**CRISTIANE LEIKO TATEKAWA**

# PROPOSTA DE PROCESSO DE GESTÃO DE SEGURANÇA EM SISTEMAS COMPUTACIONAIS

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para conclusão do Curso de Engenharia de Software MBA.

Área de Concentração:
Engenharia de Software

Orientação:
Profa. Dra. Lucia Vilela Leite Filgueiras

São Paulo

2003

FICHA CATALOGRÁFICA

Tatekawa, Cristiane Leiko

Proposta de Processo de Gestão de Segurança em Sistema Computacionais. São Paulo, 2002. 60 p.

Dissertação (MBA) - Escola Politécnica da Universidade de São Paulo.

1. Segurança computacional.

# RESUMO

O presente trabalho propõe um modelo de Processo de Gestão de Segurança em Sistemas Computacionais com base na Gerência de Risco de Projetos do *Project Management Body of Knowledge* (PMBOK) e nas práticas de mercado em gerência da segurança em sistemas de informação. Este modelo pretende prover ao mercado um processo estruturado e com objetivos bem definidos em cada fase, a fim de que as empresas saibam balancear o excesso ou a falta de investimentos em proteção nos pontos de vulnerabilidade, o que se tornou muito comum na corrida das empresas na ânsia de proteger seus recursos. O processo abrange desde a identificação das vulnerabilidades e análise dos riscos, até um plano de manutenção e atualização periódicos. Através deste estudo conclui-se que não é possível implantar uma solução totalmente segura, mas que o processo ajuda a minimizar os riscos do negócio e, conseqüentemente, da organização.

# ABSTRACT

This report propose a Computer Systems Security Management Process Model based on the Project Management Body of Knowledge (PMBOK) Project Risk Management practices and on commom practices in information systems security management. This model intends to provide a structured process with defined goals in each phase in order to show how to balance investiments in vulnerability protections, distortion that became usual nowadays when enterprises race to protect their assets against increasing intrusions. This work starts with vulnerability identification and risk analysis and proceeds up to periodic security maintance planning. This study concludes that is not possible to implement a totally safe solution, but a structured process can help minimize business and organization risks. Even so, this report cannot be considered as the only instrument to implement computer security in an organization. This job requires much more technical knowledge in systems, applications and environment protection utilities beyound enterprise culture change and the managers support.

# SUMÁRIO

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ACL | - Access Control Lists. |
| ALE | - Annual Loss Expectancy. |
| CA | - Certification Authority. |
| CPU | - Central Process Unit. |
| DES | - Data Encryption Standard. |
| DOS | - Denial of Service. |
| FTP | - File Transfer Protocol. |
| HSM | - Hardware Security Module. |
| IDS | - Intrusion Detection System. |
| IMAP4 | - Internet Message Access Protocol Version 4. |
| IP | - Internet Protocol. |
| LAN | - Local Area Network. |
| NAT | - Network Address Translation. |
| NIST | - National Institute of Standards and Technology. |
| PKI | - Public Key Infrastructure. |
| PMBOK | - Project Management Body of Knowledge. |
| PMI | - Project Management Institute. |
| POP3 | - Point Of Presence (padrão 3). |
| RAID | - Reduntant Array of Independent Disks. |
| ROI | - Return on Investment. |
| RSA | - Rivest, Shamir e Adelman. |
| SLE | - Single Loss Expectancy. |
| SMTP | - Simple Mail Transfer Protocol. |

| | |
|---|---|
| TFN | - Tribe Flood Network. |
| VPN | - Virtual Private Networks. |
| WAN | - Wide Area Network. |

# 1. INTRODUÇÃO

O objetivo deste trabalho é estudar as práticas do processo de gestão de segurança sob a visão da gerência de riscos, para propor um roteiro que de aplicação de políticas de segurança em sistemas computacionais.

## 1.1 Motivação

A segurança é um tema e um requisito cada vez mais importante nos sistemas computacionais atuais. A disponibilidade de recursos e a divulgação ampla e rápida de formas de fraude e intrusão, aliadas ao valor da informação presente nos sistemas, têm despertado o interesse de *hackers* e colocado em pauta a segurança das empresas.

A abrangência e a diversidade do assunto exigem que haja processos que contemplem todas as suas áreas porque a omissão de um aspecto pode ser significativa para a segurança total do sistema.

Este trabalho visa identificar estes processos apresentando um modelo de implementação que contemple as etapas necessárias e as práticas comumente aplicadas em segurança de sistemas, utilizando conceitos de gestão de projetos como planejamento, avaliação e análise de riscos para levantamento das vulnerabilidades e controle da manutenção da solução.

É claro que mesmo com a aplicação de todos os mecanismos existentes de segurança não há garantia de que o sistema esteja completamente imune a intrusões, porque há sempre maneiras de quebrar as proteções, desde que exista investimento disposto a isto.

Ou seja, o processo deve ao menos assegurar que as principais medidas de segurança foram levantadas e aplicadas para que ele seja implantado em produção com o maior nível de proteção possível e viável, e com o cuidado de deixar o sistema bastante seguro, e ao mesmo tempo funcional.

## 1.2 Perspectivas de contribuição

Espera-se que com base no produto deste trabalho seja possível identificar os principais passos para a gestão de riscos dos sistemas relacionados à segurança. Ele pode contribuir no desenvolvimento ou aperfeiçoamento de um processo estruturado e cíclico no controle da segurança de sistemas computacionais.

Este estudo tem o objetivo de fornecer uma visão gerencial do processo, portanto, ele não detalha as opções de solução existentes para cada vulnerabilidade do sistema, nem descrever como são operacionalmente aplicadas.

## 1.3 Metodologia

A metodologia adotada para definir o Processo de Gestão de Segurança seguiu o roteiro:

- Pesquisa em bibliografia selecionada sobre o assunto e em organizações internacionais que promovem certificação em segurança;
- Consolidação da pesquisa bibliográfica com a experiência profissional da autora em empresa de consultoria especializada em segurança.

Não foi considerado escopo deste trabalho a aplicação da proposta para efeito de sua validação.

## 1.4 Estrutura do trabalho

O trabalho é dividido em 6 capítulos e apresenta a seguinte estrutura:

- Introdução: Consiste neste capítulo, onde são apresentados o escopo, os objetivos e a metodologia utilizada no trabalho.
- Conceitos relacionados à segurança: É composto por definições sobre os principais termos relacionados ao assunto citados nesta monografia.

- Riscos à informação: Apresenta algumas das vulnerabilidades e as principais ameaças das quais as empresas estão expostas, justificando a importância de um planejamento de proteção contra todos estes riscos.
- Proposta de Processo de Gestão de Segurança: É o capítulo principal em que são apresentadas as fases propostas para um Processo de Gestão de Segurança, prevendo desde o planejamento até a manutenção das políticas definidas.
- Conclusão: Faz o desfecho da monografia apresentando o resultado conclusivo das pesquisas realizadas, do processo definido e da experiência obtida.
- Referências: Cita as referências bibliográficas utilizadas no trabalho.

# 2. CONCEITOS RELACIONADOS À SEGURANÇA

O objetivo deste capítulo é descrever os conceitos dos termos relacionados à segurança que são utilizados neste trabalho.

## 2.1 Segurança

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. Suas características básicas são a garantia de integridade, a confidencialidade e a disponibilidade.

D'Andrea (2000) conceitua estas premissas como:

- Integridade: Princípio que trata sobre a proteção da informação ou dos bens de informação contra a criação ou a modificação não autorizada. A perda de integridade pode ser causada por erros humanos, ações intencionais ou contingências e pode resultar em falta de confiabilidade nos dados e retrabalho na sua recuperação.
- Confidencialidade: Princípio que trata sobre a disponibilidade de informações apenas às pessoas autorizadas. A confidencialidade pode ser conseguida com várias técnicas, como controle de acesso ou criptografia da informação.
- Disponibilidade: Princípio que trata sobre prevenir que a informação ou o recurso da informação esteja indisponível quando requerida. Aplica-se não só à informação, mas também aos canais eletrônicos, equipamentos da rede e pessoal.

## 2.2 Recurso

Em artigo publicado pela Microsoft Corporation (2002), recurso é definido como tudo no ambiente que precisa ser protegido. Nisto se incluem dados, aplicações, servidores, roteadores e até pessoas. O propósito da segurança é evitar que os

recursos sejam atacados. Uma parte importante da gerência do risco é justamente determinar o valor dos recursos para ser possível definir o nível de segurança apropriado para ele.

## 2.3 Ameaça

Para a Microsoft Corporation (2002), ameaça é uma pessoa, lugar ou qualquer coisa que possa acessar os recursos e causar prejuízo. A ameaça pode ser de diferentes tipos:

- Natural ou física: guerra, fogo, água, terremoto, queda de energia. São ameaças que causam principalmente danos físicos, por isso precisam ser consideradas na preparação da infra-estrutura da empresa.
- Não-intencional: funcionários desinformados.
- Intencional: Terroristas, espiões, governo, código malicioso, *hackers* e principalmente funcionários.

## 2.4 Vulnerabilidade

Segundo o conceito da Microsoft Corporation (2002), vulnerabilidade é um ponto onde o recurso é suscetível a ataque. A vulnerabilidade pode ser:

- Física: Portas destrancadas ou falta de controle de acesso.
- Em hardware e software: são as vulnerabilidades mais comuns - configurações inadequadas, *bugs* de softwares, antivírus desatualizados, etc.
- Em mídia: interferência elétrica.
- Na comunicação: transmissão de dados sem criptografia.
- Humana: falhas em procedimentos sem segurança, divulgação da senha.

As vulnerabilidades, junto às ameaças, vão constituir o foco das análises do processo para a identificação dos riscos potenciais.

## 2.5 Ataque

Harris (2002) definiu ataque como uma tentativa de desvio dos controles de segurança em um sistema com a missão de usar o sistema ou comprometê-lo. Um ataque passivo lê os dados sem modificá-los. Um ataque ativo os modifica. Um ataque geralmente ocorre através da exploração de uma vulnerabilidade.

Conforme a Microsoft Corporation (2002), o ataque pode gerar conseqüências sérias, como perda de confiabilidade, de integridade ou disponibilidade da informação, que são as premissas básicas da segurança.

O ataque não é a única forma de ameaça à segurança computacional pois existem também ações não intencionais que podem causar danos a informações relevantes.

## 2.6 Criptografia

Turban et al. (2000) definiram criptografia como "a ciência que se dedica a transcrever dados em cifras ou códigos". Segundo eles, toda criptografia tem quatro partes básicas: texto plano (a mensagem original em forma legível a todo ser humano), texto em código (o texto simples depois que foi codificado em uma forma não legível), algoritmo (a fórmula matemática usada para criptografar o texto simples em texto codificado e vice versa) e a chave (string secreta usada para criptografar e reverter a criptografia de mensagens).

Como os tipos de criptografia mais confiáveis são aqueles conhecidos pelo mercado, o algoritmo não é segredo para ninguém. O que assegura a informação criptografada é a chave utilizada.

Turban et al. (2000) afirmaram que é possível adivinhar uma chave simplesmente tendo um computador tentando todas as possibilidades até a criptografia ser revertida, por isso que o comprimento da chave é o fator principal para assegurar uma mensagem.

Há dois tipos básicos de criptografia: simétrica e assimétrica.

A criptografia simétrica é mais simples, e consiste nas duas partes pactuarem uma chave que será utilizada na criptografia e na sua reversão. Segundo Turban et al (2000), alguns exemplos de criptografia são o DES, RC2, RC4, e RC5 cujas chaves alcançam um comprimento de 56 a 2048 bits.

O outro tipo de criptografia é a criptografia assimétrica, em que são utilizadas duas chaves: uma pública e outra privada. A chave pública é utilizada para criptografar a mensagem, é de conhecimento público e só com a chave privada é possível decifrá-la. Ou seja, só o proprietário da chave privada consegue decodificar o objeto criptografado. Um dos poucos algoritmos existentes para esse tipo de criptografia é o RSA, chamado pelo nome de seus inventores, Ronald Rivest, Adi Shamir e Leonard Adelman

Segundo Turban et al (2000), este algoritmo emprega chaves que alcançam de 513 a 1024 bits, e é o algoritmo mais amplamente utilizado ara criptografar Web e mensagens de e-mail.

Como a criptografia assimétrica possui problema de velocidade de processamento, comumente é usada a combinação entre as duas formas de criptografia. É criada uma chave simétrica para criptografar o texto original e a chave simétrica é enviada ao destinatário criptografada com o algoritmo assimétrico. Assim, o processamento pesado concentra-se num objeto de tamanho reduzido, tornando o processo bem mais rápido. Só o proprietário da chave privada consegue descobrir a chave simétrica e assim, decodificar a mensagem inteira.

A criptografia assimétrica também permite o uso de assinaturas digitais, que consiste no cálculo de um *hash* da mensagem com o uso da chave privada. O hash, que funciona como um dígito verificador da mensagem, pode ser validado no seu destinatário com o uso da chave pública, certificando assim a autenticidade do emissor.

## 2.7 Risco

Segundo Harris (2002), risco, em segurança computacional, é a probabilidade ou a perda potencial de uma ameaça explorar e tirar vantagem de uma vulnerabilidade.

E, mesmo que todas as medidas cabíveis sejam adotadas, Benson et al. (2000); Harris (2002) consideraram que nenhum sistema ou ambiente consegue estar 100% seguro e operacional ao mesmo tempo. Isto significa que a empresa lida com um risco mesmo se adotadas todas as medidas possíveis de proteção. Este risco é chamado de Risco Residual.

