Gestão de Segurança da Informação
Marcos Aurelio Pchek Laureano
marcos@laureano.eti.br
01/06/2005

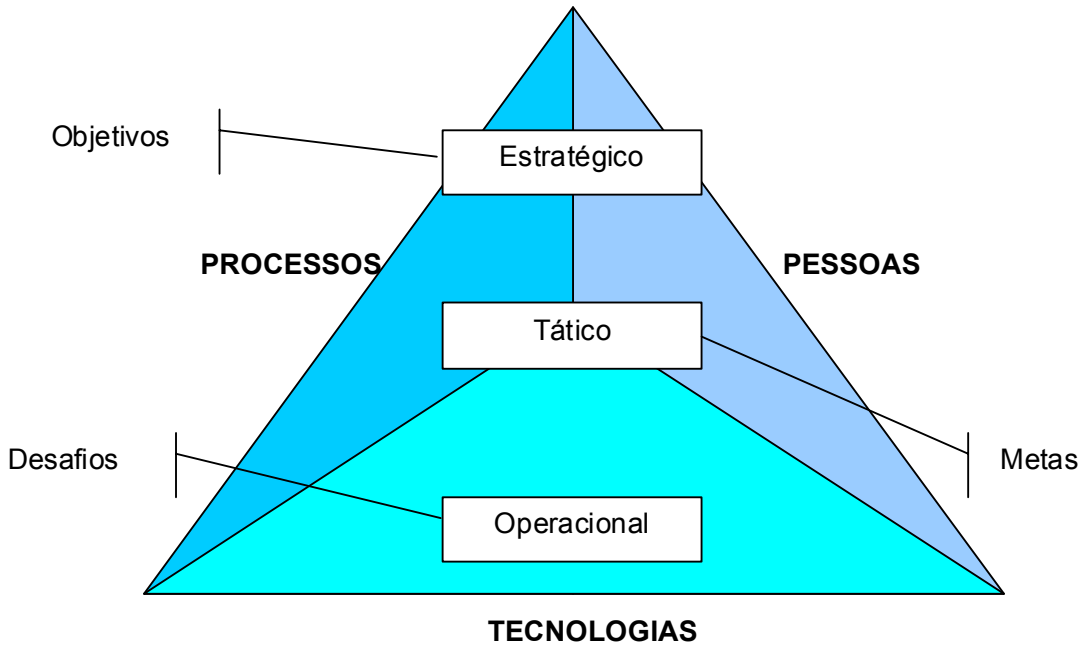
GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005

CAPÍTULO I

A importância da Informação

A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário (Rezende e Abreu, 2000). A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias. A próxima figura demonstra, do ponto de vista estratégico, o relacionamento dos processos, tecnologias e pessoas.



Vivemos em uma sociedade eu se baseia em informações e que exibe uma crescente propensão para coletar e armazenar informações e o uso efetivo da informação permite que uma organização aumente a eficiência de suas operações (Katzam, 1977).

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida (NBR 17999, 2003). Na sociedade da informação, a informação é o principal patrimônio da empresa e está sob constante risco (Dias, 2000). A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa (Sêmola, 2003). A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade (Rezende e Abreu, 2000).

As empresas já perceberam que o domínio da tecnologia como aliado

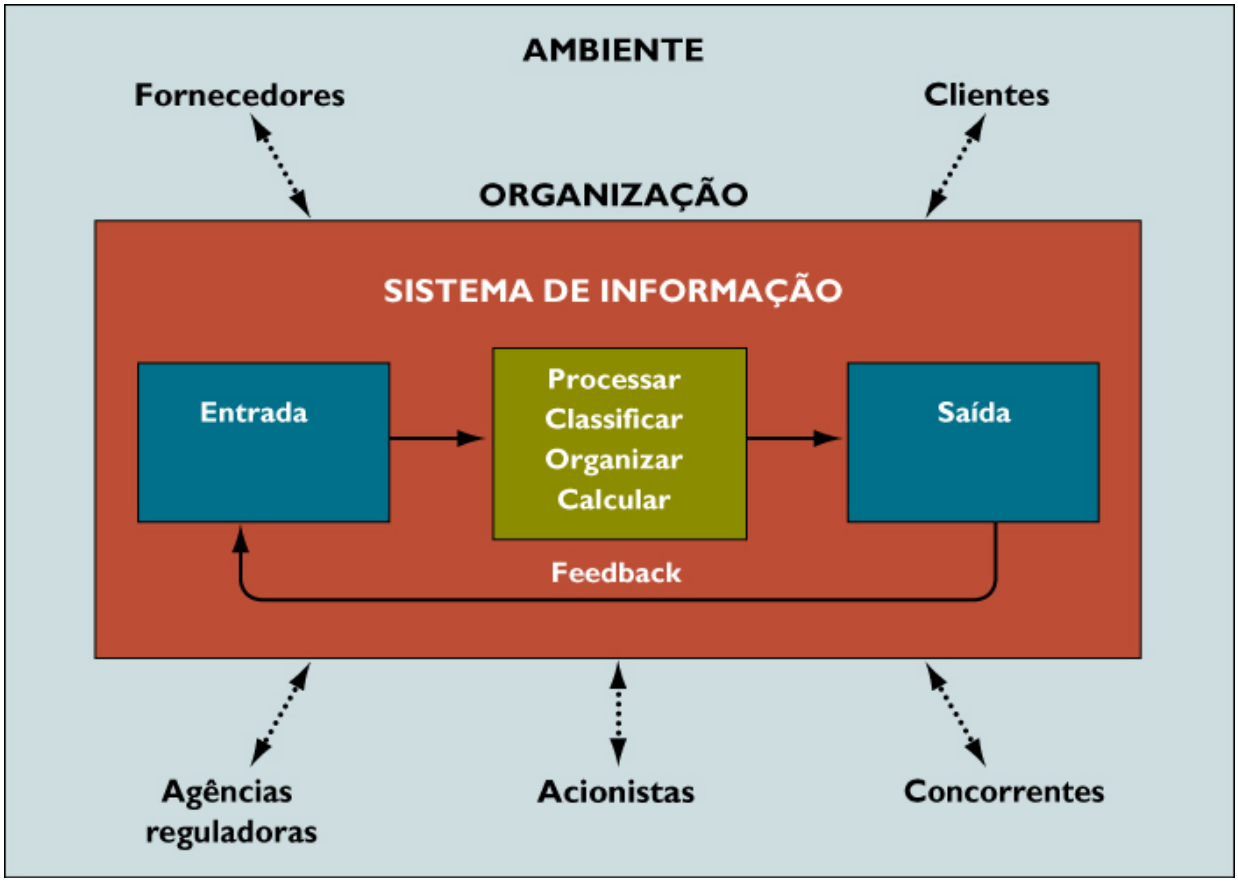
para o controle da informação é vital. O controle da informação é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial (Synnat, 1987; Feliciano Neto, Furlan e Higo, 1988). Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão. A informação é substrato da inteligência competitiva; deve ser administrada em seus particulares, diferenciada e salvaguardada.

Sistema de Informação[1]

Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização. Além de dar suporte à tomada de decisões, à coordenação e ao controle, esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos.

Os sistemas de informação contêm informações sobre pessoas, locais e coisas significativas para a organização ou para o ambiente que a cerca. Três atividades em um sistema de informação produzem as informações de que as organizações necessitam para tomar decisões, controlar operações, analisar problemas e criar novos produtos ou serviços. Essas atividades são a entrada, o processamento e a saída (veja a próxima figura).

[1] Baseado em (Laudon e Laudon, 2004)

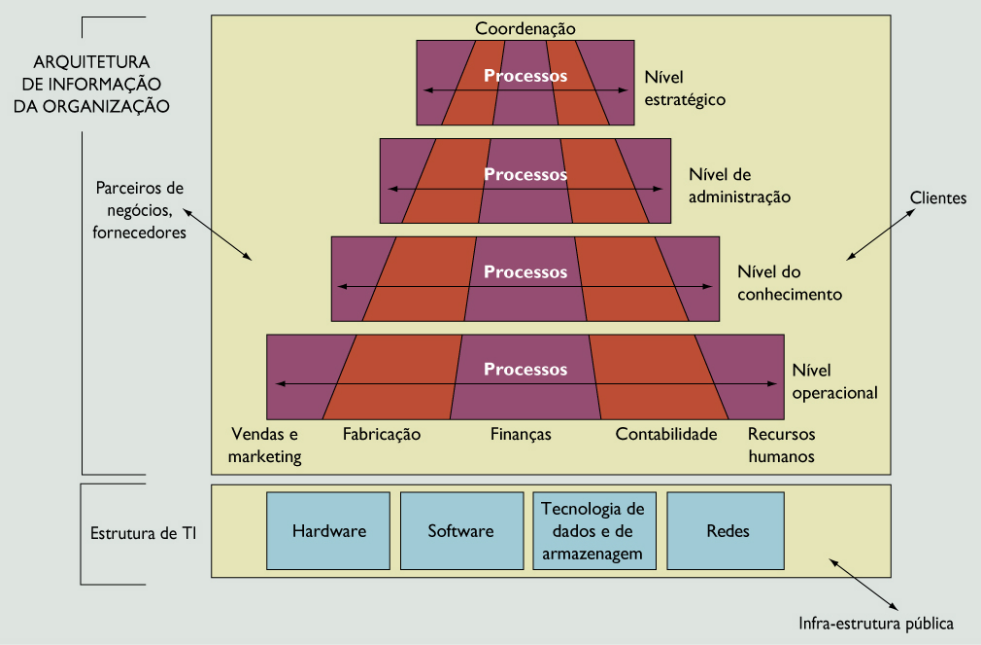


A entrada captura ou coleta dados brutos de dentro da organização ou de seu ambiente externo. O processamento converte esses dados brutos em uma forma mais significativa. A saída transfere as informações processadas às pessoas que as utilizarão ou às atividades em que serão empregadas. Os sistemas de informação também requerem um feedback, que é a entrada que volta a determinados membros da organização para ajudá-los a avaliar ou corrigir o estágio de entrada.

Os sistemas de informação são partes integrantes das organizações. Na verdade, para algumas empresas, como as que fazem avaliação de crédito, sem sistema de informação não haveria negócios.

Os administradores de hoje devem saber como estruturar e coordenar as diversas tecnologias de informação e aplicações de sistemas empresariais para atender às necessidades de informação de cada nível da organização e às necessidades da organização como um todo.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005



Informação, competitividade e estratégia

Segundo (Rezende e Abreu, 2000), a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia. A informação auxilia os executivos a identificar tanto as ameaças quanto as oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz. A informação funciona também como um recurso essencial para a definição de estratégias alternativas. A informação é essencial para a criação de uma organização flexível na qual existe um constante aprendizado.

As organizações estão modificando-se profundamente, invertendo suas pirâmides organizacionais, criando unidades de negócios autônomas, descentralizando decisões e constituindo parcerias. A garantia de sua integração e da manutenção de parâmetros comuns de atuação é dada pela informação, que flui entre suas várias partes.

A eficácia de uma empresa pode ser definida pela relação entre resultados obtidos e resultados pretendidos. Para que uma empresa possa adotar políticas estratégicas eficazes, é necessário que estas sejam baseadas em informação, que passa a ser a principal matéria-prima de qualquer organização.

Da perspectiva de uma empresa, o sistema de informação é uma solução organizacional e administrativa baseada na tecnologia de informação para enfrentar um desafio proposto pelo ambiente (Laundon e Laudon, 2004). Desta forma, os sistemas de informação são essenciais para qualquer organização (veja a próxima figura). Ter o controle sobre este ambiente é essencial para a qualidade dos serviços prestados pela empresa.

A informação certa comunicada a pessoas certas é de importância vital para a empresa. Para a tomada de decisões, é necessários um cuidado detalhado com a integridade, precisão, atualidade, interpretabilidade e valor geral da informação.

Classificação das Informações

Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente. Em (Wadlow, 2000; Abreu, 2001; Boran, 1996) é exposto, a necessidade de classificação da informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa:

- **Pública** – informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;

- **Interna** – o acesso a esse tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;

- **Confidencial** – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;

- **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

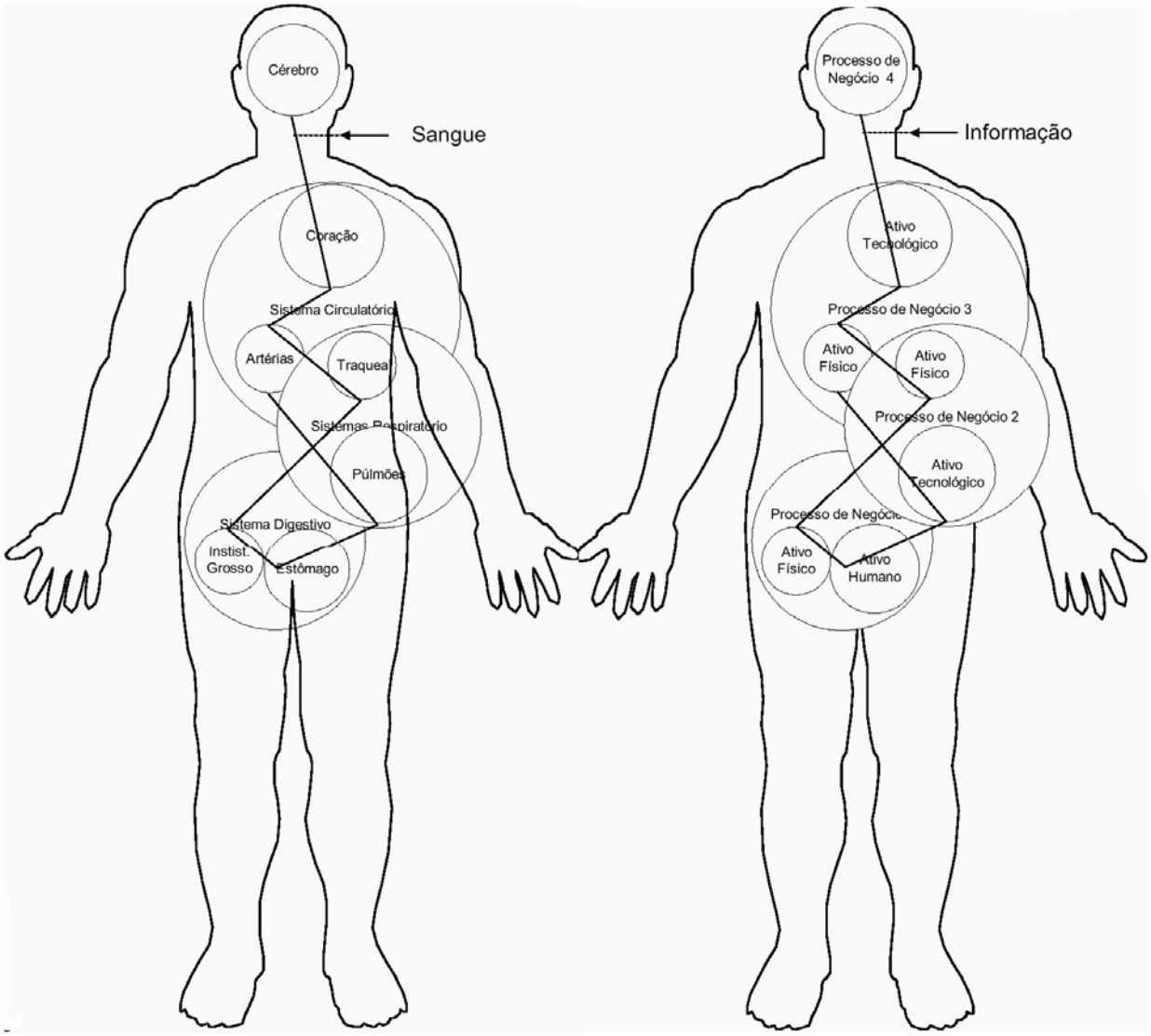
Entretanto, independentemente da relevância ou tipo da informação, a gestão dos dados organizacionais é estratégica, pois possibilita o apoio para a tomada de decisões em qualquer âmbito institucional. Algumas informações são centrais para organização e a divulgação parcial ou total destas pode alavancar um número de repercussões cuja complexidade pode ser pouco ou nada administrável pela organização com conseqüências possivelmente nefastas.

O conceito de engenharia da informação – que é um conjunto empresarial de disciplinas automatizadas, dirigindo ao fornecimento da informação correta para a pessoa certa no tempo exato (Martin, 1991; Feliciano Neto, Furlan e Higo, 1988) – já demonstrava a importância da segurança da informação para as instituições.

Conforme (Crosby, 1992), a qualidade dos processos custa dinheiro, mas a falta dela custa muito mais. Estabelecendo uma analogia, a segurança custa dinheiro mas a sua ausência poderá custar muito mais.

Ciclo de Vida da Informação[2]

O Ciclo de Vida é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, pos sua vez, mantêm a operação da empresa. A próxima figura demonstra uma relação entre o corpo humano e o negócio de uma empresa.

