futuro podemos esperar otimizações, no entanto nunca haverá uma fórmula mágica que uma organização possa utilizar, mas com um pouco de análise do negócio, análise de riscos, dados estatísticos e técnicas eficientes todas as empresas podem mensurar o ROSI.

Outra questão importante que foi possível visualizar com esse trabalho é que em empresas que não possuem um setor de segurança com autonomia e com conhecimento do negócio da organização, a SI é mal compreendida. Por isso sugerimos a estas empresas, que desmembre o departamento de TI e crie um departamento que cuide somente da segurança da informação. Porém lembre-se, que pouco adiantará um departamento de SI que pense somente na parte técnica, esta visão que tem que acabar, SI não é um fim é um meio, só existe para proteger o negócio.

Sugerimos também se sua empresa não possui know-how para demonstrar o ROSI que contrate uma consultoria na área para tal serviço, sua empresa pode estar perdendo muito dinheiro e você nem sabe.

Considerando as conclusões acima, este trabalho pode ser visto como auxílio para o entendimento do processo de mensuração do ROSI, bem como apontar pontos que devem ser verificados para que haja um amadurecimento no departamento de Segurança da Informação.

Fica uma proposta para trabalhos futuros, que é estudar por que o ROSI não é utilizado por grandes partes das empresas já que foi comprovado a sua eficiência.

REFERÊNCIAS

BENSON, C. **Microsoft Solutions Framework: Best Practice for Enterprise Security.** Disponível em http://www.microsoft.com/technet/security/bestprac/bpent/bpent.sec >Acesso em 31/01/2006.

CARUSO, C. A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** São Paulo: SENAC, 1991.

DIAS, C. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

FERREIRA, A. **Dicionário Aurélio eletrônico. V. 2.0**. Rio de Janeiro: Nova Fronteira, 1996.

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

FONTES, E. L. G. **Vivendo a segurança da informação**. São Paulo: Sicurezza, 2001.

FONTES, E. ROI, **Meta-ROI e Despesa**. Artigo publicado na It Web em 13/11/2003. Disponível em <http://www.itweb.com.br/colunistas/artigo.asp?id=44619>. Acesso em 05 de dezembro de 05.

GUROVITZ, H. **Falta de medida**. Revista Exame. 18 de abril de 2001.

MOREIRA, N. S. **Segurança mínima – uma visão corporativa da segurança de informações.** Rio de Janeiro: Axcel Books do Brasil, 2001.

NERY, F. **Segurança Percebida versus Segurança Real do Mundo Corporativo.** Disponível em <http://www.modulo.com.br>. Acesso em 30 de Janeiro de 2006.

SÊMOLA, M. **As sete ações de empresas muito eficazes em Segurança da Informação.** Disponível em: <http://www.semola.com.br/WebSite99/SWebArtigo53.htm>. Acesso em Maio de 2002.

GLOSSÁRIO

Ataque: O ato de tentar desviar dos controles de segurança de um sistema. Um ataque pode ser ativo, tendo por resultado a alteração dos dados; ou passivo, tendo por resultado a liberação dos dados. Nota: O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes.

Auditoria: Revisão e exame dos registros e das atividades do sistema para avaliar sobre sua confiabilidade, executados com independência.

Autenticação: Verificação reivindicada de uma identidade. O processo de determinar a identidade de um usuário que esteja tentando alcançar um sistema.

Autorização: O processo de determinar que tipos de atividades são permitidos. Geralmente, a autorização está no contexto da autenticação: uma vez que você autentica um usuário, está também autorizando acessos e/ou atividades. O poder dado pela gerência aos indivíduos específicos que permite que aprovem transações, procedimentos, ou sistemas; inclusive conceder direitos de acesso a um usuário, a um programa, ou a um processo.

Criptografia: “estudo da grafia secreta, isto é, o estudo de métodos para esconder o conteúdo de mensagens ou dados armazenados. O processo de cifragem corresponde à transformação da mensagem original em algo ininteligível, utilizando um código secreto – a chave criptográfica. A decifragem, por sua vez, é o processo inverso, isto é, de recuperação da mensagem original a partir de sua forma criptografada”. (Dias, 2000).