Porém, se a probabilidade de ataque por uma ameaça é pequena e o custo de implementar uma medida de proteção contra ela for muito alto, a empresa pode optar por não investir nesta medida. Este risco é adicionado ao chamado Risco Total.

Ou seja, o risco total é a probabilidade de cada ameaça vezes o valor do recurso. O risco residual é este valor multiplicado pelas lacunas existente entre os controles.

É importante saber distinguir os 2 tipos de risco e identificar a qual deles a empresa está vulnerável. Mesmo que a empresa esteja protegida, ela precisa saber da existência dos riscos não eliminados e preparar políticas de contingência para estarem preparados para se recuperar de qualquer um deles.

## 2.8 Gestão de Riscos

A Microsoft Corporation (2002) considerou que a Gestão de Riscos voltada para a segurança da informação visa analisar as ameaças para a informação e infra-estrutura do sistema, e levantar as suas vulnerabilidades através de técnicas e ferramentas especializadas. A probabilidade e o impacto de cada risco são avaliados para que sejam priorizadas as necessidades de proteção contra eles. Com base nesta avaliação pode-se criar um plano de redução de riscos ou medidas a serem tomadas no caso de ocorrência de algum deles.

Neste estudo concluir-se que a Gestão de Riscos é ainda mais abrangente porque exige o teste do plano de segurança proposto, a implementação efetiva na instituição,

o acompanhamento ou o monitoramento de indicadores que podem alarmar sobre riscos iminentes e coletar informações para melhoria do processo. Devido à complexidade e importância deste trabalho, as empresas começam a criar equipes específicas destinadas a esse trabalho.

A gestão do risco também compreende a percepção do limite que pode ser colocado nas atividades operacionais dos usuários, balanceando o nível de risco que a empresa aceita correr com a flexibilidade das aplicações.

Como regra geral, quanto maior o nível de segurança, maior o custo para sua implementação e menor a flexibilidade quanto a funcionalidades. Após a análise dos riscos potenciais, pode ser necessário elevar o nível de risco com o intuito de diminuir os custos e expandir as funcionalidades. A restrição muito rigorosa das atividades dos usuários pode comprometer a flexibilidade necessária em algumas operações e inibir a criatividade de usuários na resolução de problemas e otimização de processos. A segurança não pode ser a obsessão da empresa com risco de comprometimento do negócio.

Por exemplo, no mercado financeiro, é necessário que os operadores de bancos tenham liberdade de criar operações compostas visando o lucro em um determinado cenário mundial, e que essa dinâmica não pode ser prevista a tempo de ser possível mudar perfis e acessos restritos às suas operações básicas diárias. Outro exemplo é o uso da criatividade do usuário na solução de pendências do sistema com as funcionalidades disponíveis, enquanto o controle específico não é desenvolvido. Isso só é possível através da flexibilidade que as aplicações permitem, aliadas ao conhecimento e à maior liberdade de adaptação do usuário a um novo contexto. Por isso a linha entre segurança e liberdade deve ser bem definida a fim de que o dia-a-dia do usuário não se torne nem tão rígido, nem tão liberal, tendo como objetivo manter um ambiente o mais seguro possível, e operacional ao mesmo tempo.

# 3. RISCOS À INFORMAÇÃO

Este capítulo é baseado no trabalho de Benson et al. (2000), adotando-se a estrutura proposta pelos autores.

Ele descreve as principais vulnerabilidades e ameaças sofridas pelos sistemas computacionais, que são os principais fatores que compõem os riscos à informação.

## 3.1 Principais vulnerabilidades

Podem existir diversos tipos de vulnerabilidades de acordo com a arquitetura de hardware e de software e a política e cultura da organização. Para encontrar as vulnerabilidades que existem em um sistema particular, é necessário avaliar a organização, conversar com vários distribuidores de software e de hardware e fazer a pesquisa e os testes nos produtos. Já existem também no mercado nacional algumas ferramentas que auxiliam na detecção de algumas vulnerabilidades, principalmente relacionadas à configuração de software e de *firewall*.

Algumas das vulnerabilidades mais comuns são:

- Senhas, que pela dificuldade de memorização, levam os usuários a selecionar termos comuns que sejam fáceis de recordar como aniversários e nomes de quem ama. Esta é uma vulnerabilidade porque permitem a outros que descubram a senha correta.
- Projeto de protocolos de comunicação, que podem possuir alguns pontos fracos. Para garantir a compatibilidade entre eles, são trocados usuários e senhas em claro, que podem ser facilmente interceptados por usuários internos ou externos ao ambiente. Alguns exemplos de protocolos nesta condição são o Telnet e o FTP.
- Modems, porque representam uma forma de contornar o *firewall* que protege uma rede dos intrusos externos. Um *hacker,* usando da uma ferramenta para o

discador, identifica o telefone do modem, o número e de uma ferramenta de quebra de senha, consegue quebrar uma senha fraca e ganhar o acesso ao sistema. Uma vez que um *hacker* consegue se conectar a esse computador, ele pode facilmente se conectar a qualquer outro computador na rede.

Algumas vulnerabilidades são parte integrante do sistema operacional ou aplicação, geradas ou por falha de projeto ou falta de testes maciços voltados à validação da segurança ou ainda porque não foram encontrados mesmo, já que não existe um ambiente 100% seguro. Periodicamente os fabricantes divulgam pacotes de correção que visam à correção de algumas destas vulnerabilidades, e que precisam ser atualizados no ambiente para diminuir o seu nível de risco.

Anderson (2002), demonstrou a dificuldade de se proteger contra todos os ataques possíveis porque atacar é muito mais simples do que se proteger. Se um sistema grande e complexo, com inúmeros *bugs* ainda desconhecidos, for avaliado por pessoas com intuito de proteger o sistema e, ao mesmo tempo, por pessoas com o objetivo de atacá-lo, mesmo que as pessoas encarregadas pela proteção troquem informações entre si através de fóruns e grupos com esse mesmo fim, elas não conseguem saber qual das brechas vai ser descoberta e atacada. Qualquer um dos milhares de pontos de vulnerabilidade pode ser atacado, enquanto que para o sistema estar seguro, seria necessário proteger todos eles. A variável do tempo conta bastante neste aspecto, porque mesmo que todas as vulnerabilidades fossem conhecidas, o tempo de protegê-las é consideravelmente menor que o tempo de uma delas ser antes atacada, se alguém estiver disposto a isto.

Além disso, com o passar do tempo, observa-se que o número de vulnerabilidades tem aumentado, devido, principalmente, ao crescimento do nível de exposição da informação e dos recursos associados a ela. Ou seja, esse aumento é resultado do surgimento e crescimento das redes de computador e, recentemente, pela propagação do uso da internet.

### 3.1.1 Uma abordagem econômica das vulnerabilidades

Segundo Anderson (2002), a segurança da informação é muito difícil de ser eliminada e não depende apenas de tecnologias aplicadas ao ambiente. Ela envolve algumas questões econômicas que não são consideradas normalmente na análise de risco de uma solução.

Em alguns casos, a segurança de um membro da rede depende de outros membros, como no caso dos ataques DOS (*Denial of Service*). Mas as pessoas geralmente se empenham na sua proteção mas não fazem o mínimo esforço para evitar que seus recursos sejam utilizados para o ataque de recursos de outros, justamente por não serem elas as prejudicadas.

Outra causa da existência de vulnerabilidades é a arquitetura do sistema, que para ser mais simples e amigável, leva o fabricante a não implementar alguns requisitos de segurança contra alguns tipos básicos de ataque. Além contribuir para que o sistema fique mais barato por ficar menos complexo, permite que os desenvolvedores se adaptem melhor e mais rapidamente a um ambiente mais simples, conquistando mais adeptos. Chega a ser uma estratégia financeira e de marketing ao mesmo tempo.

Até hoje não há regulamentação dos governos que indiquem o nível de segurança mínimo aceitável nos sistemas, e por questões econômicas, ele normalmente não é avaliado com o devido cuidado, deixando seus usuários sob grande risco.

A economia gera muitos outros efeitos na engenharia da segurança, como o uso de soluções proprietárias pelas empresas desenvolvedoras de software, que ao invés de utilizarem arquiteturas padrões, procuram por outros caminhos, para aumentar a dependência de seu cliente e obrigando outros sistemas associados a se adequarem. O objetivo é a precificação diferencial, que considera não o custo do produto, mas seu valor para o cliente.

Todos estes fatos indicam que a proteção de todas as vulnerabilidades de segurança da informação é bastante complexa, ou seja, elas não têm origem estritamente técnica, elas também são consequência de aspectos políticos e econômicos.

## 3.2 Principais Ameaças à Segurança

As ameaças podem se originar de duas fontes principais, humanas e naturais, sendo que as maiores ameaças contra os sistemas computacionais e suas informações vêm de humanos, embora as ações nem sempre sejam propositais.

### 3.2.1 Desastres Naturais

Terremotos, furacões, enchentes, raios e fogo podem causar prejuízos sérios para os sistemas de computadores. Informações podem ser perdidas, pode haver perda de produtividade, danificação de hardware e interrupções em serviços essenciais.

Poucas precauções podem ser tomadas contra desastres naturais. A melhor ação é ter tomar alguns cuidados no projeto de infra-estrutura da empresa, pelo menos na sala dos servidores, onde há a maior concentração de informação, e desenvolver planos de contingência e recuperação que podem ajudar a organização a voltar a operar.

As instituições mais preparadas contra este tipo de ameaça são as grandes instituições financeiras e os *Data Centers* - centros de armazenamento e processamento de dados, que hospedam sites de produção ou de contingência de várias empresas, compartilhando os custos de infra-estrutura. Estas empresas geralmente possuem geradores com capacidade de turbinas de navios, sensores de fumaça, estrutura contra enchentes e monitoração eletrônica de toda a infra-estrutura.

Outros tipos de ameaças que podem ser classificadas nessa categoria são as guerras e ataques terroristas, que embora sejam resultados de ações humanas, são vistos como desastres porque são difíceis de serem evitados por medidas preventivas.

### 3.2.2 Ameaças Humanas

As ameaças humanas podem ser quebradas em 2 categorias: maliciosas ou não maliciosas. As não maliciosas geralmente vêm de usuários e funcionários sem treinamento ou que não conhecem as várias ameaças à segurança do sistema. Ataques maliciosos geralmente vêm de pessoas que não são da organização ou de funcionários insatisfeitos e que podem causar grande impacto nas atividades da empresa.

#### 3.2.2.1 Ameaças Humanas não maliciosas

A ameaça pode vir de usuários autorizados que não estão conscientes de suas ações, cujos erros e omissões podem gerar perda, danificação ou alteração de dados valiosos.

Usuários, digitadores, operadores de sistemas e programadores freqüentemente cometem erros não-intencionados que contribuem para os problemas de segurança, direta ou indiretamente. Às vezes o erro é a ameaça, como uma entrada de dados errada ou um erro de programa que danifica o sistema. Em outros casos, erros criam vulnerabilidades. Erros podem ocorrer em todas as fases do ciclo de vida do sistema

desde o projeto até a instalação, e variam de perturbadores a catastróficos. A melhoria na qualidade do software tem reduzido esta ameaça, mas não eliminado. Muitos programas, especialmente aqueles desenvolvidos para usuários de computadores pessoais, não possuem medidas de controle de qualidade. Entretanto, mesmo os programas mais sofisticados não podem detectar todos os tipos de erros.

#### 3.2.2.2 Ameaças Humanas Maliciosas

As ameaças maliciosas podem ter origem interna ou externa à organização.

Os funcionários são as pessoas que têm maior familiaridade com os computadores e aplicações da organização, e sabem inclusive de quais ações podem causar os maiores danos e quais são as vulnerabilidades dos sistemas e dos procedimentos. Estas pessoas podem trazer vírus, cavalos de Tróia ou navegar através da rede sem autorização. Este tipo de ataque pode ser extremamente difícil de se deter ou de se evitar.

O ataque interno pode afetar vários componentes de um esquema de segurança: acessando a rede, um funcionário pode ler informações confidenciais; ou ameaçar a integridade e confidencialidade das informações do sistema trazendo um vírus, ou afetar a disponibilidade do sistema sobrecarregando o seu processamento.

Estes ataques são possíveis por várias razões, que podem ser desde sabotagens através de falhas de configurações de sistemas que não refletem a política de segurança da organização como gravação de trilhas de auditoria até a inserção de dados incorretos nos sistemas.

Os ataques externos são feitos por *'hackers'* ou *'crackers'*. A definição de *hacker* mudou ao longo dos anos. Um *hacker* antes era um indivíduo especialista em determinado sistema e que conhecia com detalhes todas as suas nuances. Agora, o termo *'hacker'* refere-se à pessoa que acessa ou interfere em sistemas em que não tem autorização. O seu termo correto seria *'cracker'*.

O objetivo destes dois tipos de ataque geralmente não é a destruição física do computador, mas a penetração e remoção ou cópia de informações importantes, por satisfação pessoal ou em troca de uma recompensa. As ações mais comuns destes invasores são:

- Exclusão e alteração de informações para provar um ponto ou se vingar de alguma coisa que tenha acontecido a eles. Ataques internos normalmente ocorrem por rancor à organização por causa de algum descontentamento.
- Roubo de informação e fraude, tanto através dos sistemas como através do furto do hardware. Sistemas financeiros não são os únicos objetos de fraude, as vítimas podem ser sistemas que controlam o acesso a qualquer recurso, como sistemas de atendimento, inventário, notas escolares ou de telefonia. Funcionários antigos da organização também podem oferecer ameaças nestes casos, principalmente se seu acesso não for cancelado prontamente. O furto do hardware também oferece preocupação pelos computadores serem relativamente pequenos e valiosos, portanto fáceis de roubar e vender. Além disso, se o computador é roubado, a informação que ele contém estará à disposição de quem agora o possui. O ladrão pode apagá-la ou pode lê-la. O ladrão pode vender as informações confidenciais, usá-las para chantagem ou para comprometer outros sistemas.