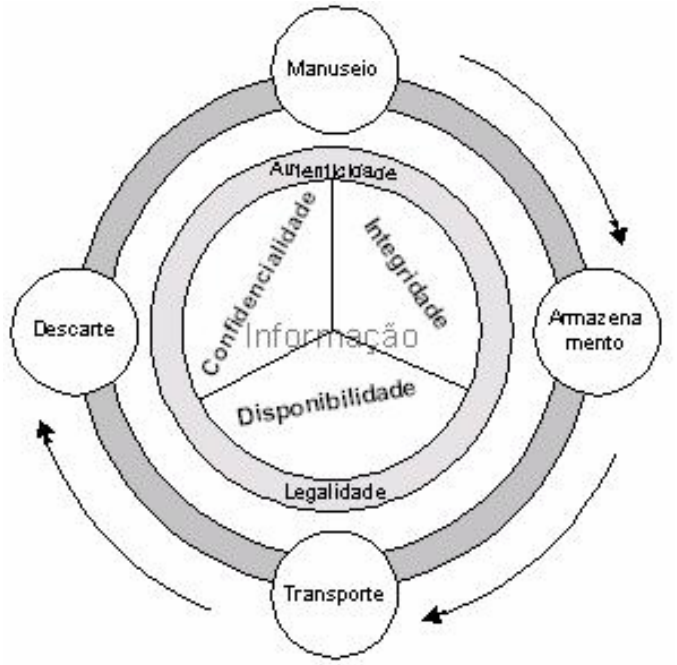


Os órgãos (analogamente, ativos físicos, tecnológicos e humanos), se utilizam sangue (analogamente, informação), para pôr em funcionamento os

[2] Baseado em (Sêmola, 2003)

sistemas digestivo, respiratório, etc. (analogamente, processos de negócio), para conseqüentemente, manter a consciência e a vida do indivíduo (analogamente, a continuidade do negócio).

Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, a próxima figura revela todos os 4 momentos do ciclo de vida que são merecedores de atenção.



- **Manuseio** – Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.
- **Armazenamento** – Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo.
- **Transporte** – Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
- **Descarte** – Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD-ROM usado que apresentou falha na leitura.

CAPÍTULO II

Segurança da Informação e seus Critérios

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

As redes de computadores, e conseqüentemente a Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como os riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (Laureano, 2004).

A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (NBR 17999, 2003; Dias, 2000; Wadlow, 2000; Krause e Tipton, 1999).

Segurança é a base para dar ás empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma a proporcionar confidencialidade, integridade e disponibilidade – que conforme (NBR 17999, 2003; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002), são os princípios básicos para garantir a segurança da informação – das informações:

- **Confidencialidade** – A informação somente pode ser acessada por pessoas explicitamente autorizadas; É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

- **Disponibilidade** – A informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;

- **Integridade** – A informação deve ser retornada em sua forma original no momento em que foi armazenada; É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

O item integridade não pode ser confundido com confiabilidade do conteúdo (seu significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer integra (não sofrer alterações por pessoas não autorizadas).

A segurança visa também aumentar a produtividade dos usuários através de um ambiente mais organizado, proporcionando maior controle sobre os recursos de informática, viabilizando até o uso de aplicações de missão crítica.

A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem os seus objetivos, pois seus sistemas de informação serão mais confiáveis.

Outros autores (Dias, 2000; Wadlow, 2000; Shirey, 2000; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002; Sêmola, 2003; Sandhu e Samarati, 1994) defendem que para uma informação ser considera segura, o sistema que o administra ainda deve respeitar:

- **Autenticidade** – Garante que a informação ou o usuário da mesma é autêntico; Atesta com exatidão, a origem do dado ou informação;

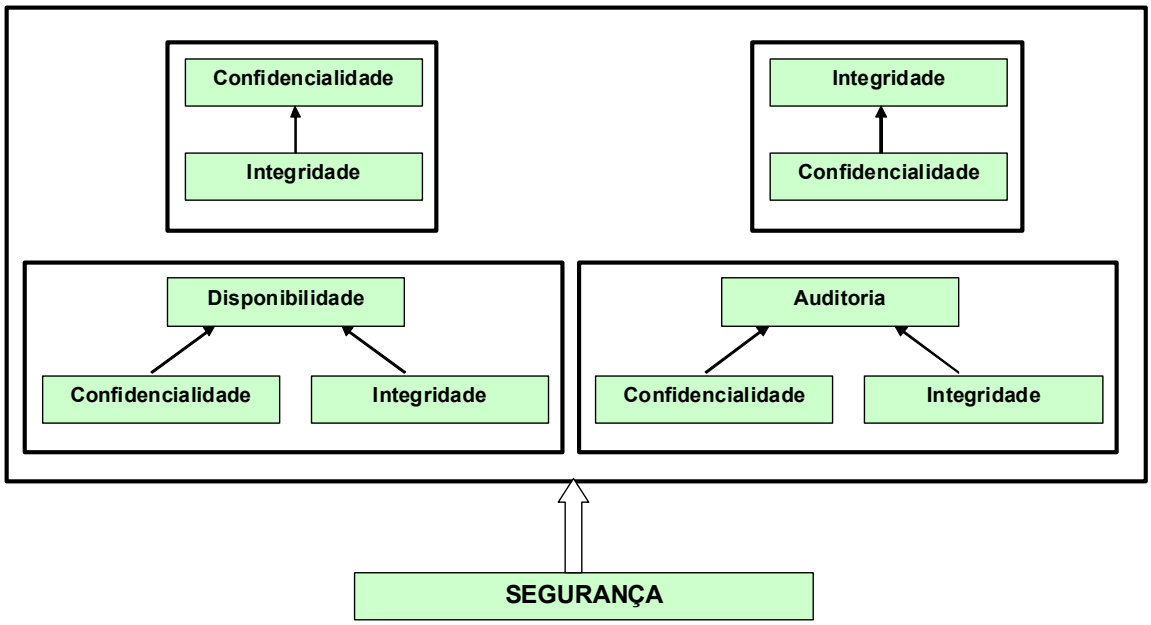
- **Não repúdio** – Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;

- **Legalidade** – Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

- **Privacidade** – Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste é caso é atribuído o caráter de confidencialidade a informação); É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.

- **Auditoria** – Rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em software significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

Em (Stoneburner, 2001) é sugerido que a segurança somente é obtida através da relação e correta implementação de 4 princípios da segurança: confidencialidade, integridade, disponibilidade e auditoria. A próxima figura ilustra a relação dos princípios para a obtenção da segurança da informação.



A confidencialidade é dependente da integridade, pois se a integridade de um sistema for perdida, os mecanismos que controlam a confidencialidade não são mais confiáveis.

A integridade é dependente da confidencialidade, pois se alguma informação confidencial for perdida (senha de administrador do sistema, por exemplo) os mecanismos de integridade podem ser desativados.

Auditoria e disponibilidade são dependentes da integridade e confidencialidade, pois estes mecanismos garantem a auditoria do sistema (registros históricos) e a disponibilidade do sistema (nenhum serviço ou informação vital é alterado).

Morais da Segurança e Composição da Segurança[3]

Como não poderia deixar de ser, a segurança também possui algumas "morais" que surgiram no decorrer do tempo:

- As portas dos fundos são tão boas quanto às portas da frente.

- Uma corrente é tão forte quanto o seu elo mais fraco.

- Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.

[3] Publicação de Steve Bellovin, na lista de distribuição de firewalls em 10 de dezembro de 1992

CAPÍTULO III

Outros Conceitos

Ameaças

Em inglês, é utilizado utilizamos o termo "*threat*" para definir ameaça. E temos vários tipos de *threat* (Shirey, 2000):

- **Ameaça Inteligente**: Circunstância onde um adversário tem a potencialidade técnica e operacional para detectar e explorar uma vulnerabilidade de um sistema;

- **Ameaça**: Potencial violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano;

- **Ameaça de Análise**: Uma análise da probabilidade das ocorrências e das conseqüências de ações prejudiciais a um sistema;

- **Conseqüências de uma ameaça**: Uma violação de segurança resultado da ação de uma ameaça. Inclui: divulgação, usurpação, decepção e rompimento;

A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e conseqüentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem.

Conforme descrito em (Sêmola, 2003), as ameaças podem ser classificadas quanto a sua intencionalidade e ser divididas em grupos:

- **Naturais** – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.

- **Involuntárias** – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causados por acidentes, erros, falta de energia, etc.

- **Voluntárias** – Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Algumas outras ameaças aos sistemas de informação:

- Falha de hardware ou software
- Ações pessoais
- Invasão pelo terminal de acesso
- Roubo de dados, serviços, equipamentos
- Incêndio
- Problemas elétricos
- Erros de usuários
- Mudanças no programa
- Problemas de telecomunicação

Elas podem se originar de fatores técnicos, organizacionais e ambientais, agravados por más decisões administrativas (Laudon e Laudon, 2004).

Ataques

Em inglês, é utilizado o termo "*attack*" para definir ataque. E existem vários tipos de ataques. Ataque pode ser definido como um assalto ao sistema de segurança que deriva de uma ameaça inteligente, isto é, um ato inteligente que seja uma tentativa deliberada (especial no sentido de um método ou técnica) para invadir serviços de segurança e violar as políticas do sistema (Shirey, 2000).

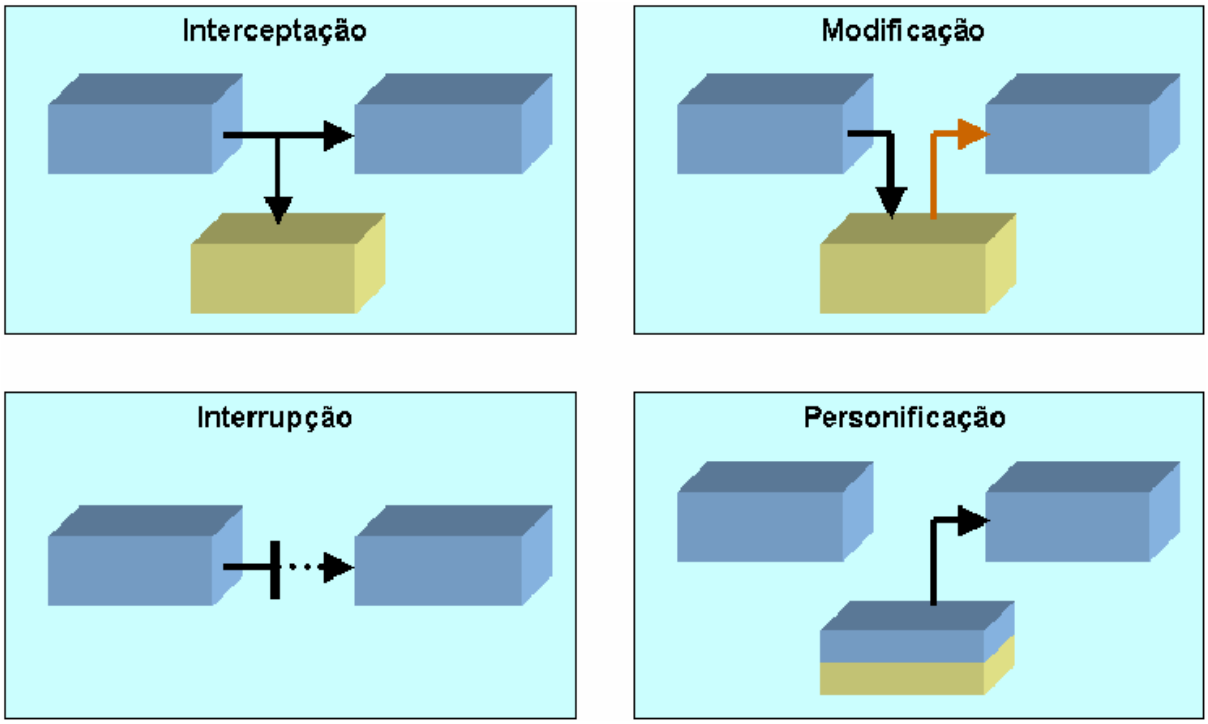
O ataque é ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios citados anteriormente.

Um ataque pode ser *ativo*, tendo por resultado a alteração dos dados; *passivo*, tendo por resultado a liberação dos dados; ou *destrutivo* visando à negação do acesso aos dados ou serviços (Wadlow, 2000).

O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes.

Para implementar mecanismos de segurança faz-se necessário classificar as formas possíveis de ataques em sistemas:

- **Interceptação**: considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).
- **Interrupção**: pode ser definida como a interrupção do fluxo normal das mensagens ao destino.
- **Modificação**: consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.
- **Personificação**: considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.



Vulnerabilidades

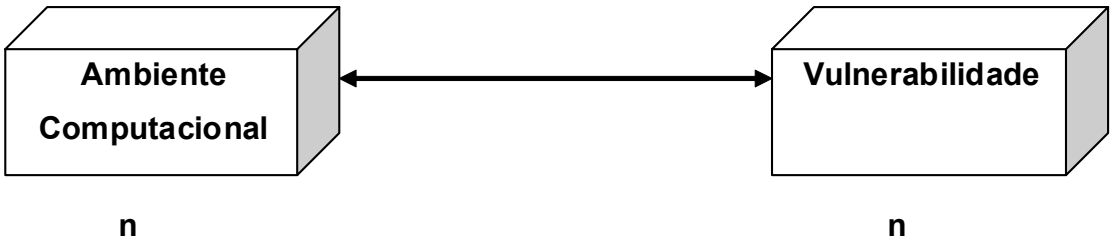
A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc.

Todos os ambientes são vulneráveis, partindo do principio de que não existem ambientes totalmente seguros. Muitas vezes encontramos vulnerabilidades nas medidas implementadas pela empresa.

Identificar as vulnerabilidades que podem contribuir para as ocorrências de incidentes de segurança é um aspecto importante na identificação de medidas adequadas de segurança.

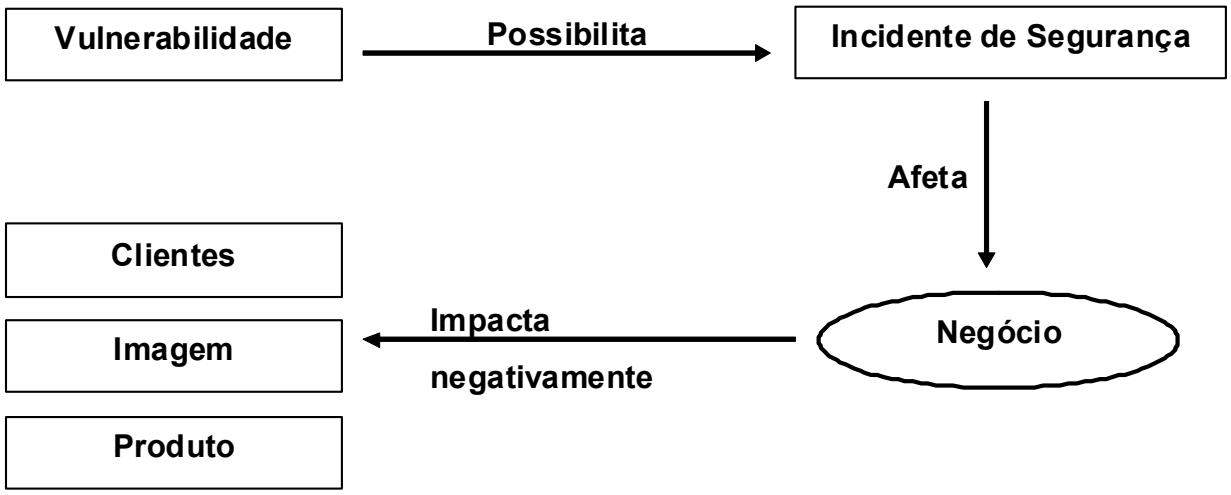
As vulnerabilidades estão presentes no dia-a-dia das empresas e se apresentam nas mais diversas áreas de uma organização.

Não existe uma única causa para surgimento de vulnerabilidades. A negligência por parte dos administradores de rede e a falta de conhecimento técnico são exemplos típicos, porém esta relação pode ser entendida como sendo de **n** para **n**, ou seja, cada vulnerabilidade pode estar presente em diversos ambientes computacionais, conforme demonstra a próxima figura.



Relação Ambiente Computacional X Vulnerabilidades

Cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança. Desta forma, podemos concluir que são as vulnerabilidades as principais causas das ocorrências de incidentes de segurança, conforme apresenta à próxima figura.



Por que sistemas são vulneráveis[4]

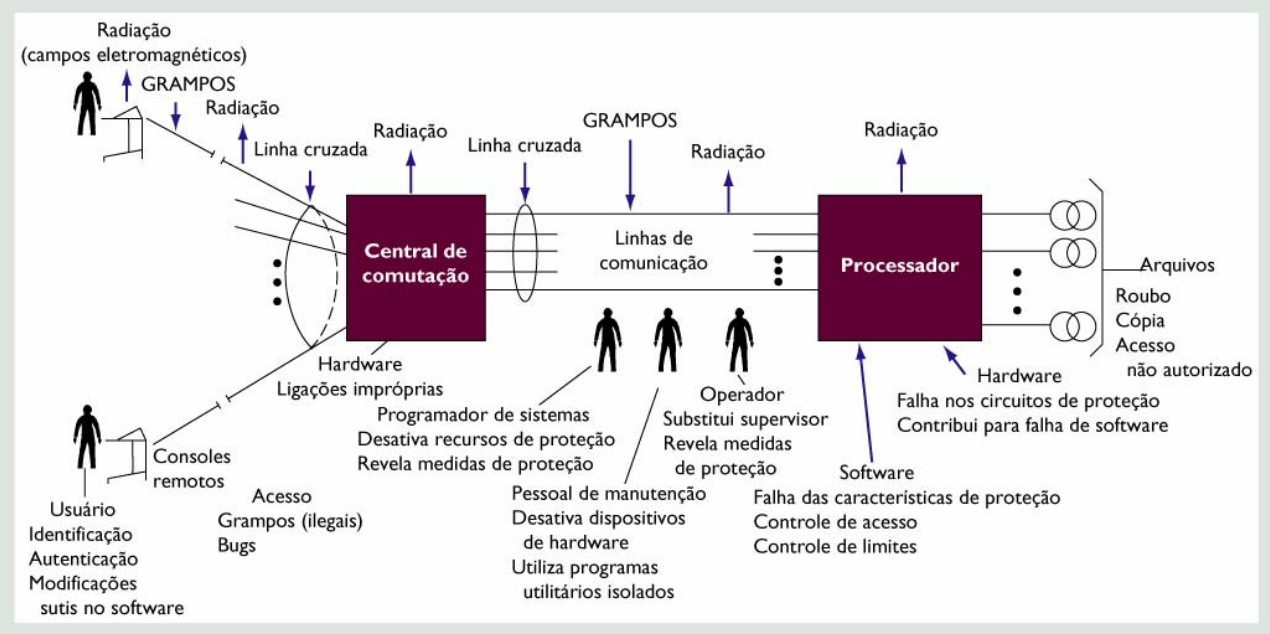
Quando grandes quantidades de dados são armazenadas sob formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual.