Firewalls: “dispositivos utilizados na proteção de redes de computadores contra ataques externos, dificultando o trânsito de invasores entre as redes”. (Dias, 2000).

Hacker: Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a um determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de Craker, Lammer ou BlackHat.

Internet: termo derivado da palavra inglesa Internetworking, que significa interconexão de redes. A Internet, na verdade, é composta por uma infra-estrutura computacional e de telecomunicações que propicia a transferência de informações por redes espalhadas por diversos países (Dias, 1999). “Rede mundial de computadores”. (Ferreira, 1996).

Intranet: aplicação da tecnologia Internet no âmbito interno da empresa.

Intrusion Detection: A detecção dos arrombamentos ou das tentativas de arrombamento por processos manuais ou através dos sistemas que operam sobre os registros ou a outra informação disponível na rede.

IP Splicing/Hijacking: Um ataque no qual uma sessão ativa, já estabelecida, é interceptado pelo atacante. Os ataques deste tipo podem ocorrer depois que uma autenticação foi feita, permitindo ao atacante passar-se pelo papel de um usuário já autorizado.

IP Spoofing: Um ataque em que um sistema assume ilicitamente a personalidade de outro sistema usando seu endereço de rede.

Logging: Processo de estocagem de informações sobre eventos que ocorreram num firewall ou numa rede.

On-line: “diz-se da possibilidade do usuário desenvolver uma ação recíproca ou interação com o computador”; “dispositivo periférico que pode operar sob o controle do computador ou em comunicação direta com ele”; “estado de um equipamento ou terminal quando este efetua transmissão de dados diretamente pelas linhas de comunicação de uma rede; conectado à linha”. (Ferreira, 1996).

Página web: página hipertextual disponível na Internet ou na Intranet. O termo web é usado para designar a própria rede Internet/Intranet ou a tecnologia que nela é utilizada.

Password: Uma única palavra ou seqüência de caracteres usada para autenticar uma identidade. A senha é confidencial, opostamente a identificação do usuário.

Política de Segurança Corporativa: Conjunto de diretrizes, normas e procedimentos que regulam como os ativos, incluindo informação sensível, serão gerenciados, protegidos e distribuídos para os usuários de uma organização.

Portal corporativo: conceito considerado uma evolução do uso das Intranets, incorporando, a essa tecnologia, novas ferramentas que possibilitam identificação, captura, armazenamento, recuperação e distribuição de grandes quantidades de informações de múltiplas fontes, internas e externas, para os indivíduos e equipes de uma instituição (REYNOLDS, 1999). Também denominado portal de informações empresariais ou institucionais.

Problema de usabilidade: qualquer característica, observada em determinada situação, que possa retardar, prejudicar ou inviabilizar a realização de uma tarefa, aborrecendo, constrangendo ou traumatizando o usuário.

Public key: Uma chave criptográfica disponível para distribuição sem necessidade de segredo. É o oposto de uma chave privada ou chave secreta.

Security Officer: Pessoa(s) que garante(m) que os procedimentos de segurança estão de acordo com a política de segurança.

Teoria do Perímetro: Saber segmentar os ativos físicos, tecnológicos e humanos de acordo com a similaridade de sua criticidade e importância é a base para a especificação e aplicação dos controles certos que oferecerão o nível de proteção adequado para cada perfil e necessidade.

Trojan horse: Um programa de computador com função aparentemente ou realmente útil que contem as funções (escondidas) adicionais que exploram secretamente as autorizações legítimas do processo provocando perda da segurança. Tipo de ataque em que um software aparentemente inofensivo, inicia de forma escondida, ataques ao sistema.

Usabilidade: capacidade de um produto ser usado por usuários específicos para atingir objetivos específicos com eficácia, eficiência e satisfação em um contexto específico de uso (ISO, 1998). Alguns autores preferem adotar a expressão “qualidade de uso”.

Violação: Ato ou efeito de violar um sistema alheio; é o comprometimento da segurança através de ataques ou invasões.

Vírus: Uma classe do software malicioso que tem a habilidade de auto replicar e infectar partes do sistema operacional ou dos programas de aplicação, com o intuito de causar a perda ou dano nos dados.

Vulnerabilidade: Probabilidade de uma ameaça transformar-se em realidade.