  Dados também podem ser roubados de um computador sem o conhecimento do seu dono, como por um *Zip drive*, que pode ser conectado a uma porta paralela do computador e permitir a cópia de vários megabytes de dados. Neste caso, a melhor medida a ser adotada é a criptografia.

- Interrupção do funcionamento do sistema (*Denial Of Service-DOS* ) através do envio de grande quantidade de requisições ao sistema. A causa de uma atitude desta pode ser o descontentamento de um funcionário ou pode ser um concorrente que esteja querendo dificultar o trabalho de uma empresa.

#### 3.2.2.3 Métodos, ferramentas e técnicas de ataque.

Ataque = motivo + método + vulnerabilidade

O método nesta fórmula explora a vulnerabilidade da organização a fim lançar um ataque. Os intrusos, usando técnicas bem conhecidas, podem penetrar em várias redes através de suas vulnerabilidades.

Os métodos comuns de se conseguir acesso a um sistema são a quebra de senha, exploração de fragilidades de segurança conhecidas, *spoofing* de rede e abordagem de pessoal.

Uma forma de se proteger é o uso da detecção de intrusão, que é o processo de detectar uso não-autorizado ou ataque a um computador ou rede. A detecção de intrusão provê duas funções importantes na proteção das informações sistêmicas:

o mecanismo de *feedback,* que informa o status dos componentes de segurança e o gatilho que ativa respostas planejadas para um incidente. Mas a ausência de intrusões detectadas é uma indicação de que não há intrusões conhecidas e não que o sistema está completamente seguro.

Embora os ataques possam continuar, o sistema de detecção de intrusos (*Intrusion Detection System* – IDS) pode detectar estas tentativas, bloqueá-las e alertar o pessoal da segurança para que se tome a ação apropriada.

Estão listados abaixo alguns dos tipos de ataque mais conhecidos no mercado:

- **DOS (*Denial of Service*)**: Ataques DOS são projetados para evitar o uso legítimo do serviço. Os ataques dos podem causar a saturação de recursos da rede, impedindo os usuários de utilizá-los; podem quebrar a conexão entre dois computadores, impedindo a comunicação entre serviços; ou bloquear um serviço a um sistema específico. Os ataques DOS sobrecarregam uma rede remota com uma enorme quantidade de pacotes de protocolo. Então os roteadores e

servidores se sobrecarregam por manipular cada pacote. Em minutos, a atividade de rede cresce exponencialmente e a rede pára de responder para o tráfego normal e as requisições de serviço das estações. O ataque também pode ser feito através do bombeamento de e-mails a um sistema até que ele falhe.

- **Vírus:** um vírus de computador é um pedaço de código auto-replicável para outro pedaço de código, com o principal objetivo de danificar informações ou sistemas do computador atingido.

  As seguintes características são comuns nos vírus:

  - Habilidade de se replicar;
  - Necessidade de haver um programa hospedeiro;
  - Ativação por uma ação externa;
  - Limitação da habilidade de replicação aos sistemas virtuais.

  Benson et al. (2000) classificaram os vírus encontrados como:

  - Variante: vírus que foi gerado pela modificação de um vírus conhecido.
  - De sobreposição: destrói o código ou dados do programa substituindo-os pelo código do vírus.
  - Residente: instala-se como parte do sistema operacional e se mantém ativo enquanto o sistema estiver no ar. Uma vez estando na memória, ele infecta todas as máquinas que são acessadas.
  - Oculto é um vírus residente que tem o objetivo de fugir da detecção escondendo sua presença em arquivos infectados. Para realizar isso, o vírus intercepta as chamadas de sistema que examina o conteúdo ou os atributos de arquivos infectados.
  - Criptografado: tem duas partes, um mecanismo de criptografia e o corpo do vírus criptografado. Quando o vírus é executado, o mecanismo de reversão da criptografia será executado e irá decifrar o corpo do vírus.

- Polimórfico: cria cópias durante a replicação que são funcionalmente equivalentes, mas têm diferentes seqüências de bytes geradas randomicamente ou em ordem alterada.
- De pesquisa: aquele que foi desenvolvido, mas nunca chegou ao público. Nestes são incluídos as amostras que são enviadas para pesquisadores pelos codificadores de vírus.

- **Cavalos de Tróia:** O Cavalo de Tróia é um código escondido em um programa que possui efeitos colaterais escondidos. Quando o programa é rodado, parece funcionar como o usuário espera, mas na realidade ele está destruindo, danificando ou alterando informações por trás. Ele é um programa independente e não precisa de um programa hospedeiro para se alojar. Cavalos de Tróia geralmente são espalhados por e-mail e troca de arquivos e informações entre computadores. Os danos que eles causam são semelhantes aos de um vírus.

- **Violação de *E-mail*:** Os protocolos de transferência mais comuns (SMTP, POP3, IMAP4) geralmente não incluem características de autenticação confiável como parte do protocolo padrão, permitindo que mensagens de *e-mail* sejam facilmente forjadas. Estes protocolos também não exigem o uso de criptografia que poderia assegurar a privacidade ou confidencialidade das mensagens de e-mail. Embora existam extensões para estes protocolos básicos, a decisão de utilizá-los precisa ser estabelecida como parte da política de administração do servidor de *mail*.

- **Engenharia Social**: Esta é uma forma comum de invasão, ela pode ser usada tanto por pessoal externo quanto interno à organização. Engenharia social é um termo entre *hackers* de enganar pessoas para que revelem suas senhas ou alguma informação que afete a segurança. Um exemplo comum de engenharia social é quando um hacker envia um e-mail para um funcionário identificando-se como o administrador do sistema que precisa de sua senha para fazer algum trabalho administrativo. "Surfar no ombro" é também comum entre *hackers* e usuários que desejam descobrir a senha de alguém. Neste caso, eles rodeiam a mesa do usuário, conversando e esperando o usuário digitar a senha. Outra forma de engenharia social é descobrir informações sobre a vida pessoal dos usuários,

verificar palavras que eles possam ler de suas mesas, e utilizá-las na tentativa de adivinhar suas senhas

### 3.2.3 Medidas de proteção

Para combater as vulnerabilidades do ambiente e as ameaças internas e externas, o método mais comum utilizado é a adoção de medidas de proteção.

Harris (2002) conceituou medida de proteção como um controle, método, técnica ou procedimento que é implementado para prevenir uma ameaça de explorar uma vulnerabilidade. Ela é colocada em prática para mitigar o risco.

Conforme Benson et al. (2000) as medidas de proteção em sistemas computacionais podem ser classificadas como de:

- Prevenção: Medidas que previnem a informação de ser danificada, alterada ou roubada. Medidas preventivas podem variar de trancar a sala do servidor até configurar políticas de segurança de alto nível.
- Detecção: Medidas que permitem detectar quando e como a informação está sendo danificada, alterada ou roubada, e quem causou o dano. Várias ferramentas estão disponíveis para ajudar na detecção de intrusos, danos, alterações e vírus.
- Reação: Medidas que permitem a recuperação da informação, mesmo se a informação for perdida ou danificada.

Estão aqui citadas algumas das medidas utilizadas pelo mercado com esse fim, e que podem servir como alternativas na composição da Política de segurança.

#### 3.2.3.1 Controle de Acesso

Segundo D'Andrea (2000), o controle de acesso contribui diretamente para assegurar a confidencialidade, integridade, disponibilidade e uso legítimo das informações e recursos.

Os meios que permitem o controle de acesso são:

- A autorização, que é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acesso, definindo quais atividades poderão ser realizadas por quais usuários ou grupos de usuários. As aplicações comerciais comumente dispõem de controles que restringem o acesso do usuários a módulos, menus, botões e filiais. Para o caso de sistemas com necessidade maior de segurança, a restrição pode chegar a restringir o acesso por tipo de informação, como no SPB, que podem delimitar até quais tipos de mensagens podem ser acessadas para cada grupo.
- A autenticação, que é o meio pra obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser. Ela assegura o controle de acesso, determina quem está autorizado a ter acesso à informação, permite trilhas de auditoria e assegura a legitimidade do acesso. A autenticação pode ser feita por identificação positiva, na qual o requerente demonstra conhecimento de alguma informação do processo de autenticação, como a senha; pode ser feita por identificação proprietária, a partir da posse de algo necessário no processo de autenticação, como um cartão; e pode ser feita por identificação biométrica, a partir de uma característica própria, como impressão digital ou reconhecimento de voz. A senha sempre foi a forma mais comum de se garantir a autenticação, mas ultimamente tem se mostrado falho tanto em sistemas simples de aplicação comercial quanto para sistemas bancários. A tecnologia que começa a se espalhar no Brasil é o uso de autenticação através da biometria, que agora além de estar mais confiável e mais disponível no mercado interno, está mais acessível ao orçamento das empresas.

#### 3.2.3.2 Criptografia/Assinatura digital

Para evitar que as informações sejam coletadas ou até mesmo modificadas no seu trajeto ou no seu armazenamento, a técnica utilizada como medida de segurança é a criptografia.

Benson et al. (2000) apresentaram que a combinação da criptografia com a assinatura digital oferecem as características básicas para segurança da informação:

- *Autenticação:* Valida a informação com relação à sua origem, prevenindo que um impostor se passe pelo seu emissor.
- *Integridade:* Indica se a informação não foi modificada em seu trajeto ou armazenamento. Mas ela consegue apenas detectar a modificação, não preveni-la.
- *Não-repúdio:* Prova a identificação de quem gerou ou enviou a informação e confirma que mensagem foi entregue.
- *Confidencialidade:* Previne a leitura da informação por pessoas não-autorizadas.

Para garantir estas a segurança de transmissão, no SPB - Sistema de Pagamentos Brasileiro é utilizada a combinação entre a criptografia simétrica (3DES) e a assimétrica (RSA) além da assinatura digital. Todas as mensagens trocadas entre instituições financeiras, Clearings e Banco Central são assinadas e criptografadas, e as que operam com grande volume utilizam hardwares específicos e especializados em criptografia, os chamados HSMs, que tem como características a segurança da chave privada e um processador voltado a operações de criptografia, tornando o processo ainda mais rápido e seguro. A grande preocupação em todas estas instituições, é na guarda da chave privada, porque a sua posse pode permitir a decodificação e a assinatura de mensagens, podendo provocar movimentações financeiras válidas e grandes prejuízos à instituição.

Em operações bancárias pela internet é utilizada a mesma técnica, que é considerada uma das mais seguras sendo utilizadas pelo mercado.

#### 3.2.3.3 Infra-estrutura de Chaves Públicas (PKI - Public Key Infrastructures)

Benson et al. (2000) definiram a infra-estrutura de chave pública como a forma de prover os meios de relacionar as chaves públicas a seus donos e ajudar na distribuição de chaves públicas confiáveis em redes grandes e heterogêneas. Esse relacionamento é feito através dos certificados digitais, que contêm informações como o nome de seu dono e a chave pública emitido por uma Certificadora (CA – *Certification Authority*) confiável.

O certificado digital representa a chave pública da organização e é assinada eletronicamente por uma certificadora. A certificadora pode ser externa, como é o

caso da Verisign, Certisign, Unicert, Serasa, etc, que são reconhecidas pelas máquinas através do registro de seus certificados no sistema operacional. Há casos em que as certificadoras são montadas na própria organização, e então ela fica responsável pela segurança e confiabilidade dos certificados que são emitidos.

Uma PKI é freqüentemente composta de várias certificadoras organizadas hierarquicamente sob uma "CA raiz". As certificadoras podem ser configuradas independentemente numa rede, formando assim a arquitetura da PKI.

A principal vantagem da PKI, para Hayday (2001), é que as chaves privadas normalmente são seqüências longas de 1024 bits e não podem ser desvendadas da mesma forma que uma senha. Portanto, os certificados associados a elas proporcionam uma autenticação de alta segurança.

#### 3.2.3.4 Smart Cards

Benson et al. (2000) descreveram *smart cards* como, basicamente, tipos de cartões de crédito com uma pequena memória e às vezes, um processador. Eles são utilizados quando estas características são necessárias no cartão, como o *logon*, quando é utilizada a chave privada junto com outra informação pessoal do usuário, como a senha. Normalmente o cartão é inserido em um dispositivo de leitura conectado ao computador e o software usa a informação armazenada no *smart card* para efetuar a autenticação. Se, além disso, for utilizado uma senha ou um identificador biométrico, o nível de segurança aumenta. Outro uso do *smart card* é para guarda da chave utilizada em criptografia de arquivos.

#### 3.2.3.5 Firewall

D'Andrea (2000) citou o *Firewall* como um dispositivo de defesa composto por um sistema que reforça o cumprimento de políticas de acesso entre duas ou mais redes, permitindo somente tráfego de informação autorizada. Basicamente, o controle e restrição ao fluxo de dados são realizados por meio de filtros dos pacotes, serviços e rotas, entre outras medidas. Eles são ainda uma ferramenta importante nos processos de monitoramento e auditoria de uma rede, podendo ser também parte da solução de detecção de intrusos, auxiliando nas tarefas de alarme e rastreamento de ataques

internos e externos, conforme a rede estiver desenhada. Os modelos e as características de cada firewall variam de um para outro, mas todos apresentam duas características fundamentais: controle de acesso e log do tráfego de dados. Eles também podem fazer a tradução dos IPs da rede interna para a rede externa, protegendo a rede interna contra ataques diretos e monitorar as tentativas de intrusão emitindo avisos aos administradores da rede.