Os avanços nas telecomunicações e nos sistemas de informação ampliaram essas vulnerabilidades. Sistemas de informação em diferentes localidades podem ser interconectados por meio de redes de telecomunicações. Logo, o potencial para acesso não autorizado, abuso ou fraude não fica limitado a um único lugar, mas pode ocorrer em qualquer ponto de acesso à rede.

Além disso, arranjos mais complexos e diversos de hardware, software, pessoais e organizacionais são exigidos para redes de telecomunicação, criando novas áreas e oportunidades para invasão e manipulação. Redes sem fio que utilizam tecnologias baseadas em rádio são ainda mais vulneráveis à invasão, porque é fácil fazer a varredura das faixas de radiofreqüência. A Internet apresenta problemas especiais porque foi projetada para ser acessada

[4] (Laudon e Laudon, 2004)

facilmente por pessoas com sistemas de informações diferentes. As vulnerabilidades das redes de telecomunicação estão ilustradas na próxima figura.



Redes de telecomunicação são altamente vulneráveis a falhas naturais de hardware e software e ao uso indevido por programadores, operadores de computador, pessoal de manutenção e usuário finais. É possível por exemplo, grampear linhas de telecomunicação e interceptar dados ilegalmente. A transmissão de alta velocidade por canais de comunicação de par trançado, por sua vez, causa à interferência denominada linha cruzada. E, finalmente, a radiação também pode causar falha da rede em vários pontos.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

CAPÍTULO IV

Mecanismos para Controles de Segurança

Autenticação e autorização

A autorização é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acessos (*Acess Control Lists* – ACL), definindo quais atividades poderão ser realizadas, desta forma gerando os chamados perfis de acesso.

A autenticação é o meio para obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser. É um serviço essencial de segurança, pois uma autenticação confiável assegura o controle de acesso, determina que está autorizado a ter acesso à informação, permite trilhas de auditoria e assegura a legitimidade do acesso.

Atualmente os processos de autenticação estão baseados em três métodos distintos:

- **Identificação positiva (O que você sabe)** – Na qual o requerente demonstra conhecimento de alguma informação utilizada no processo de autenticação, por exemplo uma senha.

- **Identificação proprietária (O que você tem)** – Na qual o requerente demonstrar possuir algo a ser utilizado no processo de autenticação, como um cartão magnético.

- **Identificação Biométrica (O que você é)** – Na qual o requerente exibe alguma característica própria, tal como a sua impressão digital.

Combate a ataques e invasões

Destinados a suprir a infra-estrutura tecnológica com dispositivos de software e hardware de proteção, controle de acesso e conseqüentemente combate a ataques e invasões, esta família de mecanismos tem papel importante no modelo de gestão de segurança, à medida que as conexões eletrônicas e tentativas de acesso indevido crescem exponencialmente. Nesta categoria, existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados pra a segmentação de perímetros, identificação e tratamento de tentativas de ataque.

Firewall[5]

Um firewall é um sistema (ou grupo de sistemas) que reforçam a norma de segurança entre uma rede interna segura e uma rede não-confiável como a Internet. Os firewalls tendem a serem vistos como uma proteção entre a Internet e a rede privada. Mas em geral, um firewall deveria ser considerado como um meio de dividir o mundo em duas ou mais redes: uma ou mais redes seguras e uma ou mais redes não-seguras

Um firewall pode ser um PC, um roteador, um computador de tamanho intermediário, um mainframe, uma estação de trabalho UNIX ou a combinação destes que determine qual informação ou serviços podem ser acessados de fora e a quem é permitido usar a informação e os serviços de fora. Geralmente, um firewall é instalado no ponto onde a rede interne segura e a rede externa não-confiável se encontram, ponto que também é conhecido como ponto de estrangulamento.

A fim de entender como um firewall funciona, considere que a rede seja um edifício onde o acesso deva ser controlado. O edifício tem uma sala de

[5] (Laureano, 2002).

espera como o único ponto de entrada. Nesta sala de espera, as recepcionistas recebem os visitantes, os guardas de segurança observam os visitantes, as câmeras de vídeo gravam as ações de cada visitante e leitores de sinais autenticam os visitantes que entram no edifício.

Estes procedimentos devem funcionar bem para controlar o acesso ao edifício, contudo se uma pessoa não autorizada consegue entrar, não há meio de proteger o edifício contra as ações do intruso. Porém, se os movimentos do intruso são monitorados, é possível detectar qualquer atividade suspeita.

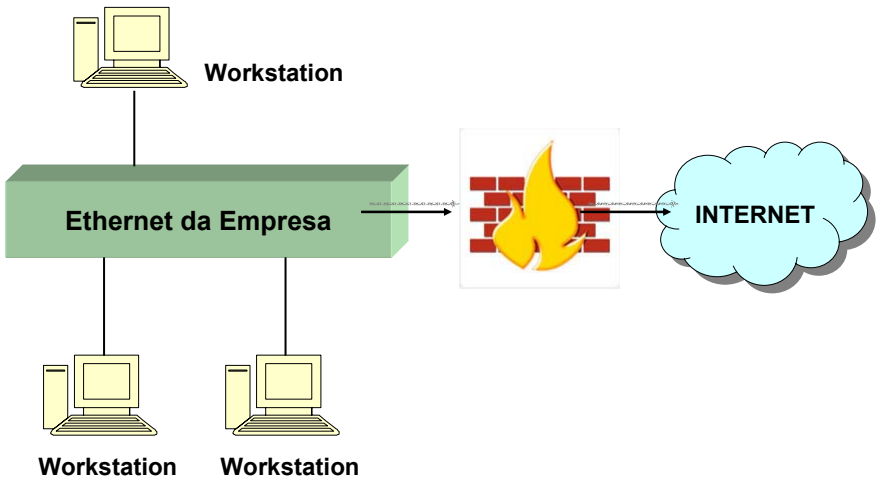
Um firewall é projetado para proteger as fontes de informação de uma organização, controlando o acesso entre a rede interna segura e a rede externa não-confiável. É importante notar que mesmo se o firewall tiver sido projetado para permitir que dados confiáveis passem, negar serviços vulneráveis e proteger a rede interna contra ataques externos, um ataque recém-criado pode penetrar o firewall a qualquer hora. O administrador da rede deve examinar regularmente os registros de eventos e alarmes gerados pelo firewall.

Os firewalls podem ser divididos em duas grandes classes: Filtros de pacote e servidores proxy;

Filtros de Pacotes – A filtragem de pacotes é um dos principais mecanismos que, mediante regras definidas pelo administrador em um firewall, permite ou não a passagem de datagramas IP em uma rede. Poderíamos filtrar pacotes para impedir o acesso a um serviço de Telnet, um chat ou mesmo um site na Internet.

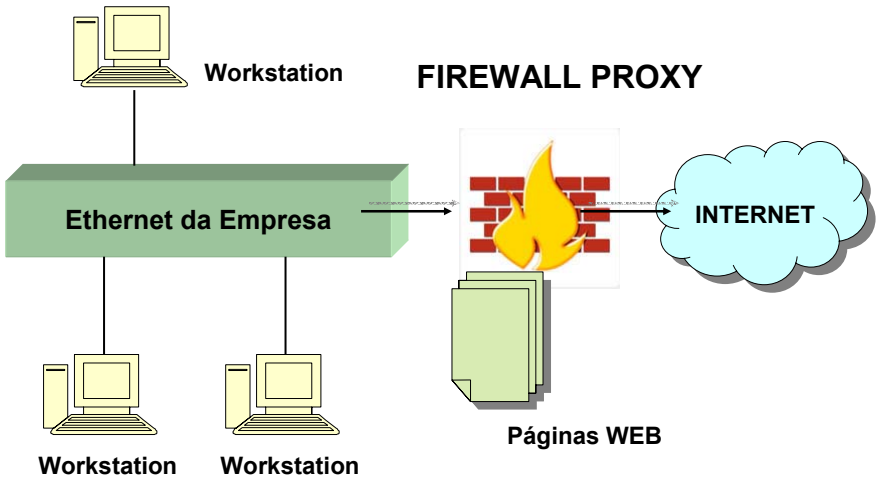
O modelo mais simples de firewall é conhecido como o *dual homed system*, ou seja, um sistema que interliga duas redes distintas. Este sistema possui um servidor com duas placas de rede que faz com que os usuários possam falar entre si. O exemplo clássico é um firewall entre uma Intranet e a Internet (próxima figura).

FIREWALL DUAL HOMED HOST



Servidores Proxy – Permite executar a conexão ou não a serviços em uma rede modo indireto. Normalmente os proxies são utilizados como caches de conexão para serviços Web. Um proxy é utilizado em muitos casos como elemento de aceleração de conexão em links lentos (veja a próxima figura).

INTRANET



Detector de Intrusos[6]

A maneira mais comum para descobrir intrusões é a utilização dos dados das auditorias gerados pelos sistemas operacionais e ordenados em ordem cronológica de acontecimento, sendo possível à inspeção manual destes registros, o que não é uma prática viável, pois estes arquivos de logs apresentam tamanhos consideráveis.

Nos últimos anos, a tecnologia de detecção de intrusão (*Intrusion Detection System* – IDS) tem se mostrado uma grande aliada dos administradores de segurança. Basicamente, o que tais sistemas fazem é tentar reconhecer um comportamento ou uma ação intrusiva, através da análise das informações disponíveis em um sistema de computação ou rede, para alertar um administrador e / ou automaticamente disparar contra-medidas. Para realizar a detecção, várias tecnologias estão sendo empregadas em produtos comerciais ou em projetos de pesquisas, as tecnologias utilizadas incluem análise estatística, inferência, inteligência artificial, data mining, redes neurais e diversas outras.

Um IDS automatiza a tarefa de analisar dados da auditoria. Estes dados são extremamente úteis, pois podem ser usados para estabelecer a culpabilidade do atacante e na maioria das vezes é o único modo de descobrir uma atividade sem autorização, detectar a extensão dos danos e prevenir tal ataque no futuro, tornando desta forma o IDS uma ferramenta extremamente valiosa para análises em tempo real e também após a ocorrência de um ataque.

Classificação de Detectores de Intrusão

O IDS tem como principal objetivo detectar se alguém está tentando entrar em um sistema ou se algum usuário legítimo está fazendo mau uso do mesmo. Esta ferramenta é executada constantemente em *background* e somente gera uma notificação quando detecta
alguma ocorrência que seja suspeita ou ilegal. Os sistemas em uso podem ser classificados com relação a sua forma de monitoração (origem dos dados) e aos mecanismos (algoritmos) de detecção utilizados.

Quanto à Origem dos Dados

Existem basicamente dois tipos de implementação de ferramentas IDS:

- ***Host Based IDS*** (HIDS) – são instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um servidor;
- ***Network Based IDS*** (NIDS) – são instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes de rede e seus detalhes como informações de cabeçalhos e protocolos.

Os sistemas NIDS podem monitorar diversos computadores simultaneamente. Todavia, sua eficácia diminui na medida em que o tamanho e

[6] (Laureano, 2004).

a velocidade da rede aumenta, pela necessidade de analisar os pacotes mais rapidamente. Além disso, o uso de protocolos cifrados (baseados em SSL – *Secure Socket Layer*) torna o conteúdo dos pacotes opaco ao IDS. A velocidade da rede e o uso de criptografia não são problemas para os sistemas HIDS. Todavia, como esse sistema é instalado na própria máquina a monitorar, pode ser desativado por um invasor bem-sucedido. Existem IDS que trabalham de forma híbrida, ou seja,combinando as duas técnicas citadas anteriormente.

Quanto à Forma de Detecção

Muitas ferramentas de IDS realizam suas operações a partir da análise de padrões do sistema operacional e da rede tais como: utilização de CPU, E/S de disco, uso de memória, atividades dos usuários, número de tentativas de login, número de conexões, volume de dados trafegando no segmento de rede entre outros. Estes dados formam uma base de informação sobre a utilização do sistema em vários momentos ao longo do dia. Algumas ferramentas possuem bases com padrões de ataque (assinaturas) previamente constituído, permitindo também a configuração das informações já existentes bem como inclusão de novos parâmetros. As técnicas usadas para detectar intrusões podem ser classificadas em:

- **Detecção por assinatura** – os dados coletados são comparados com uma base de registros de ataques conhecidos (assinaturas). Por exemplo, o sistema pode vasculhar os pacotes de rede procurando seqüências de bytes que caracterizem um ataque de *buffer overflow* contra o servidor WWW Apache;
- **Detecção por anomalia** – os dados coletados são comparados com registros históricos da atividade considerada normal do sistema. Desvios da normalidade são sinalizados como ameaças.
- **Detecção Híbrida** – o mecanismo de análise combina as duas abordagens anteriores, buscando detectar ataques conhecidos e comportamentos anormais.

A detecção por assinatura é a técnica mais empregada nos sistemas de produção atuais. Um exemplo de IDS baseado em assinatura é o SNORT. Os sistemas antivírus também adotam a detecção por assinatura. A detecção de intrusão por anomalia ainda é pouco usada em sistemas de produção.

Privacidade das Comunicações

Criptografia

A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia,escrita) e define a arte ou ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada comumente de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem.

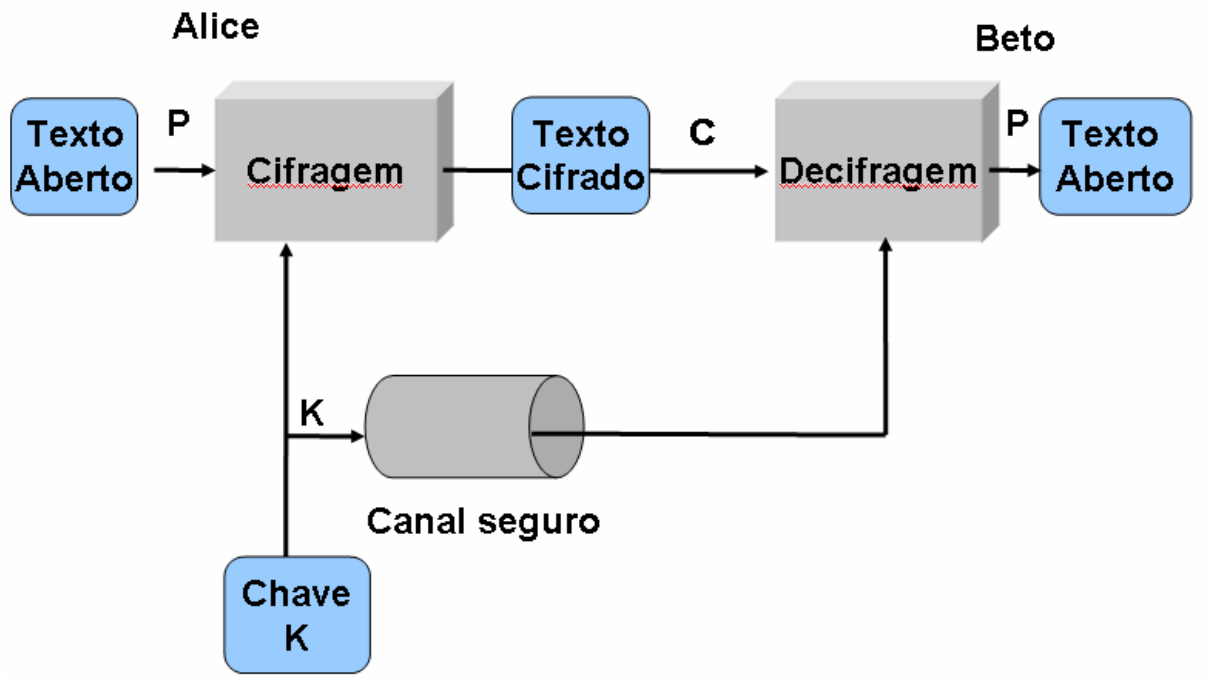
Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Criptografia é a ciência de escrever ocultamente e hoje, sem dúvida, é a maneira mais segura de se enviar informações através de um canal de comunicação inseguro como, por exemplo, a Internet.

A criptografia representa um conjunto de técnicas que são usadas para manter a informação segura. Estas técnicas consistem na utilização de chaves e algoritmos de criptografia. Tendo conhecimento da chave e do algoritmo usado é possível desembaralhar a mensagem recebida.

Simétrica ou de chave privada

Estes são os algoritmos convencionais de criptografia, onde a mesma chave secreta é utilizada tanto para cifrar como para decifrar uma mensagem, devendo ser conhecida por ambos os lados do processo. Este é o grande problema do método, pois a chave tem de ser entregue aos participantes de modo seguro, e as transações só podem ser realizadas depois disso.



O fato de ambos os lados conhecerem a chave também leva à possibilidade de repúdio da transação, pois um lado pode sempre alegar que o outro usou a chave e realizou a transação em seu nome, indevidamente.

Como cada par de participantes deve ter uma chave própria, o número de chaves necessárias para comunicação segura entre muitos participantes cresce combinatoriamente, com agravante adicional de que todas essas chaves são secretas e devem ser protegidas adequadamente. Ou seja, um participante do ciclo de criptografia deverá ter a chave de todos os outros para se comunicar com cada um deles. Isso inviabiliza o uso destes algoritmos isoladamente em certas aplicações.

Os algoritmos de chave simétrica são usados para cifrar a maioria dos dados ou fluxos de dados. Estes algoritmos são projetados para serem bem rápidos e (geralmente) terem um grande número de chaves possíveis. Os

melhores algoritmos de chave simétrica oferecem boa segurança quando os dados são cifrados com determinada chave, e dificilmente pode-se decifrar os dados sem possuir a mesma chave. Como a criptografia é sempre uma carga adicional ao processamento, esta vantagem é importante e deverá ser utilizada adequadamente.

Os algoritmos de chave simétrica podem ser divididos em duas categorias: de bloco e de fluxo:

2 **Algoritmos de Bloco** – Cifram os dados a partir de blocos, ou seja, se o dado a ser cifrado é um texto, esse texto será dividido em blocos e a criptografia será aplicada em cima de cada bloco. Um problema com essa cifragem é que se o mesmo bloco de texto simples aparecer em dois lugares, ele encriptará o mesmo texto, gerando assim, um padrão de repetição.

3 **Algoritmos de Fluxo** – Cifram os dados byte a byte. O dado a ser criptografado não é cifrado por blocos, como o anterior e sim, serialmente. A informação vai sendo criptografada do inicio ao fim, sem separações.

Há muitos algoritmos de chave simétrica em uso atualmente. Alguns dos algoritmos mais comuns no campo da segurança são:

- **DES** – o Padrão para Criptografia de Dados (*Data Encryption Standard*) foi adotado como padrão pelo governo dos EUA em 1977, e como padrão ANSI em 1981. O DES é um algoritmo de bloco que usa uma chave de 56 bits e tem diferentes modos de operação, dependendo da finalidade com que é usado. O DES é um algoritmo poderoso, mas o seu reinado no mercado começou a ruir em janeiro/1997, quando a empresa *RSA Data Security Inc*. (que detém a patente do sistema criptográfico RSA) - decidiu colocar o DES à prova, oferecendo um prêmio de US$ 10 mil à primeira pessoa ou instituição que decifrasse uma frase criptografada com o DES (vencido o primeiro desafio, a RSA decidiu repeti-lo a cada semestre, condicionando o pagamento do prêmio à quebra do recorde de tempo estabelecido até o momento). Atualmente uma máquina preparada para a tarefa é capaz de decifrar uma mensagem cifrada com o DES em poucas horas.
- **Triple DES** – É uma maneira de tornar o DES pelo menos duas vezes mais seguro, usando o algoritmo de criptografia três vezes, com três chaves diferentes. Usar o DES duas vezes com duas chaves diferentes não aumenta tanto a segurança quanto se poderia pensar devido a um tipo teórico de ataque conhecido como *meet-in-the-midle* (encontro no meio), com o qual o atacante tenta cifrar o texto limpo simultaneamente com uma operação do DES e decifrar o texto com outra operação, até que haja um encontro no meio. Atualmente, o Triple-DES está sendo usado por instituições financeiras com uma alternativa para o DES.
- **IDEA** – O *International Data Encryption Algorithm* (IDEA - Algoritmo de Criptografia de Dados Internacional) foi desenvolvido em Zurique, na Suíça, por James L. Massey e Xuenjia Lai, e publicado em 1990. O IDEA usa chave de 128 bits, e é bastante forte.
- **RC2** – Este algoritmo de bloco foi desenvolvido originalmente por Ronald Rivest, e mantido em segredo pela RSA Data Security. Foi revelado por

uma mensagem anônima na Usenet em 1996, e parece ser relativamente forte (embora algumas chaves sejam vulneráveis). O RC2 é vendido com uma implementação que permite a utilização de chaves de 1 a 2048 bits.

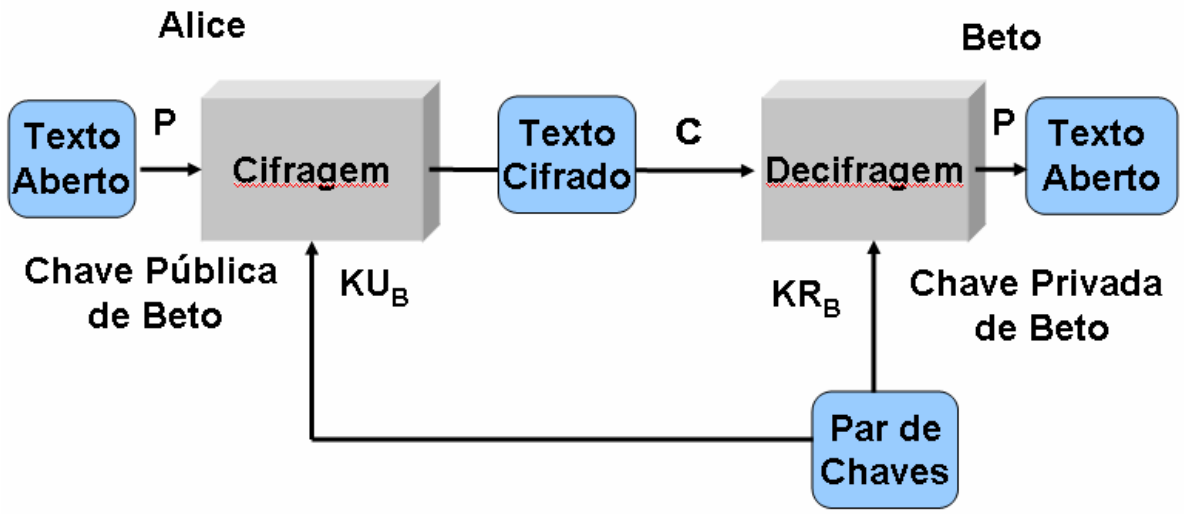
- **RC4** – Inventado em 1987 pela RSA, nunca teve o seu algoritmo de funcionamento interno publicado. Esse segredo possuía interesses financeiros e não de segurança. A empresa esperava que o mantendo em segredo, ninguém mais o implementaria e o comercializaria. É uma cifragem muito utilizada hoje em dia, até fazendo parte no protocolo de comunicação SSL (*Security Socket Layer*).
- **RC5** – Este algoritmo de bloco foi desenvolvido por Ronald Rivest e publicado em 1994. O RC5 permite que o tamanho da chave, o tamanho dos blocos de dados e o número de vezes que a criptografia será realizada seja definida pelo usuário.
- **Blowfish** – É um algoritmo de criptografia em bloco, rápido, compacto e simples, inventado por Bruce Schneier. O algoritmo permite a utilização de uma chave de tamanho variável, de até 448 bits, e é otimizado para executar em processadores de 32 ou 64 bits. Não é patenteado e foi colocado em domínio público.

Assimétrica ou de chave pública

A existência da criptografia de chave pública foi postulada pela primeira vez em meados de 1975 por Withfield Diffie e Martin Hellman. Os dois pesquisadores, na época na universidade de Stanford, escreveram um artigo em que pressuponham a existência de uma técnica criptográfica com a qual a informação criptografada com uma chave poderia ser decifrada por uma segunda chave, aparentemente sem relação com a primeira. Robert Merkle, então estudante em Berkeley que tinha idéias semelhantes mas, devido à lentidão do processo de publicação acadêmica, seus artigos só foram publicados quando a idéia de criptografia de chave pública já era bem conhecida.

Os algoritmos assimétricos utilizam-se de duas chaves diferentes, uma em cada extremidade do processo. As duas chaves são associadas através de um relacionamento matemático, pertencendo a apenas um participante, que as utilizará para se comunicar com todos os outros de modo seguro.

Essas duas chaves são geradas de tal maneira que a partir de uma delas não é possível calcular a outra a um custo computacional viável, possibilitando a divulgação de uma delas, denominada chave pública, sem colocar em risco o segredo da outra, denominada chave secreta ou privada.



Os principais sistemas de chaves públicas atualmente em uso são:

- **Diffie-Hellman** – Um sistema para troca de chaves criptográficas entre partes. Na verdade, não é um método de criptografia ou decifragem, é um método para troca de chave secreta compartilhada por meio de um canal de comunicação público. Com efeito, as duas partes estabelecem certos valores numéricos comuns e cada uma delas cria uma chave. As transformações matemáticas das chaves são intercambiadas. Cada parte calcula então uma terceira chave (a chave de sessão) que não pode ser descoberta facilmente por um atacante que conheça os valores intercambiados.
- **ElGamal** – Batizado com o nome de seu criador, Taher ElGamal, é um sistema criptográfico de chave pública baseado no protocolo de troca de chaves de Diffie- Hellman. O ElGamal pode ser utilizado para criptografia e assinatura digital, de forma semelhante ao algoritmo RSA.
- **DSS** – O *Digital Signature Standard* (DSS - Padrão de Assinatura Digital) foi desenvolvido pela Agência Nacional de Segurança (NSA), e adotado como Padrão Federal de Processamento de Informação (FIPS) pelo Instituto Nacional de Padrões Tecnologia (NIST) dos EUA. O DSS é baseado no Algoritmo de Assinatura Digital - DSA (*Digital Signature Algorithm*) - que permite a utilização de qualquer tamanho de chave, embora no DSS FIPS só sejam permitidas chaves entre 512 e 1024 bits. O DSS só pode ser usado para a realização de assinaturas digitais, embora haja implementações do DSA para criptografia.
- **RSA** – RSA é um sistema criptográfico de chave pública conhecido, desenvolvido por Ronald Rivest, Adi Shamir e Leonard Adleman, então professores do MIT (Instituto de Tecnologia de Massachusets). O RSA utiliza criptografia em blocos e possui uma segurança muito forte, devido ao alto poder computacional necessário para se tentar quebrar uma chave RSA. Pode tanto ser usado para cifrar informações como para servir de base para um sistema de assinatura digital. As assinaturas digitais podem ser usadas para provar a autenticidade de informações digitais. A chave pode ser de qualquer tamanho, dependendo da implementação utilizada.

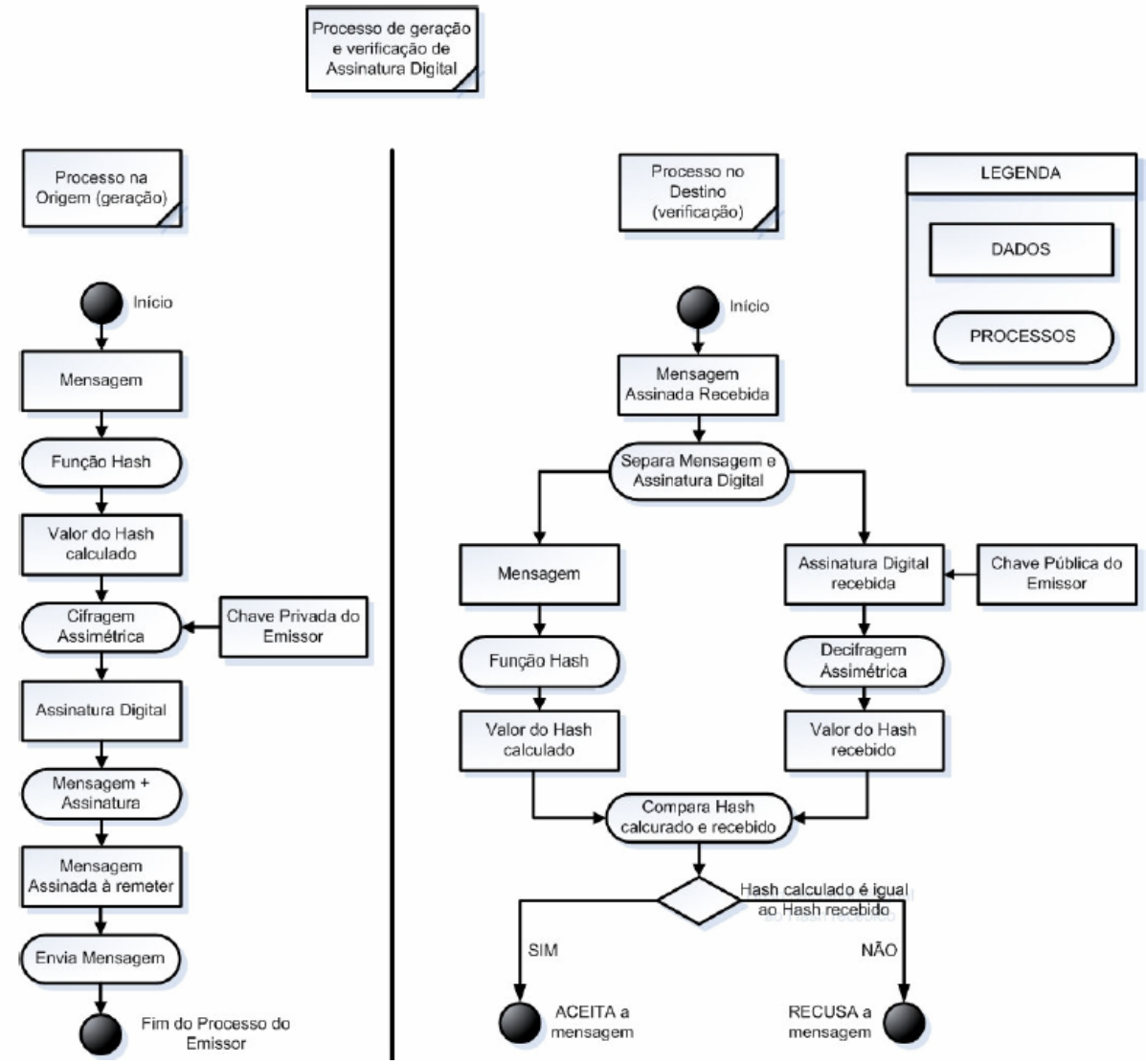
Assinatura Digital

Outra grande vantagem dos algoritmos assimétricos, particularmente o RSA, que é o mais conhecido e utilizado atualmente, é que o processo funciona também na criptografia no outro sentido, da chave secreta para a chave pública, o que possibilita implementar o que se denomina assinatura digital.

O conceito de assinatura é o de um processo que apenas o signatário possa realizar, garantindo dessa maneira sua participação pessoal no processo. Como a chave secreta é de posse e uso exclusivo de seu detentor, um processo de cifragem usando a chave privada do signatário se encaixa nesse conceito, permitindo, assim, a geração de uma assinatura por um processo digital.

No caso da assinatura digital, é inadequado cifrar toda a mensagem ou documento a ser assinado digitalmente devido ao tempo gasto na criptografia de um documento utilizando chaves assimétricas. A criptografia é aplicada apenas sobre um identificador unívoco do mesmo. Normalmente é utilizado como identificador o resultado da aplicação de uma função tipo HASH, que mapeia um documento digital de tamanho qualquer num conjunto de bits de tamanho fixo. Ao valor do HASH podem ainda ser anexados a data/hora, número de seqüência e outros dados identificadores, e este conjunto é então cifrado com a chave secreta do signatário constituindo a assinatura digital do documento. A função de HASH será explicada em seguida.

Qualquer participante pode verificar a autenticidade de uma assinatura digital, bastando decifrá-la com a chave pública do signatário, o qual todos podem ter acesso. Se o resultado é significativo, está garantido o uso da chave secreta correspondente na assinatura, e portanto sua autenticidade. Resta ainda comprovar a associação da assinatura ao documento, o que é feito recalculando o HASH do documento recebido e comparando-o com o valor incluído na assinatura. Se forem iguais, prova-se ainda a ligação com o documento, assim como a integridade (não alteração) do mesmo. Uma vez que a verificação é realizada utilizando a chave pública, sua validação pode ser realizada por terceiros, tais como árbitros e auditores.



Virtual Private Network [7]

A idéia de utilizar uma rede pública como a Internet em vez de linhas privativas para implementar redes corporativas é denominada de *Virtual Private Network* (VPN) ou Rede Privada Virtual. As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

Outro serviço oferecido pelas VPNs é a conexão entre corporações

[7] Retirado de (Chin, 1998).

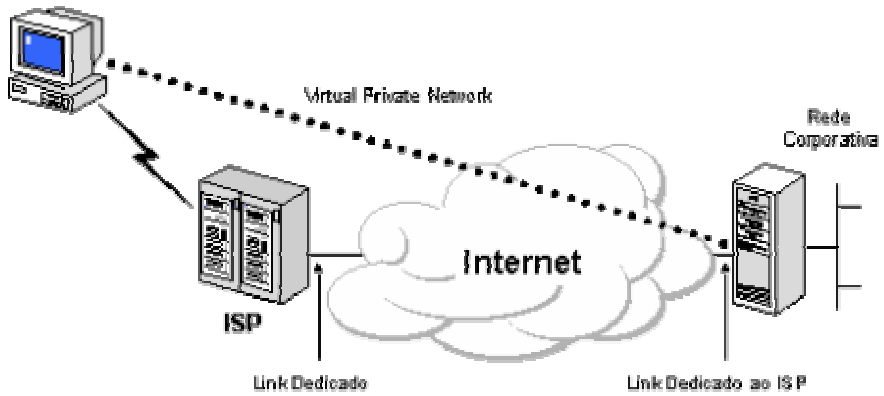
(Extranets) através da Internet, além de possibilitar conexões *dial-up* criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

Uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois elimina a necessidade de links dedicados de longa distância que podem ser substituídos pela Internet. As LANs podem, através de links dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet. Esta solução pode ser bastante interessante sob o ponto de vista econômico, sobretudo nos casos em que enlaces internacionais ou nacionais de longa distância estão envolvidos. Outro fator que simplifica a operacionalização da WAN é que a conexão LAN-Internet-LAN fica parcialmente a cargo dos provedores de acesso.