#### 3.2.3.6 Monitoração

A monitoração preventiva e reativa do ambiente ajuda na identificação de ataques e irregularidades encontradas, além de ser um processo automático e cíclico, que poderia ser impossível ser feito manualmente pelos operadores ou administradores da rede e dos servidores.

D'Andrea (2000) apresentou alguns recursos e técnicas como:

- **Sistema de detecção de intrusos:** verificam as informações que trafegam na rede e identificam potenciais intrusos que estejam tentando acessar ou tornar indisponível o sistema. Existem também os sistemas ***Honeypot***, implementados com o propósito de atrair ataques, registrando toda atividade de forma confiável e segura, e instantaneamente disparando alarmes para os responsáveis pela segurança. O objetivo é coletar maiores informações sobre o intruso enquanto ele tenta invadir um sistema desenhado para ludibriá-lo. A desvantagem é que estes sistemas aumentam a complexidade do ambiente e requerem gerência e manutenção como todo sistema.
- Os **monitores de log** procuram nos registros gerados pelos serviços de rede por padrões que possam indicar um ataque de intruso como uma grande quantidade de tentativas de conexão recusada, aumento no tráfego de rede ou aumento na utilização da CPU e na unidade de disco. Um tipo de monitor são os ***sniffers,*** que são sistemas capazes de capturar informações destinadas a um outro dispositivo de um mesmo segmento de rede. Eles podem ser utilizados para um monitoramento pró-ativo e reativo, analisando diversos aspectos da rede, tais como a sua disponibilidade e integridade, ou podem ser utilizados de forma maliciosa, com o intuito de monitorar e gravar todos os pacotes de informação

que transitam naquele segmento. Já existem hoje no mercado recursos chamados *anti-sniffers*, que realizam varreduras periódicas objetivando detectar *sniffers* analisando o tráfego de informações da rede.

- **Antivírus:** Não existe um meio totalmente seguro de prevenção contra os vírus. É indicada a implementação de boas medidas de segurança contra as diversas formas existentes, como barreiras e monitores antivírus atualizados residentes em memória, a prevenção de dados através da manutenção de discos de inicialização e de recuperação normalmente criados por antivírus e de *backups* dos dados importantes presentes no computador. Já é prática em empresas com alguma política de segurança que proíbe a entrada de dados via disquete ou CD-ROM diretamente da máquina dos usuários. Os drives são retirados ou desativados e os dados só podem entrar ou sair da empresa após validação e cópia por uma área responsável.
- **Logs e trilhas de auditoria**: As trilhas de auditoria são registros históricos das transações e estados de dados de um sistema, de forma que a permitir que, a partir de qualquer ponto da transação, seja possível percorrê-la até sua origem, ou verificar subseqüentes efeitos para a determinação de causas e impactos de um erro no sistema.

Benson et al. (2000) indicaram que as trilhas de auditoria são um recurso a ser usado com cuidado, pois podem causar muita perda de performance. Os sistemas operacionais geralmente permitem a auditoria de vários eventos e mas que precisam ser bem escolhidos para que a performance não seja muito degradada. Geralmente são oferecidas as trilhas de auditoria de informações de *logon* e *logoff*, informações de *shutdown* e reinicialização do sistema, acesso a arquivos e pastas, alterações de senha, acesso a objetos, mudança de política, etc.

#### 3.2.3.7 Acordos de Nível de Serviço

Os acordos de nível de serviço são muito importantes para garantia de prestação de serviço com qualidade satisfatória para o cliente, e podem ser feitos para qualquer tipo de serviço prestado pelo fornecedor. A qualidade e o tempo de resposta do fornecedor podem fazer bastante diferença, principalmente nos momentos de

emergência, e por isso muitas empresas exigem que este acordo seja firmado já no contrato.

Segundo D'Andrea (2000), os acordos de nível de Serviço são "acordos formais feitos entre fornecedores e clientes (internos e externos), pelos quais definem, conjuntamente, condições, responsabilidades e níveis de desempenho para os serviços a serem executados".

Os acordos de nível de serviço geralmente contêm as políticas e práticas adotadas pelo fornecedor; os papéis existentes; a relação de serviços prestados e seus responsáveis; o critério de classificação da severidade dos problemas relativos a cada serviço e cada usuário que vão definir as prioridades de atendimento; as penalidades e benefícios do acordo e a forma de medição do desempenho dos serviços prestados.

O acordo de nível de serviço é uma forma da empresa selecionar e conhecer a abrangência do serviço oferecido pelo fornecedor e indicar nos planos de contingência quando eles podem ser acionados.

# 4. A PROPOSTA DE PROCESSO DE GESTÃO DE SEGURANÇA

Segundo D'Andrea (2000), o ciclo de vida da segurança tem 4 fases distintas: a fase de avaliar, de projetar, de implementar e de acompanhar. Em cada fase se requer enfoque metodológico e envolvimento de profissionais com conhecimento técnico e de negócio específicos e, familiaridade com as boas práticas utilizadas em sistemas computacionais, de forma que se alcancem os melhores resultados em cada uma delas.

Como a gestão da segurança se assemelha muito, conceitualmente, à gestão de riscos, foram utilizadas as práticas do PMBOK para Gerência de Riscos na definição das fases do Processo de Gestão de Risco deste trabalho. Assim, o processo se torna mais completo e com respaldo no trabalho de uma organização conhecida como o *Project Management Institute* (PMI).

Desta forma, o Processo de Gestão de Segurança é apresentado com as seguintes fases:

Fase 1 – Planejamento da Gerência de Risco.

Fase 2 – Identificação dos Riscos.

Fase 3 – Avaliação dos Riscos.

Fase 4 – Projeto de Segurança.

Fase 5 – Implementação da Segurança.

Fase 6 – Manutenção da Segurança.

São demonstradas aqui cada uma destas fases e as principais atividades envolvidas.

## 4.1 Fase 1 – Planejamento da Gerência de Risco

Esta fase consiste em definir como abordar e planejar a gerência do risco. Através de reuniões, com participação dos responsáveis pela segurança da empresa, é desenvolvido o plano de gerência do risco, descrevendo como as demais fases estarão estruturadas.

Este plano contém:

- Metodologia: define a abordagem, ferramentas e fontes de dados a serem utilizadas na gestão do projeto. Este item indica quais serão as atividades do projeto, quais técnicas de identificação e análise de risco serão utilizadas e quais são os produtos esperados de cada fase.
- Funções e responsabilidades: indica o patrocinador do projeto e os membros da equipe. É recomendável que a equipe esteja dedicada somente a este projeto para que se obtenha foco das atividades.
- Orçamento: estabelece quanto pode ser gasto pela equipe no projeto e nas medidas a serem implementadas.
- Pontuação e interpretação: define o método de pontuação e interpretação a serem utilizados nas análises que serão utilizadas para medir qualitativamente e quantitativamente os recursos considerados críticos para a empresa. Aqui se definem os critérios de classificação e o peso de cada uma destas análises. A pontuação reflete a importância que a empresa dá para a análise qualitativa em comparação com a qualitativa, e permite que seja possível se concluir numericamente qual é o resultado do trabalho, sem interpretações subjetivas. Em algumas empresa, principalmente públicas, a pontuação precisa ser definida com antecedência ao processo, para que todos conheçam as regras desde o início e fique claro que não houve áreas com "vantagens" por critérios "criados" durante o processo.
- Tolerância: define quem influencia e como é influenciado o critério de tolerância a riscos. Esta definição vai ser importante na especificação do nível de risco aceito pela empresa.

- Relatos formatados: define o formato da documentação referente ao projeto de segurança e sua forma de divulgação.
- Monitoração: indica como os processos serão acompanhados, auditados e documentados. A documentação deve realimentar o processo, em novo planejamento.
- Macro-cronograma: estabelece as fases da gerência de riscos, estima o tempo necessário para cada uma e prevê a data aproximada da implantação em produção. Esta data será importante como meta da equipe e para indicação do esforço previsto para entrega do trabalho para a direção da empresa.

Este planejamento forma as premissas do trabalho e evita que seja perdido tempo ou que estes itens sejam definidos depois que parte do processo já esteja em andamento. O planejamento permite que sejam definidas as regras do trabalho e as responsabilidades na equipe a fim de que todos trabalhem harmonicamente pelo objetivo em comum.

## 4.2 Fase 2 - Identificação dos Riscos

O PMBOK cita o risco como "um evento ou condição incerta que, se acontecer, tem um efeito positivo ou negativo, e um objetivo de projeto".

No caso dos riscos relacionados à segurança, eles serão predominantemente de efeito negativo pois justamente corresponde a perdas ou danos a informações, recursos ou pessoal.

Esta é uma das primeiras fases do processo porque se trata do mapeamento e priorização dos riscos que formarão o escopo do projeto.

Para D'Andrea (2000), nesta fase, o objetivo é identificar riscos e vulnerabilidades do ambiente, considerando os objetivos do negócio e as características dos recursos tecnológicos utilizados. Para cada risco devem ser relacionados os seus impactos.

Além dos riscos, é necessário levantar o nível de conscientização em segurança da informação das áreas envolvidas, já que os riscos existem tanto nas áreas de negócio

quanto nas de tecnologia. É com a participação de todas as áreas que se consegue uma lista mais completa e detalhada dos riscos que afetam as principais informações da empresa.

Esta é a fase considerada mais delicada porque exige levantamento de informações de todas as áreas da empresa e envolve a capacidade analítica das pessoas envolvidas. A qualidade da identificação dos riscos depende bastante da competência das pessoas encarregadas no levantamento e análise das situações existentes, além do conhecimento dos gestores ou encarregados das áreas entrevistados sobre procedimentos, situações, perfil e cultura da empresa.

Por isso, para auxiliar nesta fase, existem algumas técnicas que podem direcionar os trabalhos desta fase, permitindo minimizar a margem de erro ou falha na identificação de riscos críticos.

### 4.2.1 Técnicas de Identificação de Riscos

Algumas técnicas citadas por D'Andrea (2000) que podem ser utilizadas nessa fase para identificação de riscos ou para o diagnóstico de vulnerabilidades são:

- Análise de vulnerabilidade: permite a identificação de vulnerabilidades de segurança na infra-estrutura tecnológica relacionadas com estratégia, planejamento e políticas de segurança, acessos lógicos, configurações de segurança e boas práticas. Esta é uma atividade para empresas que já possuem a cultura e políticas de segurança definidas e implantadas, e consiste na revisão da configuração existente e sua aderência com boas práticas de mercado. É uma técnica trabalhosa mas que precisa ser aplicada para que a equipe tenha ciência do que existe implantado para que se possa identificar suas vulnerabilidades.
- Diagnóstico de segurança: permite a revisão de segurança direcionada para componentes específicos da infra-estrutura tecnológica, como sistemas operacionais, redes locais, sistemas aplicativos ou *firewalls*. Esta análise precisa considerar todos os sistemas da empresa, identificando sua arquitetura, sua importância e sua exposição interna e externa à companhia. Esta técnica exige

bastante conhecimento da tecnologia empregada, do funcionamento operacional e da estrutura do sistema. Sem isso, podem ser deixados para trás alguns pontos que podem ser as portas de entrada para os ataques.

- Testes de penetração e intrusão: permitem, por meio de ataques aos sistemas e redes, a identificação de vulnerabilidades. Dentre as tarefas se inclui a análise sobre o mapeamento da infra-estrutura tecnológica, ataques internos e externos ao hardware, ao software, ao ambiente físico, às conexões telefônicas e aos controles administrativos. Os testes de intrusão geralmente são feitos por empresas especializadas ou grandes empresas porque estes testes requerem conhecimento especializado e uso de ferramentas específicas. As empresas que não consideram a segurança computacional como prioridade do negócio, geralmente não possuem profissionais ou recursos disponíveis para investimento neste mecanismo de identificação de vulnerabilidades.

- Revisão de riscos operacionais: permite, a partir dos objetivos de negócios da área operacional, identificar e documentar ameaças, vulnerabilidades e riscos nos processos operacionais da área, bem como o conjunto de controles existentes para minimizar os riscos. Essa é uma atividade mais analítica e envolve observações, entrevistas e leitura de documentações sobre as atividades diárias relacionados ao processo. A equipe encarregada da análise do risco precisa ter a visão de segurança para conseguir identificar os riscos operacionais nas atividades cotidianas, mas que não são percebidas por seus operadores por uma questão de hábito.

- Revisão de continuidade do negócio: permite identificar as ameaças e riscos de a instituição não estar preparada para dar continuidade às operações críticas do negócio, dependentes ou não de tecnologia. Esta é uma preocupação que vem crescendo nos últimos tempos devido ao tempo de resposta exigido pelo mercado e a confiabilidade que as empresas precisam demonstrar aos seus clientes. Hoje as empresas têm muito mais desgaste na sua imagem por causa da indisponibilidade de informações do que no passado.