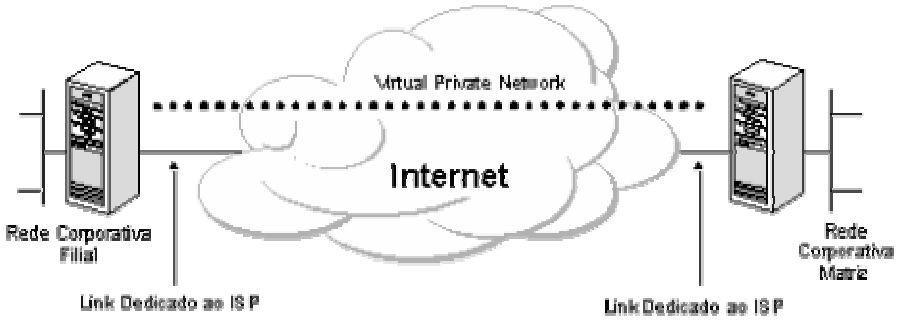
Aplicações para redes privadas virtuais

Abaixo, são apresentadas as três aplicações ditas mais importantes para as VPNs.

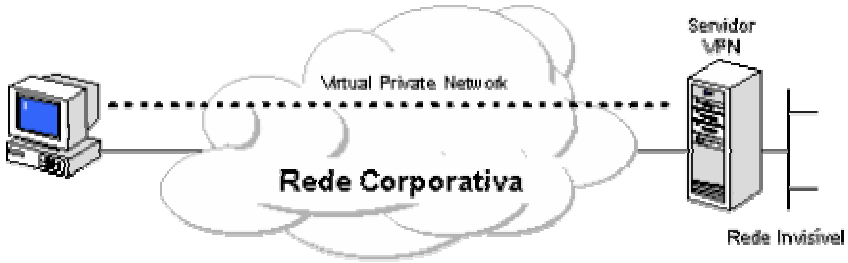
- **Acesso Remoto via Internet** – O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da ligação local a algum provedor de acesso (Internet Service Provider - ISP). A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.



- **Conexão de Lans via Internet** – Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O software de VPN assegura esta interconexão formando a WAN corporativa.
  A depender das aplicações também, pode-se optar pela utilização de circuitos discados em uma das pontas, devendo a LAN corporativa estar, preferencialmente, conectada à Internet via circuito dedicado local ficando disponível 24 horas por dia para eventuais tráfegos provenientes da VPN.



- **Conexão de Computadores numa Intranet** – Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa. Esta solução, apesar de garantir a "confidencialidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.
  As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa uma vez que o roteador possibilitaria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensitiva. Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita. Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a "confidencialidade" das informações. Os demais usuários não credenciados sequer enxergarão a rede departamental.



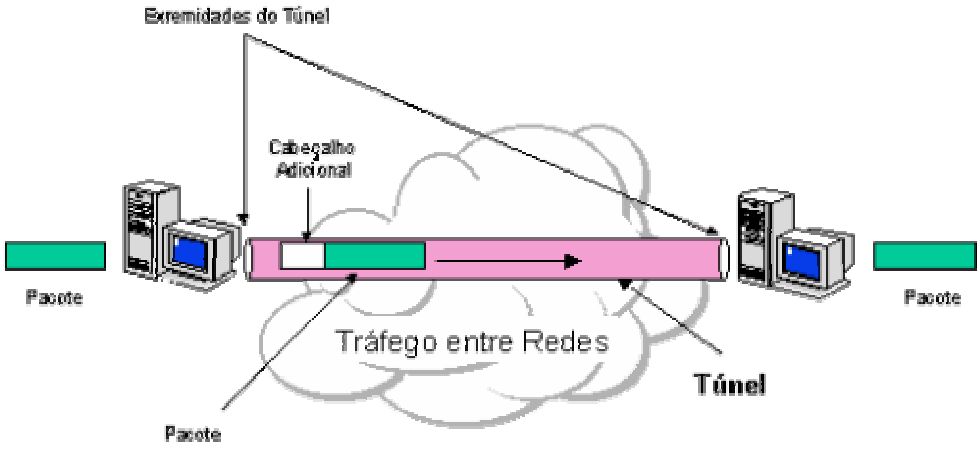
Tunelamento

As redes virtuais privadas baseiam-se na tecnologia de tunelamento cuja existência é anterior as VPNs. Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e

decriptografado, retornando ao seu formato original. Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

O protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária. Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final. A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada.

Note que o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote.



Requisitos básicos que a VPN atende

No desenvolvimento de soluções de rede, é bastante desejável que sejam implementadas facilidades de controle de acesso a informações e a recursos corporativos. A VPN deve dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos da LAN corporativa, viabilizar a interconexão de LANs de forma a possibilitar o acesso de filiais, compartilhando recursos e informações e, finalmente, assegurar privacidade e integridade de dados ao atravessar a Internet bem como a própria rede corporativa. A seguir são enumeradas características mínimas desejáveis numa VPN:

- **Autenticação de Usuários** – Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados - quem acessou, o quê e quando foi acessado.
- **Gerenciamento de Endereço** – O endereço do cliente na sua rede privada

não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo.

- **Criptografia de Dados** – Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.
- **Gerenciamento de Chaves** – O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.
- **Suporte a Múltiplos Protocolos** – Com a diversidade de protocolos existentes, torna-se bastante desejável que uma VPN suporte protocolos padrão de fato usadas nas redes públicas, tais como IP (*Internet Protocol*), IPX (*Internetwork Packet Exchange*), etc.

Public Key Infrastructure

Uma Infra-estrutura de Chaves Públicas (ICP) é um sistema de segurança baseado em tecnologia para estabelecer e garantir a confiabilidade de chaves públicas de criptografia. A criptografia de chaves públicas tem se apresentado como um importante mecanismo de segurança para o fornecimento de serviços de autenticação, geração de provas, integridade de dados e confidencialidade para operações internas e externas de *e-business*. Quando implementada como um componente integral de uma solução de habilitação de confiabilidade, uma ICP pode contribuir para a otimização da velocidade e do valor das transações de *e-business*.

A infra-estrutura de chaves públicas atrela as chaves públicas às suas entidades, possibilitando que outras entidades verifiquem a validade das chaves públicas e disponibilize os serviços necessários para o gerenciamento das chaves que trafegam em um sistema distribuído.

O objetivo maior dessa arquitetura de segurança moderna é proteger e distribuir a informação que é necessária em ambientes altamente distribuídos, nos quais os usuários, recursos e empresas podem estar em lugares diferentes.

Em transações comerciais convencionais, por exemplo, os clientes e os comerciantes baseiam-se em cartões de créditos (p.ex., VISA ou Mastercard) para completar os aspectos financeiros das transações. O vendedor autentica o cliente através da comparação de assinaturas ou verificando um documento de identidade, como um RG. O vendedor se baseia na informação contida no cartão de crédito e na informação obtida junto ao emissor do cartão de crédito para garantir que o pagamento será recebido. Da mesma forma, o cliente faz a transação sabendo que ele pode rejeitar a conta se o vendedor falhar no fornecimento do bem ou serviço. O emissor do cartão de crédito é o terceiro confiável nesse tipo de transação.

O mesmo modelo pode ser aplicado em uma transferência de informação (como um cadastro de pessoa física), mesmo sabendo que o consumidor e o vendedor talvez nunca se encontrem. O vendedor não pode

comparar as assinaturas ou pedir um documento de identidade. Eles podem estar separados por centenas de quilômetros. Mas ambos precisam ser capazes de assegurar que a outra parte é legítima para que haja a troca de informações.

A infra-estrutura de chave pública é uma combinação de software, tecnologias de encriptação e serviços que permite às empresas obterem segurança em suas comunicações e transações comerciais via rede, integrando certificados digitais, criptografia de chave pública e autoridades certificadoras numa arquitetura de segurança de redes completa para, dessa forma, criar uma estrutura de confiança para os dois lados da transação.

A ICP consegue assegurar confidencialidade, integridade e não-repúdio de uma maneira difícil de ser fraudada e que se apresenta de forma transparente para o usuário. Estes dois pontos, transparência aliada à forte base técnica de seus mecanismos, denotam o aspecto forte desta tecnologia.

Esteganografia[8]

Do grego "escrita coberta". Ramo particular da criptologia que consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença. Ao contrário da criptografia, que procura esconder a informação da mensagem, a esteganografia procura esconder a EXISTÊNCIA da mensagem.

Contrariamente à criptografia, que cifra as mensagens de modo a torná-las incompreensíveis, a esteganografia esconde as mensagens através de artifícios, por exemplo imagens ou um texto que tenha sentido mas que sirva apenas de suporte (como o alfabeto biliteral de Francis Bacon ou as famosas cartas de George Sand). A idéia é a mesma das grelhas de Cardano e o "*barn code*": mesclar a mensagem numa outra e onde apenas determinadas palavras devem ser lidas para descobrir o texto camuflado.

O primeiro uso confirmado da esteganografia está em "As Histórias" de Heródoto e remonta ao século V a.C.: um certo Histio, querendo fazer contato secreto com seu superior, o tirano Aristágoras de Mileto, escolheu um escravo fiel, raspou sua cabeça e escreveu na pele a mensagem que queria enviar. Esperou que os cabelos crescessem e mandou o escravo ao encontro de Aristágoras com a instrução de que deveriam raspar seus cabelos.

Ainda nas "As Histórias" de Heródoto, consta que, para informar os espartanos de um ataque iminente dos persas, o rei Demaratos utilizou um estratagema muito elegante: pegou tabletes, retirou-lhes a cera, gravou na madeira a mensagem secreta e recobriu-os novamente com cera. Deste modo, os tabletes, aparentemente virgens, não chamaram a atenção. O problema era que os gregos não sabiam do que se tratava quando Gorgo, mulher de Leônidas, teve a idéia de raspar a cera.

Na China antiga, escrevia-se mensagens sobre seda fina. Depois se

[8] Retirado de http://www.numaboa.com.br/criptologia/stegano/index.php em 16/10/2004.

fazia uma bolinha que era envolvida por cera. Em seguida, o mensageiro engolia a bolinha.

No século XVI, o cientista italiano Giovanni Porta descobriu como esconder uma mensagem num ovo cozido: escrever sobre a casca com uma tinta contendo uma onça de alume (± 29 g) diluído em cerca de meio litro de vinagre. A solução penetra a casca e se deposita sobre a superfície branca do ovo. Depois, basta abrir o ovo para ler a mensagem.

O historiador da Grécia antiga, Enéias, o Tático, tem a idéia de enviar uma mensagem secreta fazendo minúsculos furos em certas letras de um texto qualquer. A sucessão destas letras marcadas fornecia o texto secreto. Dois mil anos mais tarde, remetentes ingleses empregaram o mesmo método, não para garantir o segredo de suas cartas, mas para evitar o pagamento de taxas muito caras. Na realidade, antes da reforma do serviço postal ao redor de 1850, enviar uma carta custava cerca de um *shilling* para cada cem milhas de distância. Os jornais, no entanto, eram isentos de taxas. Graças a furinhos de agulha, os ingleses espertos enviavam suas mensagens gratuitamente. Este procedimento foi até utilizado pelos alemães durante a Primeira Guerra Mundial. Durante a Segunda Guerra, eles aperfeiçoaram o método marcando letras de jornais com tintas "invisíveis".

Os espiões alemães da Segunda Guerra utilizavam micropontos para fazer com que suas mensagens viajassem discretamente. Eram fotografias do tamanho de um ponto (.) que depois eram ampliadas para que a mensagem aparecesse claramente. Era uma espécie de microfilme colocado numa letra, num timbre, etc.

Em 1999, Catherine Taylor Clelland, Viviana Risca e Carter Bancroft publicaram na revista Nature o artigo "*Hiding messages in DNA microdots*" (escondendo mensagens em micropontos de DNA). Na verdade, qualquer material genético é formado por cadeias de quatro nucleotídeos (Adenina, Citosina, Guanina e Timina) que podemos comparar a um alfabeto de quatro letras: A, C, G e T. Além disso, os cientistas atualmente são capazes de fabricar cadeias de DNA com um conjunto predeterminado de nucleotídeos. Nada impede de atribuir a um grupo de três nucleotídeos uma letra do alfabeto, um número ou sinais de pontuação (por exemplo, "A"=CGA, "B"=CCA, etc) e compor uma "mensagem genética". Para disfarçar as pistas, poder-se-ia misturar algumas outras seqüências aleatórias de nucleotídeos. O resultado é apenas visível ao microscópio eletrônico. Como possível aplicação, pode-se imaginar que uma empresa que produza uma nova espécie de tomate poderá incluir sua marca de fábrica nas moléculas do tomate a fim de evitar as imitações.

Exemplo: Segurança Monetária Suiça

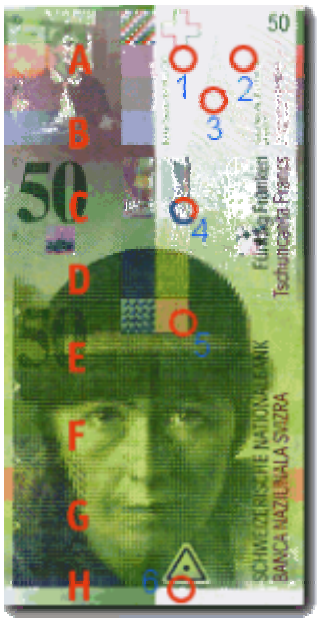
Para quem estiver pensando que a esteganografia é obsoleta ou apenas uma brincadeira de criança, um alerta: a idade ou a simplicidade dos métodos não invalidam sua aplicação.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005

No mundo financeiro, a Suiça sempre teve um papel de destaque. Conhecida pela descrição (para não dizer segredo) e pela segurança que oferece a investidores, a moeda corrente suiça não poderia ser uma exceção - precisa também oferecer um alto grau de segurança quanto à sua autenticidade. Analisando o papel moeda em detalhes, o que mais chama a atenção são os métodos esteganográficos utilizados nos dias de hoje.

A série atual de notas foi emitida pelo Banco Nacional Suiço - BNS entre 1995 e 1998. Abaixo está a série completa que esconde uma porção de "truques" esteganográficos:

Todas as notas desta série possuem diversos elementos de segurança. Tomando a nota de 50 francos como exemplo, destacam-se diversas tecnologias utilizadas tanto na frente como no verso da nota. Conheça os elementos da frente da nota, cujos pontos de aplicação estão destacados em vermelho. Cada nota é uma verdadeira "biblioteca esteganográfica", aplicando alta tecnologia em métodos conhecidos de longa data:



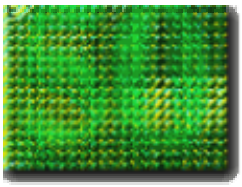
- 12A: As cifras com a tinta Iriodin®: O número mágico.
- 13B: As cifras em marca d'água
- 14C: As cifras em talhe doce: O número que tinge
- 15D: O número perfurado (microperf ®)
- 16E: A tinta com efeito óptico variável: O número camaleão
- 17F: As cifras com ultravioleta
- 18G: As cifras metalizadas: O número cintilante
- 19H: O efeito basculante
- 201: Frente e verso
- 212: Marca d'água do rosto
- 223: Guillochis
- 234: Kinegram®: A cifra dançante
- 245: Microtexto
- 256: Símbolo para deficientes visuais

As cifras com a tinta Iriodin®: O número mágico. O valor da nota é impresso no local indicado com A com uma tinta transparente e ligeiramente brilhante que se torna particularmente visível quando a luz estiver num ângulo preciso.

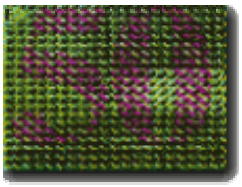
As cifras em marca d'água. A indicação do valor da nota fica incrustada no papel sob a forma de marca d'água. Posicionando a nota contra a luz e observando detalhadamente, é possível distinguir, sob a tinta de impressão, a marca d'água indicando o valor da mesma.

As cifras em talhe doce: O número que tinge. A indicação do valor da nota, impresso em talhe doce, aparece em relevo e se revela rugoso ao tato. Ao ser esfregado, por exemplo num papel branco, deixa traços da tinta de impressão bem visíveis.

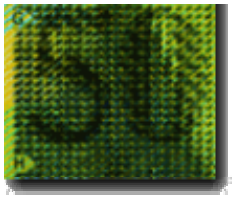
O número perfurado (microperf ®). A cifra indicando o valor é inscrita através de perfurações muito finas, denominadas microperf ®. Estas perfurações não são visíveis, a não ser que se observe a nota contra uma fonte luminosa.