O PMBOK cita outras técnicas utilizadas na identificação de riscos em projetos, e que também podem ser utilizadas na identificação das vulnerabilidades sob a visão da segurança:

- Revisão de documentação: avalia a documentação do histórico de acidentes e incidentes que ocorreram contra a segurança das informações e que ajuda na identificação de riscos que não haviam sido previstos no passado. Esta é técnica precisa ser previamente definida, para que se possa colher seus frutos no próximo ciclo. É uma técnica simples mas que precisa ser bem disciplinada para que as ocorrências sejam sempre registradas. Comumente, sempre que algum profissional da equipe de segurança é chamado devido a alguma tentativa de intrusão ou invasão, estabelece-se entre seus procedimentos o registro do ocorrido, indicando data, causa, recurso afetado e mitigação aplicada.
- *Brainstorming*: reúne algumas pessoas que contribuam para o trabalho e realizar uma reunião com contribuição de todos os membros, onde podem ser listados os vários recursos e o risco de cada um. Esta atividade também contribui para a conscientização da segurança na organização. É uma técnica bastante comum e tem o benefício dos tópicos serem avaliados sob várias perspectivas. O problema é que as discussões podem se tornar muito extensas e exigir a presença de várias pessoas chaves da instituição, o que pode comprometer a realização das reuniões. Muitas vezes os gerentes enviam representantes de área que têm visões mais restritas ou parciais dos processos, que podem comprometer a conclusão geral do assunto.
- Técnica Delphi: consiste em solicitar idéias sobre risco com base em um questionário para um grupo selecionado de consultores ou especialistas. As respostas são individualmente circuladas até se checar em um consenso. Esta técnica evita resultados tendenciosos influenciados por apenas um indivíduo. Nem sempre a empresa dispõe de especialistas no assunto, e neste caso ela convoca as pessoas que possam contribuir para o trabalho.
- Entrevistas: são feitas com gerentes de projetos que possam identificar riscos com base em sua experiência, tendo como premissas as informações do projeto. A entrevista talvez seja o método mais utilizado na identificação de riscos, mas

não é suficiente para conclusão desta atividade. É necessário pelo menos a utilização de uma das técnicas em avaliação em grupo para que as situações sejam analisadas sob diversas óticas.

- Análise de forças, fragilidades, oportunidades e ameaças: avalia dos sistemas sob a perspectiva dos elementos de forças, fragilidades, oportunidades e ameaças, aumentando a visibilidade dos riscos. Equivale à técnica denominada "análise de vulnerabilidade" citada por D'Andrea.
- *Checklist*: permite a identificação de riscos de maneira simples. É um método mais rápido, mas como não é possível listar todas as categorias de risco, pode tender à análise apenas das existentes. Ele pode ser incorporado ao processo formal do projeto para aprimorar a lista de riscos potenciais encontrados.

Como a identificação dos riscos gera, na verdade, o escopo das próximas fases por elas derivarem deste mapeamento, é importante que todos os aspectos relevantes sejam levantados, por isso comumente são utilizadas mais de uma das técnicas, aumentando assim a confiabilidade do resultado gerado. Este é o produto mais importante desta fase e sua qualidade pode garantir ou comprometer a qualidade do projeto como um todo.

Muitas empresas optam por técnicas que não exijam muito investimento, como entrevistas, checklists e brainstorming, às vezes aproveitando, inclusive, profissionais especializados em outras áreas de tecnologia para exercício destas atividades. A falta de especialização e experiência pode levar à demora de conclusão desta etapa, com o risco também de algumas vulnerabilidades deixarem de ser observadas.

### 4.2.2 Atividades desta fase

Para a identificação dos riscos, Alberts; Dorofee (2001) consideraram que a primeira atividade é identificar os tipos de informações relevantes e determinar quais são as mais importantes para a empresa.

Depois, é necessário levantar e documentar os requisitos de segurança para cada uma destas informações relevantes a respeito de sua confidencialidade, integridade e disponibilidade. Para isso, a equipe precisa ter conhecimento sobre práticas de estratégia de proteção e vulnerabilidades organizacionais, norteando suas práticas de segurança em relação a boas práticas conhecidas no mercado.

Levantadas e agrupadas todas as informações dos diferentes níveis organizacionais, os tipos de informações mais críticos são escolhidos e os requisitos de segurança são criados e refinados.

Assim, os participantes da equipe de análise constroem cenários listando as possíveis ameaças para estas informações, utilizando as técnicas citadas anteriormente.

É criada então uma lista de ameaças para cada informação crítica. É comum o uso de uma lista básica de ameaças para criar os cenários que afetam cada tipo de informação. Sempre que necessário, a lista básica de ameaças é complementada com novas fontes descobertas.

Também para Benson et al. (2000), a lista de ameaças ajuda os administradores de segurança a identificar os vários métodos, ferramentas e técnicas que podem ser usadas em um ataque. É importante que esse pessoal atualize sempre seu conhecimento porque novos métodos, ferramentas e técnicas para burlar as medidas de segurança estão sempre aparecendo.

Uma vez que as informações importantes, ameaças e vulnerabilidades foram identificadas, Alberts; Dorofee (2001) propuseram que uma equipe seja designada para analisar a informação e identificar as informações com risco de segurança. A equipe de análise fica focada na análise do risco e seu objetivo é determinar especificamente quais ameaças afetam que recursos.

Este mapeamento de riscos versus impacto será a base para a avaliação dos riscos, que é a próxima fase do processo. Além deste mapeamento, também fazem parte dos produtos desta fase os sintomas de risco ou sinais de advertência de que um risco ocorreu ou está para acontecer.

## 4.3 Fase 3 - Avaliação dos Riscos

Antes de desenvolver o projeto de segurança, que contempla um plano de mitigação, é necessário realizar a análise quantitativa e qualitativa dos riscos mapeados.

Esta fase é corresponde às fases de Análise Qualitativa de Riscos e Análise Quantitativa de Riscos do PMBOK, que conjuntamente indicam o impacto e a probabilidade dos riscos mapeados. O PMBOK analisa o risco com visão para o projeto, mas a mesma técnica cabe para a segurança porque ela possui as vulnerabilidades que põem em risco recursos e informações que podem ser de grande valor para a empresa.

Pode-se perceber essa semelhança claramente no conceito de Harris (2002) sobre a análise de risco em segurança, que para ele é o método de avaliação dos possíveis danos que podem ser causados com o intuito de justificar os métodos de prevenção. Ou seja, em segurança, a análise é feita para assegurar que a segurança seja justificável financeiramente, seja aplicado sobre o que é considerado relevante para a empresa, seja implementada no tempo apropriado e seja eficaz quanto às ameaças.

Os materiais de apoio para esta fase são o plano de gerência de riscos, o mapeamento dos riscos da fase anterior, informações históricas ou pesquisa sobre probabilidade de ocorrência dos riscos apontados e os custos dos recursos envolvidos.

Para Harris (2002), os objetivos principais da análise dos riscos são:

- Quantificar o impacto das ameaças em potencial: prover a comparação de custo/benefício, onde o custo anual das medidas de proteção é comparado com o custo esperado de perda. Pode acontecer de uma medida de proteção não ser implementada se o seu custo ultrapassar o valor anual estimado de perda. Este processo ajuda a empresa a delinear o orçamento para o programa de segurança e seus os componentes.
- Prover um balanço entre o impacto do risco e o custo das medidas de segurança.

O que se vê no mercado é que esta etapa é pouco desenvolvida nas empresas. É uma das causas das incoerências existentes entre o valor investido contra o valor estimado da perda.

A falta de hábito de se avaliar o risco, principalmente quantitativamente, acontece devido à dificuldade de se estimar os valores das perdas, já que muitas vezes envolve itens de valores subjetivos, como degradação da imagem e perda de confiabilidade na empresa. Notadamente em organizações públicas, é muito difícil, senão impossível descobrir o custo de alguns recursos utilizados, pelas áreas e superintendências trabalharem com muita independência e não compartilharem estas informações entre si. Há casos em que esta etapa é simplesmente eliminada por motivos políticos internos, e para que se consiga dar continuidade ao projeto.

O resultado deste desvio no processo é a falta de priorização adequada na implementação das medidas de segurança, o que pode gerar excesso ou falta de investimento em segurança para alguns recursos da empresa.

Harris (2002) também considera que a análise de risco ajuda ainda a integrar os objetivos do programa de segurança com os objetivos e requisitos do negócio. Quanto mais alinhados eles estiverem, maior as suas probabilidades de sucesso.

Ele sugere que seja criada uma equipe de análise de risco dedicada a esta atividade, composto por pessoas de várias ou até por todas as áreas da empresa, para que todos os riscos sejam identificados e mapeados.

O grupo precisa ser composto por profissionais de diferentes perfis, desde programadores a gerentes de produto, para que alguns riscos operacionais relacionados ao negócio podem não ser identificados ou compreendidos. Se não for possível formar um grupo com um representante de cada departamento, o time precisa entrevistar todos para garantir que todos os riscos foram identificados e quantificados.

Em pesquisa realizada em 2002 pela Consultoria Módulo, empresa especializada em segurança e com destaque no mercado nacional em segurança computacional, foi constatado que em 41% das empresas a responsabilidade da segurança da informação é atribuída à área de Tecnologia, enquanto que 31% ficam com o *Security Office* (área especializada), 23% não possui área específica e 5% fica com a Auditoria.

A formação de um grupo focado neste objetivo é imprescindível. Há toda uma visão analítica de segurança que deve fazer parte da cultura da equipe, por isso não pode

ser considerada apenas como uma atividade adicional de um profissional com outras atividades relevantes.

Mas a tendência é que a importância da equipe de segurança aumente a cada ano, principalmente por causa do crescimento do maior ponto de invasão em empresas e estações em todo o mundo, que é a internet.

E como a segurança da informação afeta a organização inteira, segundo Alberts; Dorofee (2001), a avaliação dos riscos é um problema cuja solução envolve mais que a implantação da tecnologia. A organização deve ter uma visão estratégica ao mapear seus riscos de segurança da informação. A análise do risco da informação pode ajudar a organização a avaliar práticas organizacionais junto com a implementação da tecnologia e tomar decisões baseadas nos impactos potenciais sobre a organização. Por isso, o ideal é compor uma equipe específica com a responsabilidade do projeto, mas com contribuição de várias áreas e perfis da organização.

### 4.3.1 Tipos de Análise de Risco

Há duas visões de análise de risco: quantitativa e qualitativa. Elas têm seus prós e contras, e cada uma se aplica melhor de acordo com cada situação.

Harris caracteriza a Análise Quantitativa como o método que utiliza cálculos complexos, tem facilidade de automação, propõe análise de custo/benefício, usa métricas independentes e objetivas e mostra perdas que podem acontecer no período de 1 ano.

Segundo Prado (2002), partindo do pressuposto que segurança da informação requer investimentos, deve ser estimado o valor da informação a ser protegida, de forma que seja maximizado o retorno dos investimentos. A cada novo investimento as empresas devem tornar os resultados palpáveis, expressando-os em números. Uma das técnicas disponíveis no mercado é o ROI, do inglês *Return on Investment*. Entretanto, não existe um modelo unificado para cálculo de ROI, nem o modelo ideal. Esta é uma

ferramenta que parte do princípio que a empresa é capaz de mensurar todos os seus ativos e respectivos custos, com base no comportamento histórico.

Como isso não é possível, a análise do risco não consegue ser então totalmente quantitativa.

Utiliza-se então a Análise Qualitativa, que conforme Harris (2002), envolve um grau de intuição e coleta opiniões das pessoas que melhor conhecem o processo, obtendo alto grau de participação, pelo menos dos principais gerentes da empresa.

A definição da melhor composição no processo de análise entre quantitativa e qualitativa depende bastante da cultura da empresa. Há empresas que tem como norma a apresentação de justificativa financeira detalhada de todos os seus investimentos, e há outras que se satisfazem com avaliações mais abrangentes e justificativas técnicas ou operacionais.

O PMBOK citou que a escolha é também dependente da disponibilidade de tempo e de orçamento da empresa. A análise quantitativa costuma levar mais tempo por contemplar cenários mais detalhados e levantamento de valores de todos os recursos.

Há muitos métodos e equações que podem ser usados para desenvolver uma Análise de Risco Quantitativa e Qualitativa, e muitas variáveis podem ser colocadas no processo. São apresentadas aqui as metodologias propostas por Harris (2002), que demonstram algumas das formas de avaliação utilizadas pelo mercado.

#### 4.3.1.1 Análise Qualitativa do Risco

O método de Análise Qualitativa abrange a avaliação de diferentes cenários ilustrando as possibilidades de risco e a classificação da criticidade das ameaças considerando o valor e o grau de vulnerabilidade dos recursos em risco.

As técnicas de análise qualitativa contemplam julgamento, intuição e experiência. Alguns exemplos de técnicas são: *Delphi*, *brainstorming*, *story boarding*, grupos focados, questionários, *checklists*, entrevistas. O time de análise de risco deve escolher a técnica que se adapta melhor à cultura da empresa. Este time deve ser experiente o bastante que possa reconhecer as situações de risco e avaliar como o risco pode afetar a empresa e qual a extensão de seus danos.

Um cenário é descrito para cada ameaça, sendo depois avaliado pela gerência que melhor a conhece. As medidas de segurança para a ameaça são avaliadas e o cenário é simulado com cada medida.

A técnica também citada pelo PMBOK é a construção de uma matriz de probabilidade e impacto do risco.

A possibilidade de exposição e perda pode ser classificada como alta, média e baixa, ou numa escala de 1 a 5 ou 1 a 10. A partir da possibilidade de cada ameaça atingir a empresa, da avaliação da perda potencial e as vantagens de cada medida, é gerado um relatório com os resultados, que será a base para a definição de quais as melhores medidas a serem implementadas no ambiente. Este tipo de análise força a comunicação necessária entre o time de risco para a identificação de prós e contras de cada medida de prevenção e estimula as pessoas que conhecem o assunto a serem envolvidas no processo.

#### 4.3.1.2 Análise Quantitativa do Risco

A Análise Quantitativa comumente é composta pelos seguintes passos:

- Levantar ou estimar os valores de informações e recursos.
- Estimar a perda potencial por risco ou por cenário, considerando todos os valores envolvidos como os danos físicos causados e seu custo, o custo de perda de produtividade, o valor perdido se informações confidenciais forem descobertas, o custo de recuperação contra ataques de vírus ou *hackers*, o custo de falha de dispositivos, etc.
- Analisar as ameaças, levantando informações em registros históricos e em órgãos oficiais de segurança sobre a probabilidade de ocorrência de cada risco nos departamentos; calculando a probabilidade de ocorrência de cada risco aplicada ao contexto da organização; e calculando da taxa anual de ocorrência do risco.
- Obter a perda potencial total por risco que é a combinação entre a perda potencial e a probabilidade de perda.

O PMBOK sugere como técnicas o uso de entrevistas para o levantamento da probabilidade e consequência dos riscos com especialistas e gestores dos recursos,

que podem dar uma visão mais realista e acertada dos cenários e valores que serão utilizados na análise; o uso de análise de árvore de decisão para auxiliar na avaliação do custo/benefício das medidas de proteção; ou o uso de simulações que mostre os impactos que podem ser causados através de um risco.

Na análise, os valores utilizados, correspondentes aos recursos, são relativos a todas as partes envolvidas. Esta informação é utilizada para se descobrir quanto a empresa pode estar disposta a despender na proteção de cada recurso. Este valor deve refletir todos os custos identificados que podem surgir se houver dano ao recurso. Os seguintes itens podem ser considerados na formação deste custo:

- Custo de aquisição ou desenvolvimento;
- Custo de manutenção;
- Valor do recurso para a empresa;
- Valor do recurso para adversários;
- Valor de propriedade intelectual;
- Preço de mercado;
- Custo de reposição;
- Valor da produtividade operacional afetada se o recurso não estiver disponível.

O valor do recurso é uma informação importante para definir quais mecanismos de segurança podem ser implantados e quanto pode custar essa proteção. Um erro comum é considerar apenas o valor do recurso perdido, sendo que sua extensão é muito maior para o negócio, principalmente se sua indisponibilidade afetar operações críticas da organização. Uma visão que também pode ser interessante é de verificar o quanto pode custar para a empresa se os recursos não forem protegidos.

Há sistemas críticos, como os utilizados pelas instituições financeiras para operar no Sistema de Pagamentos Brasileiro, que possuem tempo de resposta curto e perdas monetárias e danos para a imagem das instituições em caso de indisponibilidade do sistema, mesmo que seja por um período pequeno.

A expectativa de perda individual (*Single Loss Expectancy* – SLE) é um valor em dólares atribuído a um evento que representa a perda potencial da empresa caso uma ameaça específica ocorra.

SLE = valor do recurso x fator de exposição

O fator de exposição representa o percentual de perda que uma ameaça pode proporcionar a um recurso. Então, se por exemplo, um *hardware* com o valor de R$100.000, e com estimativa de 20% de danos em caso de incêndio, o valor da perda potencial calculado neste caso seria igual a R$20.000.

Para o cálculo da Perda Anual Esperada (*Annual Loss Expectancy* – ALE), é aplicada à expectativa de perda individual dada uma taxa anual de ocorrência, que é o valor que representa a possibilidade estimada de uma ameaça específica acontecer no período de um ano. O intervalo pode variar entre 0 (nunca) e 1 (sempre).

ALE = SLE x taxa anual de ocorrência

Se no exemplo anterior a probabilidade de ocorrer o incêndio for de uma vez em 10 anos, então o valor do ALE é de R$2.000.

O ALE indica que se a empresa quer tomar medidas para prevenir este tipo de dano, recomenda-se que ela gaste até R$2.000 ao ano na proteção do recurso.

Por esta fórmula fica claro por que todos os custos envolvidos na perda devem ser considerados. Se for considerado apenas o recurso atingido, a medida de segurança pode não compensar o investimento. Mas se for levado em conta o custo da indisponibilidade de produção e o custo de reposição e restauração do recurso, a implementação pode se tornar imprescindível.

As consultorias especializadas usam a combinação dos 2 tipos de análise, a qualitativa e a quantitativa, através da definição do critério de pontuação que estipula o peso da importância de cada uma das análises, criado no plano de gestão do risco gerado na primeira fase deste processo. Com o resultado chega-se a classificação final que indica qual é a prioridade de mitigação dos itens.

Um estudo realizado por Gordon; Loeb (2002) indicou que o investimento ideal em segurança não ultrapassa os 37% do valor da perda esperada. Nesta análise foram

utilizadas funções de probabilidade que, interpoladas, indicam esse percentual como suficiente para ser investido em medidas de segurança.

A demonstração do cálculo para se chegar neste percentual pode ser visto no trabalho de Gordon; Loeb (2002), "The Economics of Information Security Investiment".

## 4.4 Fase 4 - Projeto da Segurança

Relacionando com o PMBOK, esta fase corresponde à etapa de Planejamento de Resposta a Riscos, quando as opções são desenvolvidas para determinação das ações de ampliação de oportunidades e redução de ameaças. São também definidas as responsabilidades de grupos ou indivíduos em cada resposta de risco planejada.

No processo de segurança, segundo D'Andrea (2000), o objetivo desta fase é definir as ações e soluções de segurança da informação que serão aplicadas nos recursos, com base nas análises feitas na fase anterior.

Os materiais de apoio desta fase são a lista priorizada e quantificada dos riscos de segurança, a avaliação de qual o investimento aceitável para as medidas de proteção, o plano de gerência do projeto e levantamentos e práticas de medidas de segurança disponíveis no mercado.

As atividades compreendem:

- o desenvolvimento de uma estratégia de segurança;
- a elaboração ou complemento da política de segurança corporativa que incluam as medidas de proteção que serão utilizados pela empresa;
- a definição de um plano de contingência e de continuidade operacional e
- o teste do projeto elaborado.

O produto desta fase é justamente o Projeto de Segurança elaborado, já devidamente testado e validado pelos gestores das áreas envolvidas.

### 4.4.1 Estratégia de Segurança

Inicialmente, é necessário definir qual será a estratégia de segurança a ser adotada pela empresa em relação aos riscos encontrados.

Há 4 diretrizes básicas para se lidar com o risco, segundo Harris (2002):

- Reduzir: implementar medidas de prevenção, que é a opção mais indicada e adotada no Projeto de Segurança;
- Transferir: transferir o risco para outra empresa comprando um seguro, por exemplo;
- Rejeitar: negar ou ignorar o risco, deixando a empresa exposta a eles;
- Aceitar: reconhecer o risco e seus possíveis danos e decidir simplesmente em conviver com eles, dado o seu pequeno impacto ou probabilidade muito reduzida.

Ou seja, a estratégia de segurança é composta, basicamente, de quais dessas ações que vão ser selecionadas e implementadas na empresa segundo suas prioridades e sua estratégia corporativa.

Para cada risco que se queira reduzir, segundo Benson et al. (2000), devem ser traçadas duas estratégias, uma preventiva e outra reativa.

A estratégia preventiva é um conjunto de passos que ajuda a minimizar as vulnerabilidades da política de segurança e desenvolver planos de contingência. Determinar o dano que um ataque pode causar ao sistema e às vulnerabilidades exploradas durante este ataque, ajuda a desenvolver a estratégia preventiva. A estratégia preventiva pode ser desenvolvida analisando como um ataque pode afetar ou danificar o sistema e que vulnerabilidades ele explora. O conhecimento obtido nesta análise pode ajudar na implementação das políticas de segurança que vão controlar ou minimizar os ataques.

A estratégia reativa ajuda ao pessoal da segurança a assessorar o dano causado pelo ataque, reparar o dano ou implementar um plano de contingência, documentar e aprender da experiência passada e voltar o funcionamento das operações o quanto antes.

Se isso for feito para cada tipo de ataque, um padrão começará a aparecer, porque muitos fatores e soluções vão se sobrepor em diferentes tipos de ataque. Este modelo pode ser bastante útil na determinação das áreas de vulnerabilidade da empresa, e onde se concentram os seus grandes riscos.

Para a escolha de qual medida preventiva será implementada, comumente é analisada a justificativa financeira, quais são os benefícios em relação ao seu custo.

Para Harris (2002), o custo da medida, além do valor de compra, precisa também contemplar outros custos para compor o seu custo real para a empresa:

- Custo de projeto e planejamento;
- Custo de Implementação;
- Modificações de ambiente;
- Compatibilidade com outras medidas;
- Requisitos de manutenção;
- Requisitos de teste;
- Custo de Reposição, substituição ou atualização;
- Custo de Operação e suporte;
- Efeitos na produtividade.

Além do custo da medida, alguns atributos são mais favoráveis que outros e precisam ser avaliados antes da compra. Alguns destes atributos são: flexibilidade e funcionalidade, auditoria, alertas, distinção entre usuário e administrador, mínima intervenção humana, etc.

### 4.4.2 Políticas e controles de segurança

As políticas e controles também são parte importante do Projeto de Segurança. Eles são uma forma de redução do risco e vão nortear os procedimentos diários de todos os funcionários da empresa, estabelecendo os deveres de cada um quanto à segurança corporativa.

A Política de Segurança foi definida por D'Andrea (2000) como o conjunto de normas, padrões e procedimentos que deve ser seguida pela empresa a fim de que os princípios de integridade, sejam obedecidos, adequados a sua necessidade e disponibilidade de recursos.

Ela é a declaração por escrito das medidas de segurança selecionadas para a empresa, por isso é composta de:

- Procedimentos de monitoração da infra-estrutura;
- Procedimentos de identificação, priorização e solução de incidentes;
- Requisitos técnicos de segurança dos sistemas;
- Políticas de privacidade de informações;
- Definição da arquitetura de segurança corporativa, com estrutura de monitoração, estrutura organizacional, medidas de capacitação, medidas de conscientização, normas e padrões técnicos e mecanismos de segurança necessários.
- Procedimentos para atualização dos dispositivos técnicos de hardware ou software, no que tange à minimização de vulnerabilidades;
- Padrão de criptografia que deve ser utilizada;
- Procedimentos de segurança para os processos de mudança e acesso a sistemas;
- Procedimentos para auditoria da segurança de plataforma, de sistemas, de procedimentos internos, entre outros.

Benson et al. (2000) definiram que, além disso, as políticas de segurança devem definir o que é considerado valioso para a empresa e deve especificar que ações devem ser tomadas para proteger estes recursos.

O principal problema encontrado em políticas organizacionais é que a política pode não ser realmente usada pela organização. Ao invés disso, ela pode se tornar um documento que tenta apenas provar a existência de normas de segurança a auditores, advogados e outras entidades organizacionais, ou clientes, mas que não se adaptam ou não possuem credibilidade junto à organização.

Benson et al. (2000) consideraram que pode haver duas causas no fracasso de implementação das políticas de segurança: por causa de políticas fracas ou pelo fator humano. Políticas fracas podem ser combatidas com uso de pessoal especializado e testes de aderência à organização. Já o fator humano pode causar brechas porque algumas políticas tornam os processos mais rígidos ou rotineiros, que fazem com que com o tempo, as pessoas comecem a tentar se desviar delas.

Para eles, a política requer a visibilidade para ser eficaz. A visibilidade da política pode ser melhorada através de apresentações, fóruns, publicações e discussões, e precisa ser apresentada a todos os novos integrantes da empresa. A divulgação das políticas e do plano de segurança será abordado com mais detalhes na fase de implantação.

Harris (2002) classificou as políticas nas seguintes categorias:

- Regulamento: Política com o objetivo de assegurar que a empresa está seguindo os padrões definidos e geralmente é regulamentada por lei.
- Recomendação: Esta política sugere fortemente um padrão de comportamento e de atividades para uma organização e às vezes descreve as conseqüências do seu não cumprimento.
- Informativo: Tem o objetivo de ensinar ou comunicar assuntos considerados importantes para a empresa. Pode ser referente à missão e objetivos da empresa, forma de relacionamento com clientes e parceiros, etc.
- A Política de segurança deve desenvolver proteção para as seguintes categorias, Benson et al. (2000):
- Política de segurança física: abrange a proteção de procedimentos de acesso ao servidor, limpeza de equipamentos, fornecimento de energia, equipamentos contra incêndios, proteções contra roubos e cópias de segurança.
- Política de segurança de dados: controles de acesso e integridade de dados, responsabilidades de usuários na gestão de dados e aplicações, procedimentos de manutenção de dados críticos e essenciais.

- Política de segurança de rede: Controles de acesso a redes e Internet; procedimentos de autenticação; protocolos de autenticação; responsabilidade na administração da segurança.; segurança da mídia de rede utilizada (cabos, *switches* e roteadores); segurança nos servidores de arquivo e de impressoras; criptografia na internet, *Virtual Private Networks* (VPNs), sistemas de e-mail e acesso remoto e padronização da rede com o mercado.

Este é o escopo das políticas de segurança, que precisam de meios que as apóiem para que elas aconteçam. Esses meios são os padrões, procedimentos e diretrizes Harris (2002).

Os padrões especificam como os software e hardwares devem ser utilizados. Eles fazem com que as tecnologias, aplicações, procedimentos e parâmetros sejam utilizados de maneira uniforme por toda a organização. Os padrões são utilizados como regras obrigatórias, para garantir o objetivo da segurança.