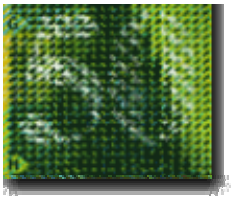
A tinta com efeito óptico variável: O número camaleão. A indicação do valor da nota é impresso no local indicado com E com uma tinta que muda de cor quando recebe luz de diferentes ângulos. Inclinando a nota lentamente para frente e para trás é possível observar como a cor dos números se modificam.

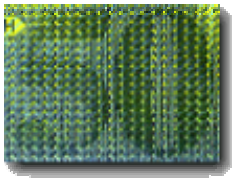


As cifras com ultravioleta. Sob luz ultravioleta, a metade esquerda da nota mostra o valor em tom escuro e o rosto claro e fluorescente. A metade direita mostra o valor da nota em tom claro e fluorescente e o rosto em tom escuro.



As cifras metalizadas: O número cintilante. As cifras indicando o valor da nota são metalizadas. Movimentando a nota como se fosse uma página de livro, as cifras cintilam numa cor prateada. Com o auxílio de uma lupa também é possível reconhecer os monogramas SNB e BNS do Banco Nacional Suiço entre as cifras metalizadas. O número cintilante está parcialmente recoberto pela tinta de impressão.

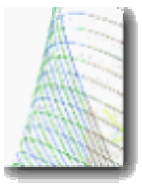




O efeito basculante. A indicação do valor da nota impressa no local identificado por H só pode ser vista de um ângulo pouco habitual. Com a nota posicionada horizontalmente, na altura dos olhos e com um discretíssimo ângulo de inclinação, pode-se ler o valor da mesma.

Frente e verso. Duas cruzes são impressas, uma em cada face da nota, exatamente na mesma posição. Uma é ligeiramente maior que a outra. Pode-se ver, por transparência, uma cruz suiça entre as duas silhuetas.

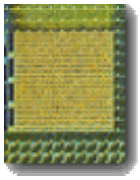
Marca d'água do rosto. A porção superior direita da frente da nota é ocupada pelo rosto em marca d'água. A direção do olhar é idêntico ao do rosto impresso.



Guillochis. A fina estrutura das curvas entrelaçadas pode modificar discretamente sua cor de linha para linha ou ao longo de cada linha.

Kinegram®: A cifra dançante. No centro da nota fica o Kinegram®: o valor da nota, mostrado em lâminas prateadas especiais, parece se mover.
Dois outros Kinegram® menores mostram a cruz suiça e os monogramas do Banco Nacional Suiço: SNB e BNS.

A forma do Kinegram®, a posição dos dois menores e o movimento dos números são diferentes de acordo com o valor da nota.



Microtexto. Nas duas faces da nota um texto curto sobre a pessoa retratada é reproduzido numa impressão tão miniaturizada que, só com o auxílio de uma poderosa lente de aumento, é possível lê-lo.

O exemplo aqui reproduzido corresponde ao texto encontrado na frente da nota de 50 francos.

Símbolo para deficientes visuais. Um símbolo, perceptível ao tato e diferente para cada valor, está gravado em relevo na porção inferior da frente de cada nota para possibilitar o reconhecimento da mesma pelos cegos e deficientes visuais.

Processos de Segurança

Service Level Agreement ou Acordo de Nível de Serviço

A área de tecnologia da informação (TI) vem adotando ao longo dos anos a estratégia de contratação de serviços terceirizados, também conhecida como "*body shop*". Nesta relação o importante é a questão da qualidade dos serviços prestados, bem como a segurança associada, uma vez que o trabalho com profissionais terceirizados traz também seus riscos.

A questão da qualidade dos serviços prestados passa a ser fundamental, e é justamente aí que entra o SLA (abreviação do termo *Service Level Agreement*) ou simplesmente Acordo de Nível de Serviço.

Os Acordos de Nível de Serviço são acordos formais entre fornecedores de serviço e clientes (internos e externos), pelos quais se definem, conjuntamente, condições, responsabilidades e níveis de desempenho para os serviços a serem executados.

Os SLAs podem ser definidos não apenas para serviços relacionados à tecnologia, mas também para serviços operacionais necessários ao funcionamento do negócio, como, por exemplo, o fornecimento de energia elétrica durante uma partida noturna de futebol.

É muito comum que os SLAs ocorram, nos relacionamentos da áreas de Tecnologia da Informação (TI), que tem suas métricas e controles mais claramente definidos.

Estes são alguns pontos que um SLA deve compreender:

- **Objetivos e escopo de acordo** – Neste ponto, deve-se providenciar um resumo de alto nível dos objetivos que os serviços devem alcançar. Estará sendo definido, aqui, o que se quer com o acordo, se ele garantirá qualidade, bom desempenho ou custos ou mesmo todos. Serão relacionadas todas as entidades envolvidas no acordo.

- **Políticas do acordo** – Este item contém a descrição das políticas e práticas adotadas pelo fornecedor e das políticas e práticas requeridas pelo cliente para alcançar seus objetivos de negócio.

- **Atualização do SLA** – Este item indica como serão as mudanças e atualizações no SLA. Como o SLA ocorre por meio da cooperação entre os fornecedores e a instituição, as mudanças devem ser aprovadas por ambas as partes, sempre avaliando em que proporção à instituição será afetado por elas.

- **Responsabilidades** – Serão definidos aqui os papéis existentes dentro do acordo, com indicação do que cada parte deverá realizar.
  Os principais papéis são:
  - Patrocinadores do fornecedor e da instituição, que definirão os recursos envolvidos no acordo e tratarão das decisões macro.
  - Representantes da instituição e dos fornecedores: geralmente são as funções diretamente envolvidas no relacionamento operacional, do dia-a-dia do acordo. Realizam ações para atingir metas e cumprir os pré-requisitos.
  - Comitê de Aprovação Técnica: envolve os responsáveis pelos serviços do cliente e do fornecedor para discutir a viabilidade técnica das solicitações.
  - Comitê de Aprovação do Acordo: envolve os representantes de ambos as partes e os patrocinadores, para discutir os valores e as condições para cumprir o acordo, bem como para sanar divergências. Este comitê avalia o impacto sobre o cliente final da

instituição sobre cada decisão técnica adotada.

- **Inventário dos serviços e atividades** – Este item apresenta uma relação sucinta dos serviços e das atividades realizadas pelo fornecedor e que serão abrangidas pelo acordo de nível de serviços. A data do inventário e o nome do responsável pelo serviço são informações importantes a serem registradas.
- **Gerenciamento de segurança e problemas** – Especificamente, o item define as cláusulas de segurança e os responsáveis pela administração da segurança e de problemas para cada serviço e para o acordo de forma geral. Normalmente, os fornecedores são responsáveis por implementar procedimentos de segurança e de gerência de problemas definidos pelo cliente.
- **Determinação de níveis de severidade, prioridade, objetivos e valores** – Deverão ser adotados critérios para definir os níveis de severidade dos problemas, distintos para cada serviço e para cada categoria de usuários dos serviços. O nível de severidade permitirá definir as prioridades de cada um dos serviços a ser prestado. Deverão ser definidos objetivos e valores a serem atingidos com a prestação dos serviços.
- **Penalidades e benefícios por nível de serviço** – Podem ser definidos como uma porcentagem da quantitativa e qualitativa dos serviços a serem prestados.
- **Medições de desempenho** – A medição garante que o SLA seja monitorado de modo que alcance os padrões de desempenho definidos.

Se você ainda não possui um SLA, procure o seu fornecedor e busque uma solução em conjunto para a criação deste documento, que é uma excelente maneira de se garantir a qualidade do serviço prestado e aumentar o nível de segurança da sua empresa.

Outros processos de Segurança

A segurança é composto de outras atividades, tais como:

- Análise e Gerência de Riscos
- Planos de Continuidade
- Estratégias de Contingência
- Políticas de Segurança
- Auditorias
- Legislação
- Outros

Estes itens serão estudados mais profundamente nos próximos capítulos.

CAPÍTULO V

Algumas Leis da Segurança

Leis Fundamentais

São 10 as leis fundamentais da segurança da informação (Ahmad e Russel, 2002). Todas as vezes que for necessário participar de um novo projeto de software ou infra-estrutura em sua empresa, se preocupe em respeitar as leis abaixo:

1. Segurança do lado do Cliente não funciona

- Segurança do lado do cliente é segurança implementada unicamente no cliente;
- O usuário sempre tem a oportunidade de quebrar a segurança, pois ele está no controle da máquina;
- A segurança no lado do cliente não fornecerá segurança se tempo e recursos estiverem disponíveis ao atacante.

2. Você não pode trocar chaves de criptografia com segurança sem uma informação compartilhada.

- As informações compartilhadas são usadas para validar máquinas antes da criação da sessão;
- Você pode trocar chaves privadas compartilhadas ou usar SSL (*Secure Socket Layer*) através do seu navegador;
- As trocas de chaves são vulneráveis a ataques do tipo *man-in-the-middle* (homem no meio).

3. Não existe proteção total contra código malicioso.

- Os produtos de software não são perfeitos;
- Os programas de detecção de vírus e cavalo de tróia se baseiam em arquivos de assinatura;
- Pequenas mudanças na assinatura de código podem produzir uma variação não detectável (até que a nova assinatura seja publicada).

4. Qualquer código malicioso pode ser completamente modificado para evitar detecção de assinatura.

- Os atacantes podem mudar a identidade ou assinatura de um arquivo rapidamente;
- Os atacantes podem usar compactação, criptografia e senhas para mudar a aparência do código;
- Você não tem como se proteger contra cada modificação possível.

5. Os firewalls não podem protegê-lo cem por cento contra ataques.

- Os firewalls podem ser software ou hardware, ou ambos;
- A principal função de um firewall é filtrar pacotes que chegam e

saem;
- Ataques sucessivos são possíveis como resultado de regras e políticas incorretas, e de problemas de manutenção.

6. Qualquer IDS pode ser burlado.
- Os sistemas de detecção de intrusão (IDS) freqüentemente são projetos passivos;
- É difícil para um atacante detectar a presença de um IDS quando está sondando;
- Um IDS está sujeito à configuração incorreta e falta de manutenção. Essas condições podem criar oportunidades de ataque.

7. Algoritmos criptográficos secretos não são seguros.
- Criptografia é difícil;
- A maioria da criptografia não é revisada e testada o bastante antes de ser lançada;
- Algoritmos comuns estão em uso em diversas áreas. Eles são difíceis, mas não impossíveis de atacar.

8. Se uma chave não for necessária, você não tem criptografia – você tem codificação.
- Esta lei é universal; não há exceções;
- A criptografia é usada para proteger a codificação. Se não existe uma chave, você não pode criptografar;
- As chaves precisam ser mantidas em segredo ou não existe segurança;
- As senhas não podem ser armazenadas com segurança no cliente a menos que haja outra senha para protegê-las;
- É fácil detectar informações de senha armazenadas em máquinas clientes;
- Se uma senha não é criptografada ou não está protegida quando armazenada, ele não é segura;
- A segurança de senha em máquinas clientes requer um segundo mecanismo para fornecer segurança.

9. Para que um sistema comece a ser considerado seguro, ele precisa submeter-se a uma auditoria de segurança independente.
- A auditoria é o começo de uma boa análise de sistemas de segurança;
- Os sistemas de segurança, muitas vezes, não são revisados correta ou completamente, permitindo furos;
- Verificação externa é vital para a defesa; a falta dela é um convite a ataques.

10. Segurança através de obscuridade não funciona.
- Ocultar não é proteger;
- É necessária proteção ativa;
- O uso da obscuridade por si só convida ao comprometimento.

As 10 Leis Imutáveis da Segurança

Segundo Scott Culp, gerente central de resposta de segurança da Microsoft, são 10 as leis da segurança (Culp,2004):

Primeira: Se um malfeitor consegue te persuadir a executar um programa no seu computador, este computador deixa de ser seu.

- O conselho de - jamais executar arquivos de estranhos - merece, justamente, o primeiro lugar nessa lista. Este é o principal problema enfrentado por usuários com excesso de confiança. Pessoas más podem facilmente tomar o controle do seu computador se te convencerem a executar os seus (deles) programas. Software como cavalos-de-Tróia fazem parte desta lei.

Segunda: Se um malfeitor consegue alterar o sistema operacional do seu computador, este computador deixa de ser seu.

- Programas executam comandos que são interpretados pelo sistema operacional do computador. Se um programa pode prejudicar seu funcionamento, imagine o que uma alteração no próprio sistema operacional pode fazer.

Terceira: Se um malfeitor tiver acesso físico irrestrito ao seu computador, este computador deixa de ser seu.

- Nenhum sistema lógico de segurança é suficientemente bom para proteger um computador se esse estiver acessível fisicamente.
- Entre os milhares de ameaças que surgem neste cenário, estão as simples - como jogar o computador pela janela - e as mais complexas - como abrir o equipamento, conectar dispositivos que façam cópias das informações que trafegam pelo computador para transferi-las para lugares remotos.

Quarta: Se você permitir que um malfeitor envie programas para seu website, este website deixa de ser seu.

- Assim como seu computador possui um sistema e programas que fazem suas tarefas diárias - como as planilhas, editores etc. – um webserver possui um sistema operacional e programas que respondem pela tarefa de "servir" páginas na internet.
- Se você permitir que um visitante instrua este computador a executar seus comandos, estará sob a mesma vulnerabilidade da primeira lei. Estes comandos isolados ou até mesmo um programa completo poderão ser transmitidos e executados pelo computador, submetendo-o à vontade do invasor.

Quinta: Senhas fracas triunfam sobre a mais forte segurança.

- Uma senha é, por definição, secreta. Entretanto, muitos usuários as compartilham com colegas ou as entregam a estranhos. Ela serve para dizer se você é quem diz ser. Deixar alguém usar sua senha é

como permitir que assumam sua identidade. Qualquer ação tomada sob essa identificação, será de sua responsabilidade.

- Isso sem falar nos que nem mesmo têm uma senha! É alarmante o número de contas, inclusive administrativas, que não possuem senha ou que a senha é igual ao login. Claro que a maioria cai no erro de senhas óbvias, nomes, datas de aniversário, marca do monitor (!) etc.

Sexta: Um sistema é tão seguro quanto seu administrador é confiável.

- Políticas de acesso restrito a serviços ou arquivos são peças-chave para se manter um mínimo de segurança nos sistemas. Mas quem diz quais arquivos ou serviços devem ou não ser acessados? Certo, o administrador.
- Ele possui controle total sobre o sistema e pode, a seu inteiro critério, acessar qualquer byte que esteja sob seu domínio, mesmo que ele não seja a pessoa certa para, digamos, abrir um relatório confidencial da diretoria ou a folha de pagamentos.
- A confiança no responsável pela administração dos sistemas de segurança deve ser apoiada por mecanismos de monitoração de acesso exclusivo dos auditores. Utilização de ferramentas para responsabilidade compartilhada, onde é necessário o consentimento de mais de uma pessoa na execução de determinadas tarefas, ajudam a minimizar um problema de confiança.

Sétima: Dados criptografados são tão seguros quanto à senha usada para sua decriptação.

- Todos os sistemas de criptografia possuem chaves com as quais é possível decifrar seu conteúdo. Um sistema - por mais forte que seja - perde seu valor caso a senha usada esteja disponível para terceiros.
- Este erro é cometido por muitos usuários, principalmente na guarda de arquivos usados como chave. Ao invés de gravá-los no próprio computador, procure guardá-los em um disquete (e leve este disquete para um lugar seguro). Caso estes arquivos estejam protegidos por senhas, ou caso as próprias senhas e *passphrases*, senhas formadas por frases, sejam usadas na criptografia, jamais as anotem em cadernos, *post-it*, palms etc.

Oitava: Um antivírus desatualizado é apenas ligeiramente melhor do que nenhum antivírus.

- As mais eficientes tecnologias de combate aos vírus são baseadas em pesquisas nos arquivos de um computador, comparando-os com trechos de vírus já catalogados pelo fabricante do antivírus.
- Quando um vírus é descoberto, o fornecedor do seu software antivírus "descreve" este vírus e fornece estes dados para que sua ferramenta possa reconhecê-lo caso o encontre perambulando pelos seus arquivos.
- Já deu para imaginar que um antivírus desatualizado, ou seja, que

não reconhece um determinado vírus - mesmo que ele esteja bem embaixo do seu nariz - não vai ser uma proteção muito eficiente. A grande maioria dos sistemas antivírus possui atualizações automáticas on-line, facilitando muito esse trabalho. Basta fazer a sua parte!

Nona: O anonimato absoluto não existe, nem dentro, nem fora da Internet.

- Durante qualquer tipo de interação com outras pessoas, dados sobre você são coletados e armazenados, independentemente do propósito e às vezes até mesmo contra a vontade do interlocutor.
- Em uma conversa sobre o tempo em um elevador você já deixou disponível, de forma aproximada, seu peso, sua altura, sua idade, seu status na sociedade, seu poder aquisitivo e, dependendo do sotaque, sua origem. Pode-se descobrir mais em crachás, observando posturas e gestos, puxando outros assuntos e, finalmente, observando em que andar você desce do elevador.
- Na Internet ou em qualquer outra rede, a situação é a mesma: computadores que conversam com outros computadores deixam as informações sobre a comunicação ou seus próprios sistemas armazenadas no interlocutor ou em pontos intermediários.
- Estas informações são geralmente arquivadas por conveniência (para futuras investigações, por exemplo), mas outras são especialmente requisitadas para um levantamento do comportamento dos usuários, verificação de um funcionário quanto ao seguimento da política de segurança de uma empresa ou até mesmo a identificação inequívoca de uma pessoa cruzando-se dados de diferentes organizações e websites.