Os procedimentos são um conjunto de ações detalhadas para a realização de uma atividade. Eles são utilizados para explicar a forma de instalar ou configurar componentes, sistemas operacionais, mecanismos de segurança, listas de controle de acesso, novas contas de usuário, auditoria, ou como reportar em caso de incidentes, etc. Eles tem o objetivo de garantir que sejam aplicadas as boas práticas de segurança na organização.

As diretrizes são recomendações a serem consideradas quando um padrão específico não se aplica ao caso. Referem-se geralmente a metodologias de segurança de computadores e de software, a assuntos que não são totalmente claros ou para circunstâncias imprevistas. Por isso são mais flexíveis.

### 4.4.3 Plano de Contingência e de Continuidade Operacional

Benson et al. (2000) apresentaram que as políticas e controles de segurança não vão ser completamente efetivos na eliminação dos ataques. Por essa razão é necessário desenvolver planos de contingência e recuperação nos eventos em que os controles de segurança podem falhar, que fazem parte da estratégia reativa. Mas é necessário

tomar cuidado para não serem implementados controles muito rígidos porque a disponibilidade da informação pode se tornar um problema. Deve haver um balanceamento cuidadoso entre os controles de segurança e o acesso à informação. A informação deve estar o mais livre e disponível possível para os usuários autorizados.

Para eles, o plano de continuidade do negócio é um plano alternativo que deve ser implementado quando um ataque atinge o sistema e danifica dados ou qualquer outro recurso que resulte na alteração das operações normais do negócio, afetando a produtividade. O plano é executado quando o sistema não pode ser restaurando em tempo hábil. É o "plano B" que assegura a disponibilidade, integridade e confidencialidade dos dados.

Para Harris (2002) ele tem como objetivo diminuir as perdas e assegurar a disponibilidade de pessoas e sistemas críticos.

Toigo (2000) lembrou que o fator mais crítico na restauração de sistemas para a continuidade do negócio é o tempo. Um estudo da Universidade de Minesota mostrou que em 1978 as empresas conseguiam sobreviver com interrupções de 2 a 6 dias de duração. Dada a dependência atual dos negócios com a tecnologia, é difícil imaginar se uma empresa conseguiria suportar hoje mais de 48 horas sem passar por sérias dificuldades em sua posição no mercado. Hoje o sucesso da recuperação do ambiente depende muito mais do tempo, e uma interrupção não planejada pode custar a perda de negócios, reputações, clientes e investidores. As instituições financeiras têm especial cuidado com este fator pois seu dia-a-dia é repleto de horários limites e prazos de confirmação apertados, que podem resultar em pesadas multas se não forem cumpridos.

O plano de contingência pode variar de uma restauração das cópias de segurança até a movimentação da produção para outro local ou site. Tudo depende da criticidade das operações envolvidas e do investimento existente para este propósito.

Para desenvolver o plano de continuidade operacional, Harris (2002) e Benson et al (2000) citaram as seguintes atividades:

- Identificar as funções críticas do negócio;
- Identificar os sistemas e recursos que dão apoio a estas funções;

- Estimar os desastres em potencial;
- Selecionar estratégias que prevejam:
- Respostas emergenciais, para a proteção de vidas e para a execução de ações contra danos maiores;
- Recuperação, para que o negócio entre em funcionamento o quanto antes;
- Retomada das atividades e funcionamento originais da empresa.
- Definir os responsáveis por cada atividade do processo.
- Implementar as estratégias através da sua documentação e divulgação;
- Testar e revisar o plano.

As funções críticas do negócio são feitas através da análise de impacto ao negócio, identificando as áreas que podem sofrer as maiores perdas financeiras ou operacionais em caso de desastre. Assim podem ser identificados os sistemas críticos da empresa que precisam sobreviver e estima o tempo máximo de inatividade que a empresa consegue suportar.

Para Harris (2002), deve ser criada uma equipe responsável pela continuidade do negócio, com as responsabilidades de:

- Identificar os regulamentos que precisam ser conhecidos;
- Realizar a análise de impacto ao negócio;
- Indicar quais departamentos, sistemas e processos devem tem prioridade de continuidade operacional;
- Desenvolver procedimentos para que as operações voltem ao normal;
- Atribuir tarefas para as pessoas desempenharem no período crítico;
- Documentar, comunicar aos funcionários e desenvolver o treinamento.

Todos estes pontos devem ser integrados para formar o plano, prevendo os procedimentos de prevenção contra vários tipos de cenários e sendo testado em cada um deles. Ele precisa relacionar os impactos esperados, a assistência externa existente e as dificuldades que podem ser encontradas em cada caso.

Toigo (2000), sugeriu que o plano tenha um fluxo de gestão em situações emergenciais que defina graficamente as tarefas de recuperação que precisam ser executadas. Este gráfico pode ajudar bastante a equipe responsável a entender o processo de recuperação como um todo.

Depois do plano estar elaborado, é necessário testá-lo. Benson et al. (2000) citaram que qualquer administrador sabe que isso custa dinheiro, equipamento e tempo, mas se os testes forem feitos adequadamente, os procedimentos de recuperação vão se tornar muito mais fáceis na hora da emergência. Muitos ambientes param ou demoram a voltar a operar porque os procedimentos não foram elaborados ou testados com antecedência.

E, para completar, Benson et al. (2000) recomendaram manter registro em base de dados das manutenções em geral que ocorram, principalmente dos sistemas críticos, para ajudar na descoberta de erros futuros. Os registros devem conter informações sobre a configuração do hardware, do software e da rede, data e hora do problema ocorrido, descrição do problema, procedimentos adotados, tempo de indisponibilidade do ambiente e tempo de retorno ao ambiente original.

Há alguns procedimentos que podem ser implementados visando maior disponibilidade do ambiente de produção, como alguns citados por Benson et al. (2000), como ter controle da utilização do hardware como do disco e partições, periféricos instalados, endereços utilizados, uso de tecnologias como cluster, RAID ou simplesmente redundância de servidores e existência de cópias sobressalentes, tanto de hardware como de software. Nisto incluem-se placas-mãe, CPUs, memórias, monitores, *drives*, suprimento de energia, placas de rede e modems, cabos, *hubs, switches, bridges*, roteadores, cópias originais dos softwares instalados, impressoras, scanners, etc.

### 4.4.4 Teste do Projeto Elaborado

Benson et al. (2000) apresentaram como último elemento de uma estratégia de segurança o teste das estratégias reativas e preventivas e avaliação dos seus resultados assim que elas forem configuradas. Simular ataques em um sistema ou

criar um laboratório de testes possibilita avaliar as vulnerabilidades existentes e auxiliar no ajuste às políticas de segurança e controles de acordo com os resultados obtidos.

Eles constataram que estes testes não devem ser realizados no sistema de produção porque o resultado pode ser desastroso. Assim, a falta de laboratórios e computadores de testes devido a restrições orçamentárias pode impedir a simulação de ataques. Para conseguir os recursos necessários para o teste, é importante esclarecer à gerência sobre os riscos e conseqüências de um ataque assim como as medidas de segurança que devem ser aplicadas para proteger o sistema, incluindo os procedimentos de teste. Se possível, todos os cenários de ataque devem ser fisicamente testados e documentados para determinar as melhores políticas de segurança possíveis e controles a serem implementados.

Benson et al. (2000) citaram que certos ataques, como desastres naturais como enchentes e raios, não podem ser testados, embora a simulação ajude. Por exemplo, simule um incêndio na sala do servidor que tenha resultado em perda ou dano de todos os dados. Este cenário pode ser útil para teste da eficiência dos administradores e do pessoal da segurança e para cronometrar quanto tempo leva para a organização funcionar de novo.

Testar e ajustar políticas e controles de segurança baseados nos resultados dos testes é um processo interativo. Ele nunca acaba e deve evoluir e ser revisado periodicamente para que as melhorias sejam implementadas.

Acabada a estratégia, conforme Alberts; Dorofee (2001), o time de análise provê um contexto da estratégia para os gerentes das áreas através um resumo dos riscos de cada informação crítica e dos resultados com a estratégia de proteção e as práticas de segurança propostas. Os gerentes os avaliam e alteram ou complementam quando considerarem apropriado.Os gerentes decidem então como eles vão trabalhar com o resultado das avaliações e como eles podem apoiar a iniciativa de melhoria da segurança para que o processo seja implantado.

## 4.5 Fase 5 - Implementação da Segurança

Esta é a fase em que é colocado em prática o que foi projetado. Ela não tem correspondência no PMBOK mas foi criada nesta proposta para enfatizar os cuidados necessários que evitam que todo o trabalho feito até agora não fique apenas no papel.

Segundo D'Andrea (2000), dependendo da complexidade e dos riscos específicos do levantados, deve-se considerar, como parte do processo de implantação, a adoção de tarefas dedicadas à gestão do projeto como adesão de todas as áreas da organização através da gerência e o acompanhamento da evolução da implantação.

Harris (2002) constatou que, infelizmente, muitas empresas possuem políticas de segurança definidas e documentadas por causa de auditoria, mas não compartilham ou divulgam essa informação. Este trabalho precisa não só ser bem desenvolvido, mas também bem implementado.

Para Harris (2002), para ser efetiva, há algumas ações a serem realizadas como a divulgação da documentação aos funcionários junto a informações sobre segurança, para que eles tenham visibilidade do conceito. Treinamentos, manuais, apresentações, informativos podem ajudar nesta visibilidade. Deve estar claro que estas diretrizes vêm da direção da empresa e tem o aval de todas gerências. Os funcionários precisam saber o que é esperado deles em suas ações, comportamento e performance.

Ou seja, a empresa não precisa apenas desenvolver políticas, procedimentos e padrões de segurança, para mostrar que tem responsabilidade em suas atividades e que tenta proteger recursos e funcionários de possíveis riscos. Ela também precisa se preocupar com o acompanhamento devido, que se faz através de atividades que asseguram que os mecanismos de segurança estão operacionais.

Harris (2002) constatou que o programa de conscientização de segurança deve ser desenvolvido orientado à cultura da empresa e para cada funcionário. As conseqüências do não cumprimento das normas, que podem variar de advertências a demissões, devem ser explanadas antes de serem postas em prática.

Para Brasiliano (2002), a implantação é a fase do planejamento onde o departamento de segurança ou o gerente de segurança tem de "vender" o projeto para os usuários,

para elevar a motivação e com isto desenvolver uma equipe de trabalho dinâmica e orientada.

Harris (2002) apresentou 3 níveis diferentes de programas de conscientização de segurança: gerência, staff e técnica. Cada grupo deve ser esclarecido sobre suas responsabilidades.

Para a gerência é indicada uma orientação curta e focada, com discussão sobre os recursos corporativos, ganhos e perdas financeiras relacionadas à segurança, possíveis ameaças e conseqüências e como a segurança deve ser incorporada ao ambiente da mesma forma que outras políticas. Eles precisam incentivar e apoiar a segurança e mais, ter em mente sua importância.

A média gerência pode ser colocada em outro treinamento se a organização for grande. Este grupo pode receber informações mais detalhadas sobre as políticas, procedimentos e como eles seus subordinados. Deve ser enfatizada a criticidade do apoio deste grupo para se assegurar a prática dos padrões de segurança e as conseqüências possíveis com a empresa como um todo se elas não forem aplicadas na sua área.

O grupo técnico deve receber uma apresentação diferente, mais alinhada às suas atividades diárias. Eles precisam de um treinamento ainda mais detalhado sobre configurações técnicas, indicações sobre diferentes tipos de conseqüências da segurança para que elas possam ser apropriadamente reconhecidas, e procedimentos de manutenção de incidentes.

Cada grupo precisa saber a quem reportar sobre as atividades suspeitas. Eles devem saber que não devem tentar combater o atacante, mas reportar a seus superiores para que seja acionada a equipe competente.

Para Harris (2002), o staff precisa entender por que a segurança é importante para a empresa e para eles mesmos. Quanto mais as pessoas souberem como podem ser afetadas negativamente com atividades inseguras, mais estarão propensas a colaborar.

Brasiliano (2002) sugeriu mais 2 outros níveis de treinamento:

- Aos usuários do sistema, que são os funcionários e colaboradores da empresa que operacionalizarão o sistema como um todo para que eles saibam a causa dos controles que serão implantados e que podem dificultar o seu dia-a-dia.
- Ao público externo: a mesma atenção dada aos usuários diretos, também se deve dar ao público externo, os visitantes e prestadores de serviço, para que eles saibam por que os controles existem e por eles também precisam passar por eles.

Harris também recomendou que as pessoas treinadas assinem um documento indicando que elas entenderam os tópicos discutidos e entende os efeitos do seu não cumprimento. Isso reforça a importância dos conceitos para o funcionário e evidencia que ele realmente deve ter conhecimento e responsabilidade sobre as regras.

Segundo ele, o treinamento de segurança deve acontecer periódica e continuamente. O aprendizado é melhor fixado através da repetição e recomenda-se que seja feito pode menos uma vez ao ano. O objetivo é não só fazer com que todos entendam como a segurança funciona no ambiente, mas também explicar o porquê.

De modo geral, implementar os mecanismos de segurança é mais fácil que fazer o pessoal usá-los corretamente. Muitas vezes as inovações em segurança são recebidas com resistência e oposição. Mudanças já são difíceis para as pessoas, ainda se elas restringem suas ações, é comum que elas tentem burlá-las.