Décima: Tecnologia não é um remédio para todos os males. OU Tecnologia não é uma panacéia.

- Algumas pessoas desconfiam de campanhas de marketing que prometem soluções milagrosas, perfeitas, definitivas e de baixo custo para qualquer tipo de produto. Profissionais da área de segurança não desconfiam: têm certeza de que não existe, na sua área, uma solução deste tipo.
- Nenhum software ou hardware é suficientemente bom para proteger eternamente seus sistemas computacionais. Assim como nem mesmo um exército inteiro é suficientemente bom para impedir um ataque inimigo bem sucedido.
- Primeiro porque segurança não se consegue só com tecnologia nem só com atitudes. Ela é uma combinação de equipamentos seguros e práticas seguras. Segundo porque a segurança não é um produto, é um processo. Mesmo que você consiga um nível de segurança satisfatório em um determinado momento, nada garante que as ameaças continuarão as mesmas e que nenhuma outra vulnerabilidade poderá ser explorada no futuro.
- Não espere que um fabricante forneça correções ou lance versões

aprimoradas dos seus sistemas de segurança que resolvam os problemas descritos acima. Não existe, hoje, outra solução para eles além de uma educação em segurança da informação.

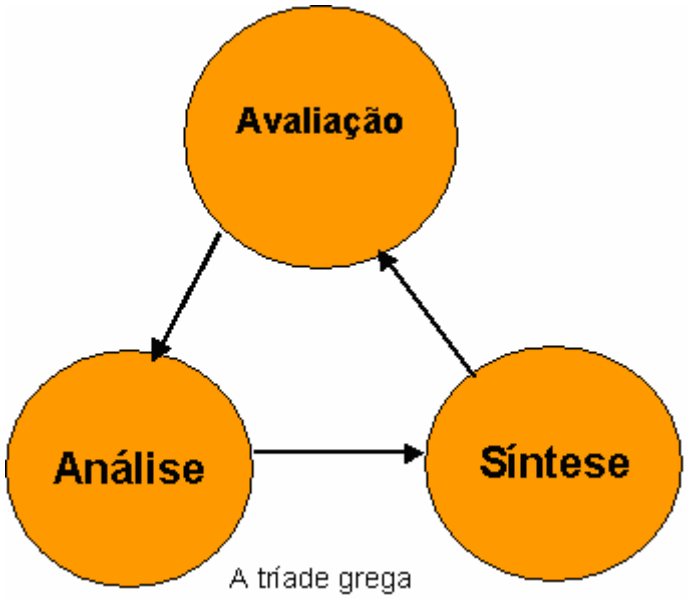
CAPÍTULO VI

Processo de Segurança

Segurança não é tecnologia, não é possível comprar um dispositivo que torne a sua empresa segura, assim como não é possível comprar ou criar um software capaz de tornar seu computador seguro (Wadlow, 2000).

Como trabalho, a segurança também se constitui de um processo. Pode-se fazer uma analogia com o trabalho de uma analista de sistemas, mas o trabalho de um profissional de segurança, deve-se resumir no mínimo em:

- Analise o problema levando em consideração tudo que conhece.
- Sintetize uma solução para o problema a partir de sua análise.
- Avalie a solução e aprenda em que aspectos não corresponderam a suas expectativas.



A tríade grega

Este processo deve ser feito continuamente, como num círculo vicioso.

O método PDCA (Plan, Do, Check e Action – Planejar, Executar, Verificar e Agir), é hoje o principal método da Administração pela Qualidade Total, tendo sido criado na década de 1920 por Shewhart. Ele se baseia no controle processos, mas pode ser adaptado para ser utilizando num ciclo de verificação da informação num processo de segurança, conforme proposto em (BS 7799-2, 2002).

Neste sentido a análise e medição dos processos são relevantes para a manutenção e melhoria dos mesmos, contemplando inclusive o planejamento, padronização e a documentação destes.

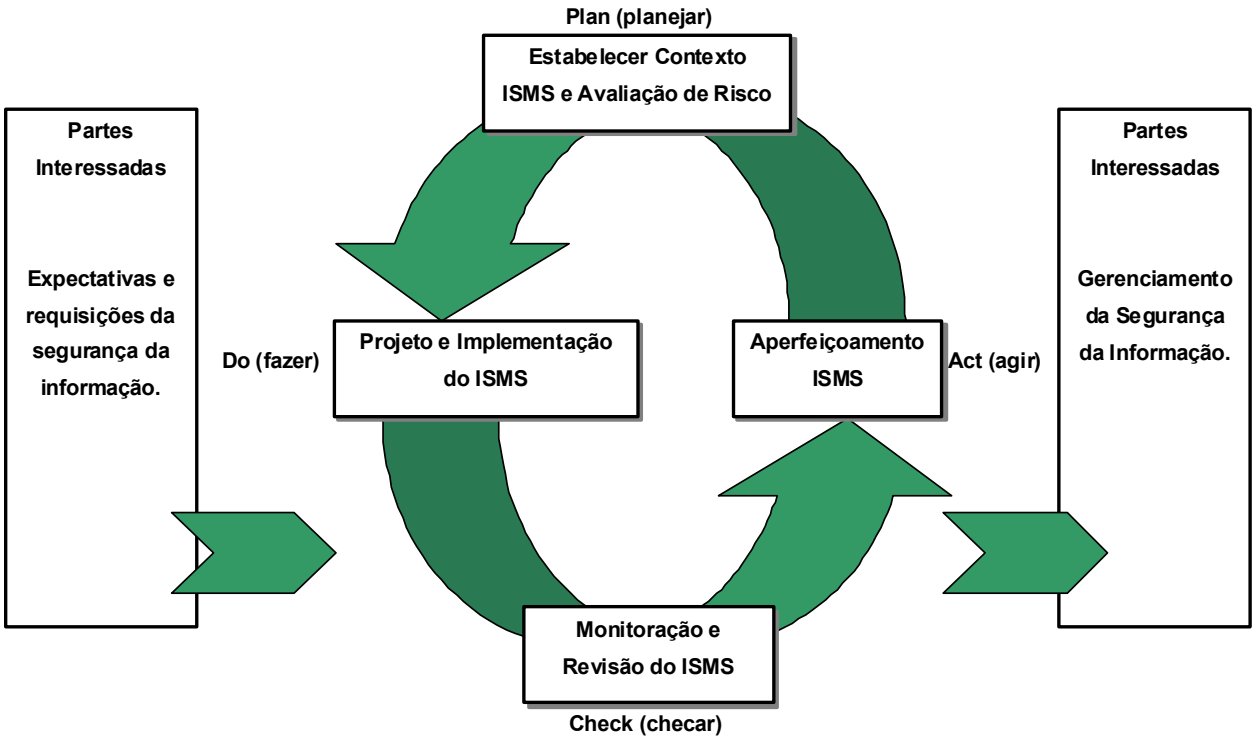
O uso dos mesmos pode ser assim descrito:

- *Plan* – Definir o que se quer, planejar o que será feito, estabelecer metas e definir os métodos que permitirão atingir as metas propostas. No caso de desenvolvimento de um Sistema de Informação, esta atividade pode corresponder ao planejamento do Sistema.

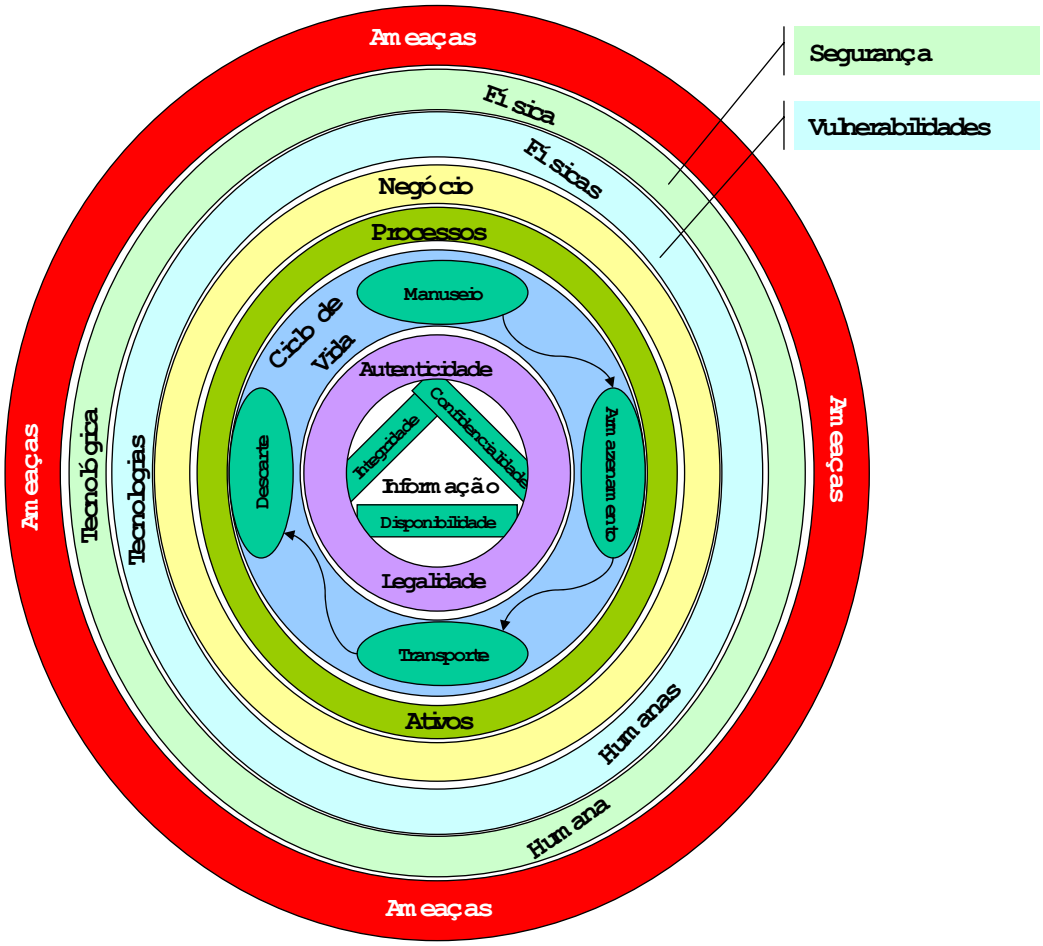
- *Do* – Tomar iniciativa, educar, treinar, implementar, executar o planejado conforme as metas e métodos definidos. No caso de desenvolvimento de um Sistema de Informação, esta atividade pode corresponder ao desenvolvimento e uso do sistema.

- *Check* – Verificar os resultados que se está obtendo, verificar continuamente os trabalhos para ver se estão sendo executados conforme planejados. No caso de desenvolvimento de um Sistema de Informação, esta atividade pode corresponder aos testes, análise das informações geradas e avaliação de qualidade do sistema.

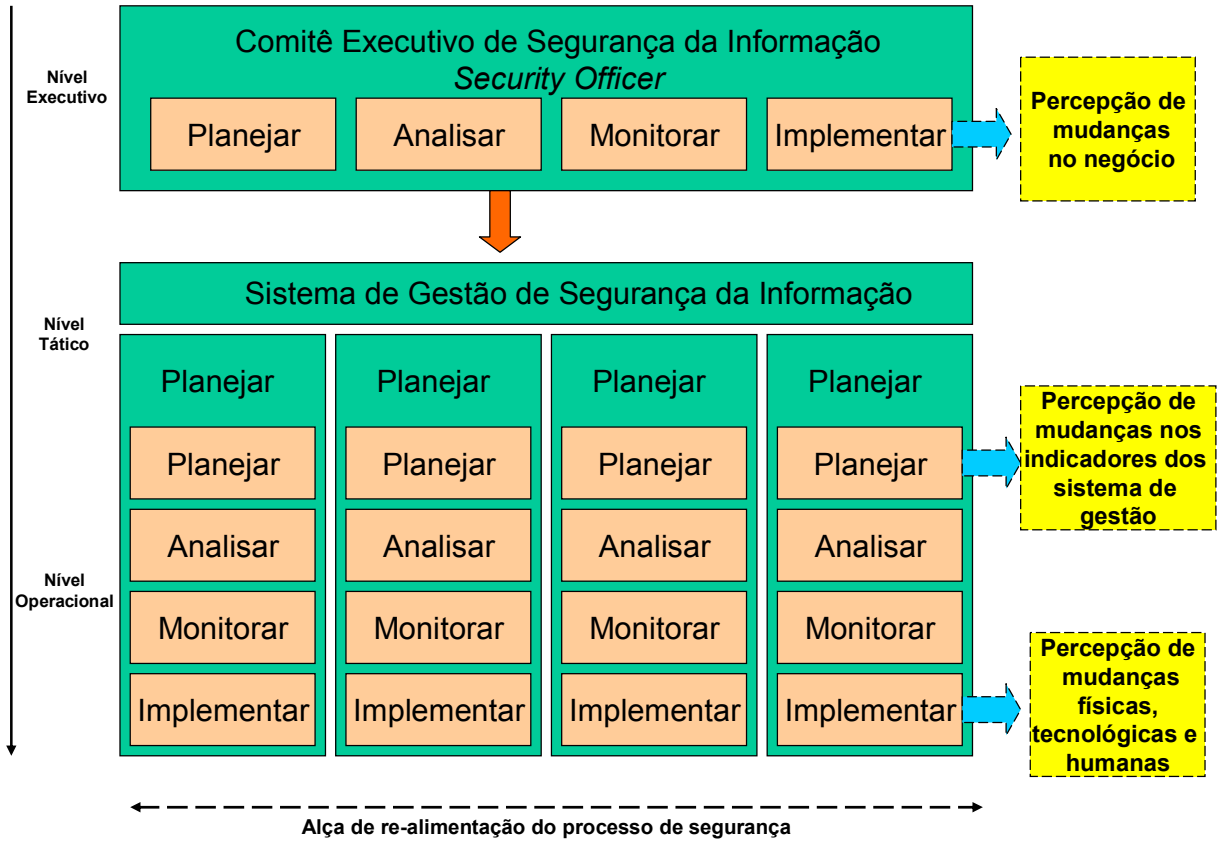
- *Action* – Fazer correções de rotas se for necessário, tomar ações corretivas ou de melhoria, caso tenha sido constatada na fase anterior a necessidade de corrigir ou melhorar processos. No caso de desenvolvimento de um Sistema de Informação, esta atividade pode corresponder aos ajustes, implementações e continuidade do sistema.



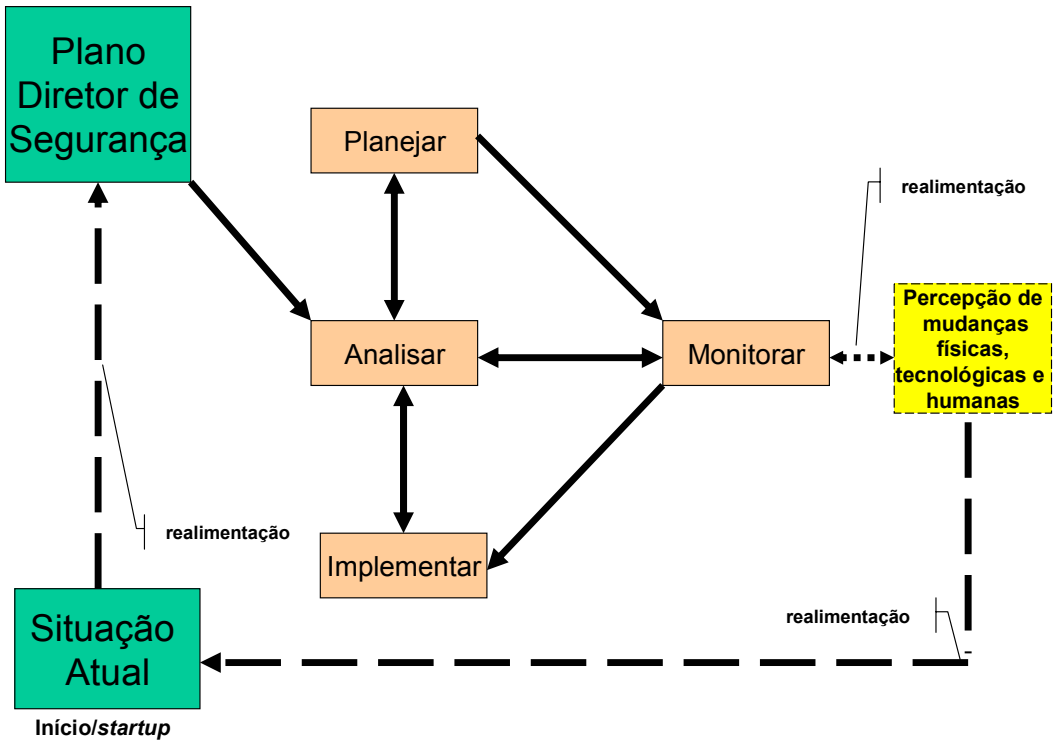
A análise da segurança deve ser vista como análise através de perímetros. Observe a próxima figura:



Planejamento é o fator crítico de sucesso para a iniciativa de gerir a segurança da informação e o Plano Diretor de Segurança (similar a um Plano Diretor de Informática) é justamente o elemento específico para este fim. Este plano é que irá apontar o caminho e os passos (atividades) que irão apontar e suprir as necessidades de segurança do negócio. Deve ser construído tendo o envolvimento de todos os níveis da empresa. Veja a próxima figura:



A próxima figura ilustra as fases do PDCA ao criar-se uma Plano Diretor de Segurança.