Harris (2002) citou que, para que a segurança dê certo, ela precisa ser apoiada pelas altas gerências e considerada em quase todas as decisões corporativas. E como nem todos os detalhes são especificados, como quais diretórios não podem ser acessados ou quais arquivos podem ser transmitidos, a harmonia dos conceitos de segurança com a cultura da empresa é um dos grandes desafios que podem garantir ou comprometer a aplicação da segurança.

Como pode se notar, esta etapa de conscientização é a mais complexa na fase da implementação da Segurança. As outras atividades desta fase, baseadas no trabalho de Brasiliano (2002), consistem em:

- Preparar o ambiente para a implementação da segurança;

- Adquirir as ferramentas e aplicativos necessários para o controle e monitoração das atividades previstas no projeto de segurança;
- Instalar e configurar os controles em ambiente de testes e homologá-los;
- Treinar o pessoal no uso do ambiente configurado através de simulações das situações diárias, juntamente com a divulgação do manual de procedimentos, da identificação das pessoas que devem ser notificadas em caso de irregularidades e da data de início da vigência dos novos controles e procedimentos;
- Instalar e configurar os mesmos controles já testados no ambiente de testes no ambiente de produção e
- Divulgar o início do funcionamento do sistema.

Esta fase parece ser simples pelas configurações já terem sido simuladas em ambiente de testes, mas tem um fator importante que vai pesar no sucesso desta etapa: a aceitação da organização. A reação do usuário pode ser de total aceitação das novas regras como pode ser de recusa ou tentativa de desvio dos procedimentos.

Outro impacto grande será na adequação de sistemas existentes nas políticas definidas, que pode exigir muitas horas de implementação ou de proposta de customizações de sistemas fora do padrão definido.

E além das medidas previstas para mitigação dos riscos, devem ser também implementadas as ações correspondentes às outras soluções de tratamento do risco, como o contrato com seguradoras.

## 4.6 Fase 6 - Manutenção da Segurança

A última fase deste processo cíclico é a manutenção da segurança, que corresponde à etapa de Controle e Monitoração dos Riscos no PMBOK. Como na segurança, após a implantação do projeto, os riscos são continuamente monitorados, para garantir que as medidas estejam sendo eficazes e para que se acompanhe a evolução e variação dos riscos no tempo.

Segundo D'Andrea (2000), esta fase tem como objetivo manter a segurança da informação em funcionamento, administrando a segurança dos recursos tecnológicos, proporcionando feedback e capacitação permanente para as áreas envolvidas e avaliando as necessidades de novas ações de segurança direcionadas às lacunas ou falhas identificadas.

Para Benson et al. (2002), assim que os mecanismos de segurança foram estabelecidos, é necessário que sejam monitorados continuamente, para saber se eles estão trabalhando apropriadamente e para observar se está ocorrendo algum problema de comportamento.

Isso pode ser feito através dos registros dos ataques e problemas ocorridos, para que possam ser eliminados ou pelo menos minimizados no futuro. Fazer simulações da situação permite melhor análise e garante bons resultados.

O PMBOK recomendou que os riscos residuais sejam cuidadosamente monitorados pois eles são os riscos que não foram mitigados. Há ainda outros riscos que surgem com o tempo, e que precisam ser submetidos também ao processo de análise.

Mas o mecanismo mais importante nesta fase é a auditoria das atividades da empresa. Segundo Hayday (2001), a auditoria determina o status de segurança da empresa. Ela se enquadra em 3 áreas principais:

- Gestão de vulnerabilidades: verifica a configuração de um sistema ou sistemas contra uma linha base definida e, talvez assegure que a linha base aplicada satisfaz às recomendações atuais de prática de segurança melhor.
- Gestão da ameaça: detecta em tempo real uma ameaça ou a efetiva intrusão.
- Gestão de eventos: coleta e analisa dados sobre eventos gerados pelos sistemas que revelam informações de segurança relacionadas com a utilização efetiva ou com o abuso de um determinado sistema. Um evento é qualquer ocorrência significativa no sistema que exige notificação.

A gestão de vulnerabilidades e de ameaças permite identificar medidas diretamente contra a ameaça.

A auditoria de eventos complementa essas duas abordagens apresentando informações sobre como os sistemas são executados diariamente pelos usuários, já

que eles também são fonte de ameaças para a empresa. Após o incidente de segurança, uma auditoria adequada e apropriada do sistema e do usuário poderá ajudar a descobrir a extensão do incidente e como foi possível sua ocorrência. Além disso, pode servir para fornecer provas do incidente.

Quando a auditoria indicar que algo de grave ocorreu, é preciso ter uma resposta planejada por antecipação. Neste caso, os planos de segurança devem prever ações que precisam ser tomadas para preservar as provas, tanto em termos da configuração do sistema atual quanto à integridade dos logs de auditoria.

Se a empresa não tem qualquer medida de auditoria instalada, verificar como a segurança foi comprometida talvez seja difícil, senão impossível.

Hoje existem monitores de trilhas de auditoria que emitem avisos aos administradores ou executam uma ação preventiva com base em comportamentos suspeitos em operações realizadas e registradas pelo sistema.

Mas o ciclo de vida da segurança não acaba aqui. Segundo Benson et al. (2002), para a manutenção da segurança, as políticas de segurança precisam ser periodicamente revisadas e avaliadas quanto a sua efetividade. Se elas não estiverem atendendo de acordo com o esperado, precisam ser atualizadas, sempre com a participação e comprometimento das principais gerências, *security officer* e administradores, e condizente com as regras gerais da organização.

Para Benson et al. (2002), é importante que o ciclo seja reiniciado periodicamente para que todo o processo de segurança seja novamente avaliado e atualizado, porque novas tecnologias de desenvolvimento, arquiteturas, sistemas operacionais, aplicações, ferramentas de proteção sempre aparecem no mercado, e principalmente porque novas tecnologias de ataque ou intrusão estão sendo constantemente criadas ou aperfeiçoadas dentro ou fora da organização.

Segundo Harris (2002), um outro plano que precisa de periódica manutenção dentro da área de segurança é o plano de continuidade operacional, por causa de mudanças no ambiente e a infra-estrutura ao longo do tempo; por causa de reorganizações e fusões na empresa; por causa de substituições no quadro de funcionários e pelo plano não ter relação direta com a rentabilidade o que significa que pode ser facilmente esquecido.

Mas ele também sugere formas de manter o plano atualizado:

- Fazer com que a continuidade do negócio seja considerada em toda decisão;
- Inserir nas responsabilidades dos cargos a tarefa da manutenção;
- Incluir a manutenção na avaliação do pessoal;
- Promover auditorias internas que incluam a avaliação de documentação e procedimentos quanto à recuperação de desastres e
- Promover treinamentos regulares que utilizem o plano.

A manutenção da segurança pode ser a última fase do processo de gestão de segurança, mas não significa que ela indica o fim do processo. Pelas suas próprias atividades pode-se perceber que este processo é contínuo, pois os planos definidos ficam desatualizados pela própria dinâmica da empresa e das tecnologias do mercado.

O que acontece nas empresas é o reinício de todo o processo periodicamente para que os novos negócios da empresa e os já existentes estejam sempre protegidos ou assumindo um nível de risco bem definido contra novas ameaças e vulnerabilidades.

As saídas desta fase são as atualizações nos planos definidos, atualizações nos checklists de riscos e o histórico das ocorrências para análises e providências em processos futuros.

# 5. CONCLUSÃO

O trabalho abordou as práticas do processo de gestão de segurança de sistemas computacionais baseado nas recomendações do PMBOK para gestão de risco de projetos.

Esta proposta pode ser utilizada como apoio para a definição do processo de gestão de segurança em empresas que ainda não possuem um processo ou políticas de segurança definidos, pois ilustra os principais cuidados a serem tomados e um resumo estruturado das práticas de mercado relacionadas a essa área.

Ele pode ainda ser utilizado para a avaliação comparativa de um processo já existente na empresa, permitindo a identificação de pontos ainda não cobertos ou atividades relevantes que não tenham sido consideradas.

Ele pode também simplesmente complementar ou enriquecer o conhecimento do leitor quanto às práticas em segurança da informação, numa visão cíclica e estruturada do processo, e não como atividades e controles isolados como se encontra geralmente em bibliografia sobre o assunto.

Para a realização deste estudo, foi muito importante a contribuição do guia de práticas de segurança utilizado para certificação internacional em segurança, e claro, do PMBOK que foi a base para a composição das fases do processo.

O desenvolvimento de um processo com este âmbito enfatizou a necessidade das empresas de um planejamento e de análises que se assemelham muito aos encontrados na gestão de riscos de projetos. As atividades deste processo mostraram-se essenciais para que vulnerabilidades e ameaças fossem convenientemente analisadas e seus riscos mitigados ou pelo menos conhecidos pela empresa.

A implantação da segurança costuma ser subestimada quanto a sua complexidade e esforço de implementação, e o que se percebe é que com o detalhamento do escopo e do planejamento muitos itens de alta complexidade técnica e operacional vão

surgindo, de forma que fica muito difícil controlá-los sem um plano e diretrizes bem definidas, alinhadas com o negócio e com as metas da empresa.

Os benefícios que se observa com a utilização de um processo definido são: a visão do grande esforço necessário para a implantação da segurança em uma organização, e a minimização de investimentos desnecessários, seja por atacar riscos irrelevantes, seja por despender em proteção mais que o valor de recuperação do recurso.

Outros aspectos relevantes para a segurança que não foram abordados por esse trabalho por não fazerem parte do escopo são a segurança aplicada ao processo de desenvolvimento de sistemas computacionais (especialmente em etapas críticas como de projeto, implantação e manutenção), novas tecnologias de autenticação de usuário como biologon, mas que podem ser estudados em uma continuação deste trabalho.

Reconhece-se também que há necessidade de validação da proposta, no entanto foge do escopo trabalho e é inviabilizado pelo prazo, já que o processo pode ser bastante extenso dependendo da variedade e complexidade do ambiente em que for aplicado.

Apesar da ausência de uma validação prática do processo, ele é bastante palpável por terem sido observadas algumas práticas já existentes em mercado e por aplicar recomendações do PMBOK, que concentra os conhecimentos e experiências de especialistas em contexto mundial.

A utilização da estrutura do processo do PMBOK sob o contexto das práticas de mercado em segurança da informação formou a base deste processo.

Mas o que especialistas e o mercado percebem é que a metodologia não é o único insumo para se atingir o objetivo de implementar controles de segurança em uma organização. O processo pode assegurar que o planejamento seja bem elaborado e completo, mas é a conscientização da importância da segurança e sua absorção pela cultura da empresa que vão determinar o sucesso do projeto. A segurança não é composta apenas de regras e controles sob todas as ações dos usuários; o que é relevante no dia-a-dia são as atitudes das pessoas que tem consciência da importância da segurança para a organização e para ela mesma.

# LISTA DE REFERÊNCIAS

ALBERTS, C.; DOROFEE, A. An introduction to the Octave Method. Software Engineering Institute, Carnegie Mellon University, 2001. Disponível em <http://www.cert.org/octave/methodintro.html>. Acesso em 01 jun. 2002.

ANDERSON, R. Why Information Security is Hard - An Economic Perspective. Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual , 2001. Páginas 358 a 365.

BENSON, C. et. al. Microsoft Solutions Framework: Best Practices for Enterprise Security. Microsoft Corporation, 2002. Disponível em <http://www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp>. Acesso em 12 jun. 2002.

BRASILIANO, A. C. R. Metodologia de Implantação de Projetos de Segurança. Brasiliano e Associados, São Paulo, 2002. 7p. Disponível em <http://www.brasiliano.com.br/artigo_598.htm>. Acesso em 21 out. 2002.

D'ANDREA, E. R. P. (Coord) Segurança em Banco Eletrônico. São Paulo: PricewaterhouseCoopers, 2000. 134 p.

GORDON, L. A.; LOEB M. P. The Economics of Information Security Investiment. University of Maryland. ACM Transactions on Information and System Security, Vol. 5, No. 4, Nov. 2002.

HARRIS, C. CISSP All-in-One Certification Exam Guide. Berkeley, California: McGraw-Hill/Osborne, 2002. 978 p.

HAYDAY, J. Segurança para Windows 2000: o guia de referência técnica / Microsoft Press. Tradução de André L. Cardoso e Anderson Almeida. Rio de Janeiro: Campus, 2001. 646 p.

MICROSOFT CORPORATION. Microsoft Prescriptive Guidance: Security Operations Guide for Windows 2000 Server. Microsoft Corporation, 2002. 187 p. Disponível em <http://www.nsa.gov/winsecurity/win2k/download.htm>

MÓDULO Security Solutions. 8ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro: Módulo Security Solutions, 2002. 23p. Disponível em <http://www.modulo.com.br/index.jsp>. Acesso em 25 nov. 2002.

PRADO, L. Quatro Passos no Gerenciamento de Riscos. Securenet, 2002. 4p. Disponível em <http://www.securenet.com.br/artigo.php?artigo=114>. Acesso em 16 nov. 2002.

BRASIL. Project Management Institute - PMI. PMBOK. Tradução livre da PMIMG. Belo Horizonte: PMIMG, 2002. 151 p. Disponível em <http://www.pmimg.org.br>. Acesso em 22 Set. 2002.

TOIGO, J. W. Disaster Recovering Planning: Strategies for Protecting Critical Information. 2. ed. Upper Saddle River, New Jersey: Prentice Hall PTR, 2000. 432 p.

TURBAN, E. et al. Eletronic Commerce: A Managerial Perspective. Upper Saddle River, New Jersey: Prentice Hall, 2000. 520 p.