Plano Diretor de Segurança
Planejar
realimentação
Percepção de mudanças físicas, tecnológicas e humanas
Analisar
Monitorar
realimentação
Implementar
Situação Atual
realimentação
Início/*startup*

CAPÍTULO VII

Políticas de Segurança[9]

Existe uma antiga piada, contada mais ou menos assim:

> Um guarda de segurança que trabalha no turno da noite em uma fábrica vê um homem baixinho sair do prédio, empurrando um carrinho de mão vazio. O guarda, com uma suspeita repentina, pára o homem, que pergunta por que está sendo parado. “Apenas quero ter certeza de que você não está roubando nada”, diz o guarda, forma grosseira. “Confira tudo o que quiser”, responde o homem, e o guarda procura, mas não encontra nada suspeito e permite que o homem vá embora. Na noite seguinte, acontece à mesma coisa. Isso se repete por algumas semanas e então o baixinho não aparece mais no portão.
>
> Passam vinte anos e o guarda, já aposentado, está sentado em um bar, quando o baixinho entra. Reconhecendo-o, o guarda aposentado se aproxima, explica quem é e oferece pagar uma bebida, se o baixinho responder a uma pergunta. O homem concorda e o guarda diz: “Tenho certeza de que você estava levando algo, mas nunca consegui descobrir o que você estava roubando”. O baixinho pegou a bebida e, enquanto levava o copo à boca, disse: ”Eu estava roubando carrinhos de mão”.

A idéia dessa piada sugere, é claro, que as medidas de segurança nada representarão se os guardas não souberem o que deverão proteger.

Experimente perguntar ao executivo de uma empresa quais são os objetivos das equipes de segurança e provavelmente receberá respostas parecidas com “são eles que nos mantêm seguros lá”. Se pressionadas, muitas pessoas poderão ir um pouco adiante, descrevendo o lado da segurança física: não permitir a entrada de visitas sem autorização, verificar se estão trancadas as portas que devem permanecer trancadas e ajudar em qualquer emergência. É bem pouco provável que as mesmas pessoas compreendam para que existe a equipe de segurança dos computadores. Na melhor das hipóteses, provavelmente você ouvirá “manter os *hackers* fora de nossa rede”. Cabe à equipe de segurança da rede partir dessa descrição vaga e mostrar que seu trabalho é mais amplo, até o ponto em que possa fixar prioridades e merecer estar incluído nos orçamentos.

Se você perguntar a profissionais de segurança o que poderá fazer de mais importante para proteger sua rede, eles responderão, sem hesitar, que é escrever uma boa política de segurança.

---

[9] Capítulo baseado em (Wadlow, 2000)

Definindo um Política de Segurança de Informações

A Política de Segurança é apenas a formalização dos anseios da empresa quanto à proteção das informações (Abreu, 2002).

A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais (Dias, 2000).

Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. Não havia como ser diferente em uma empresa. Nesta, precisamos definir padrões de conduta para garantir o sucesso do negócio.

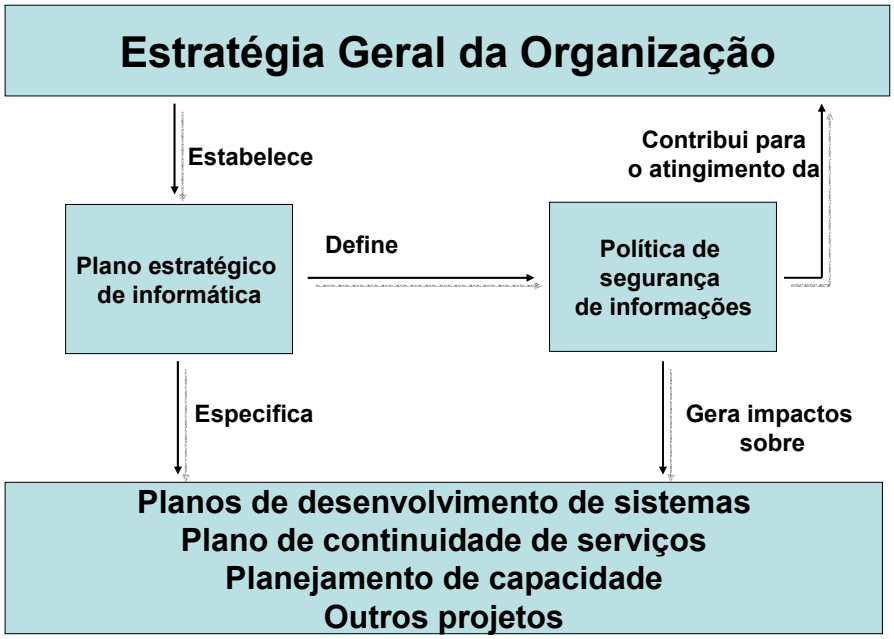
Ainda fazendo um paralelo com a legislação, temos nesta: leis, decretos, medidas provisórias entre outras.

Uma política de segurança atende a vários propósitos:

1 Descreve o que está sendo protegido e por quê;
2 Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo;
3 Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;
4 Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário;
5 Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”;
6 Impede que o departamento de segurança tenha um desempenho fútil.

A política de segurança de informações deve estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e, conseqüentemente, as informações por eles manipuladas. É importante que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos (Dias, 2000).

A política de segurança, deve ir além dos aspectos relacionados com sistemas de informação ou recursos computacionais, ela deve estar integrada com as políticas institucionais da empresa, metas de negócio e ao planejamento estratégico da empresa. A próxima figura mostra o relacionamento da política de segurança de informações com a estratégia da organização, o plano estratégico de informática e os diversos projetos relacionados (Dias, 2000).



Armadilhas

Se uma boa política de segurança é o recurso mais importante que se pode criar para tornar uma rede segura, por que a maioria das empresas considera tão difícil criar uma política eficiente? Existem várias razões principais.

- **Prioridade**: A política é importante, mas hoje à tarde é preciso que alguém coloque o servidor da Web on-line. Se for necessário que as pessoas deixem de cuidar do que consideram urgentes e usem o tempo para concordar com a política de segurança, será muito difícil ter sucesso.

- **Política interna**: Em qualquer empresa, grande ou pequena, vários fatores internos afetam qualquer decisão ou prática.

- **Propriedade**: De uma maneira bastante estranha, em algumas empresas existe uma briga entre vários grupos que desejam ser os donos da política e, em outras empresas, a briga ocorre entre vários grupos que explicitamente não querem ser os responsáveis pela política.

- **Dificuldade para escrever**: Uma boa política é um documento difícil de se organizar de maneira precisa, principalmente quando é necessário que seja abrangente. Não é possível prever todos os casos e todos os detalhes.

Algumas sugestões para ajudar a solucionar esses problemas:

- Uma boa política hoje é melhor do que uma excelente política no próximo ano;

- Uma política fraca, mas bem-distribuída, é melhor do que uma política forte que ninguém leu;
- Uma política simples e facilmente compreendida é melhor do que uma política confusa e complicada que ninguém se dá o trabalho de ler;
- Uma política cujos detalhes estão ligeiramente errados é muito melhor do que uma política sem quaisquer detalhes;
- Uma política dinâmica que é atualizada constantemente é melhor do que uma política que se torna obsoleta com o passar do tempo;
- Costuma ser melhor se desculpar do que pedir permissão.

Como organizar um golpe

Existe uma forma de estabelecer uma política decente em sua empresa. Não é perfeita nem sem riscos, mas se conseguir administrá-la, você economizará muito tempo e dificuldades. O processo é o seguinte:

1. **Escreva uma política de segurança para sua empresa**. Não inclua nada específico. Afirme generalidades. Essa política não deverá ocupar mais de cinco páginas. Nem serão necessários mais de dois dias para escrevê-la. Pense em escrevê-la durante o fim de semana, assim não será perturbado. Não peça ajuda. Faça de acordo com suas próprias idéias. Não tente torná-la perfeita, procure apenas reunir alguma idéias essenciais. Não é necessário que esteja completa e não precisa ser de uma clareza absoluta.

2. **Descubra três pessoas dispostas a fazer parte do "comitê de política de segurança"**. A tarefa dessas pessoas será criar regras e emendas para a política, sem modificá-la. As pessoas do comitê deverão estar interessadas na existência de uma política de segurança, pertencer a partes diferentes da empresa, se possível, e estar dispostas a se encontrarem rapidamente uma ou duas vezes por trimestre.
   Deixe claro que a aplicação da política e a solução de qualquer problema relacionado são sua responsabilidade e não delas. O trabalho do comitê será o de legisladores e não de executores.

3. **Crie um site interno sobre a política e inclua uma página para entrar em contato com o comitê**. À medida que as emendas forem escritas e aprovadas, acrescente-as ao site tão depressa quanto possível.

4. **Trate a política e as emendas como regras absolutas com força de lei**. Não faça nada que possa violar a política e não permita que ocorram violações. Em algum momento, a administração notará o que está acontecendo. Permita e incentive que administração se envolva no processo tanto quanto possível, a não ser que o pessoal da administração pretenda simplesmente eliminar a sua política e deixá-lo com nada. Oriente-os para a criação de uma política nova e melhor. Não será possível engajá-los a menos que realmente o queiram e este é um método excelente para envolvê-los. Se eles continuarem interessados,

você será capaz de estabelecer uma política com o aval da administração. Se eles passarem a se ocupar de outras coisas, sua política seguirá no processo em andamento.

5. **Se alguém tiver algum problema com a política, faça com que a pessoa proponha uma emenda**. A emenda poderá ter apenas uma página. Deverá ser tão genérica quanto possível. Para se tornar uma emenda, será necessário que dois dos três (ou mais) membros do comitê de política concordem.

6. **Programe um encontro regular para consolidar a política e as emendas**. Esse encontro deverá acontecer uma vez por ano e deverá envolver você e o comitê de política de segurança. O propósito desse encontro é, considerando a política e possíveis emendas, combiná-los em uma nova declaração de política de cinco páginas. Incentive o próprio comitê a redigi-la, se preferir, mas provavelmente o melhor procedimento será dedicar um fim de semana para escrever outro rascunho da política, incluindo todas as emendas.

7. **Repita o processo novamente. (item 3 em diante)**. Exponha a política no site, trate-a como uma lei, envolva as pessoas da administração, se desejarem ser envolvidas, acrescente emendas conforme seja necessário e revise tudo a cada ano. Continue repetindo esse processo, enquanto for possível.

Divisões da Política

Podemos dividir essa documentação em três tipos de texto a serem elaborados. São eles (Abreu, 2002):

Texto em nível estratégico

Há situações no dia-a-dia em que precisamos tomar decisões. E, de vez em quando, o bom senso é a ferramenta usada pelos profissionais para a tomada de uma decisão. Sim, porque se nunca ninguém passou pela situação antes e não há nenhuma orientação da empresa para o que fazer quando ela acontece, o talento é o responsável pela definição entre a genialidade da resolução do problema ou a loucura de quem tomou a decisão errada.

Vamos a um exemplo:

"A segurança da informação deve ser estabelecida desde que não inviabilize o negócio da instituição".

A frase não disse muito para aqueles que estão procurando "pão, pão; queijo, queijo", mas, em compensação, disse tudo para aquele indivíduo que se encontra na seguinte situação:

O telefone toca:
- Preciso que você libere uma regra do firewall para que eu possa realizar uma operação.

Se ele liberar o acesso ao equipamento, pode ser punido porque tomou uma decisão que, para todos, é obviamente errada. Todos sabem que liberar aquele acesso é abrir uma vulnerabilidade no sistema, mas, se ele não liberar esse acesso, a empresa deixará de executar uma operação crucial para a continuidade de um projeto que precisa necessariamente ser terminado hoje.

O que fazer ?

Lendo a frase escrita acima, o funcionário pode tomar sua decisão (liberar o acesso, apesar de expor momentaneamente a empresa) com a consciência limpa, sabendo que será parabenizado pela sua competência e alinhamento com os valores da empresa. Então, chegamos à palavra chave quando falamos em nível estratégico: valores, ou seja, um RUMO a ser seguido.

Texto em nível tático

Analisemos o comentário:

Minha empresa tem filiais em 3 cidades brasileiras, e as redes desses três locais são completamente distintas em funcionamento e padrões. Uma vez precisamos levantar um histórico de um projeto interno, e em uma das filiais esse histórico não existia. Se fosse na minha filial, existiria. Por que a diferença?

Simples. Ninguém disse ao administrador do banco de dados daquela filial que a cópia de segurança do banco precisava ser armazenada por 6 meses. O funcionário daquela cidade achou que era suficiente guardar as fitas durante 1 mês. Após esse período, as fitas eram reutilizadas para novas cópias de segurança.

"As cópias de segurança de informações referentes a projetos devem permanecer inalteradas durante o período de 6 meses após a sua efetuação."

Concordam que essa frase resolveria o problema ?

A palavra chave para o nível tático é: padronização de ambiente. Equipamentos, software, senhas, utilização de correio eletrônico, cópias de segurança, segurança física etc. Tudo isso precisa e deve ser padronizado. Isso faz com que todos os pontos da empresa tenham o mesmo nível de segurança e não tenhamos um elo mais fraco na corrente.

Texto em nível operacional

“Na mesma empresa onde tivemos problemas com backup, em uma

das cidades ninguém consegue receber e-mails com planilhas anexadas".

Obviamente, o que deve estar acontecendo nesse estado é que o administrador, sabiamente ou não, colocou um limite para mensagens de e-mail do tipo: caso ela seja maior do que X, não receba.

Por que temos esse problema, ou solução, apenas nesse estado?

Porque ninguém disse como configurar o equipamento. Nesses casos, é preciso ser minucioso na definição da padronização, visto que às vezes o "clicar" de uma "caixinha de configuração" pode ter impacto relevante no funcionamento do ambiente de TI da empresa e, talvez, nos negócios da empresa.

A palavra chave nesse caso é: detalhamento para garantir perfeição no atendimento e continuidade dos negócios, independentemente do fator humano. Se a configuração está no papel, não há como ser realizada de forma diferente.

A parte operacional da política de segurança vem exatamente para padronizar esses detalhes de configurações dos ambientes. Podemos ter um padrão nacional ou, quem sabe, um padrão por estado. Isso irá depender da necessidade da empresa. O importante é sabermos que precisamos desse padrão. As pessoas possuem conhecimentos diferentes e aposto todas as minhas fichas que, em qualquer empresa sem uma política de segurança (leia-se qualquer tipo de papel definindo o que e como deve ser feito), a configuração de uma cidade não será igual à configuração de uma outra.

Conteúdo da Política

Algumas questões cuja inclusão em uma política de segurança deverá ser levada em consideração:

O que estamos protegendo ?

- "Se não souber o que e por que está defendendo, não será possível defendê-lo"
- "Saber que está sendo atacado representa mais da metade da batalha".

Descreva de forma razoavelmente detalhada os tipos de níveis de segurança esperados para sua empresa. Por exemplo, caracterize as máquinas da rede da seguinte maneira:

- Vermelho – Contém informações extremamente confidenciais ou fornece serviços essenciais;
- Amarelo – Contém informações sensíveis ou fornece serviços importantes.
- Verde – Capaz de ter acesso às máquinas vermelhas ou amarelas, mas não armazena informações sensíveis nem executa funções cruciais de uma maneira direta.

- Branco – Sem acesso aos sistemas vermelho, amarelo ou verde e não pode ser acessado externamente. Sem funções ou informações sensíveis.
- Preto – Acessível externamente. Sem acesso aos sistemas vermelho, amarelo, verde ou branco.

Reunindo essas informações, você agora terá um vocabulário para descrever todas as máquinas existentes na rede e o nível de segurança a se atribuído a cada máquina. As mesma nomenclatura permitirá descrever as redes, além de exigir, por exemplo, que as máquinas vermelhas estejam conectadas às redes vermelhas e assim por diante.

Métodos de proteção

Descrever as prioridades para a proteção da rede. Por exemplo, as prioridades organizacionais poderão ser as seguintes:

1. Saúde e segurança humana;
2. Conformidade com a legislação aplicável local, estadual e federal;
3. Preservação dos interesses da empresa;
4. Preservação dos interesses dos parceiros da empresa;
5. Disseminação gratuita e aberta de informações não-sensíveis.

Descrever qualquer política de caráter geral para o acesso de cada categoria do sistema, e ainda criar um ciclo de qualificação que irá descrever com que freqüência uma máquina de determinado tipo de usuário deverá ser examinada para verificar se ainda está configurada corretamente de acordo com seu status de segurança.

Responsabilidades

Descrever as responsabilidades (e, em alguns casos, os privilégios) de cada classe de usuários do sistema.

- Geral
  - Conhecimento dessa política;
  - Todas as ações de acordo com essa política;
  - Informar à segurança qualquer violação conhecida a essa política;
  - Informar à segurança qualquer suspeita de problemas com essa política.

- Administrador de sistema / Operações
  - Todas as informações sobre os usuários serão tratadas como confidenciais;
  - Não será permitido acesso não-autorizado a informações confidenciais;
  - Assegurar todas as ações consistentes com o código de conduta de um administrador de sistemas.

- Administrador de segurança

- Mais alto nível de conduta ética;
- Assegurar todas as ações consistentes com o código de conduta de um responsável pela segurança;

- Contratado
  - Acesso a máquinas especificamente autorizadas na forma especificamente autorizada;
  - Solicitará autorização prévia por escrito para qualquer ação que possa ser interpretada como uma questão de segurança.

- Convidado
  - Nenhum acesso a recursos de computação, a menos que haja notificação prévia por escrito à segurança.

Uso adequado

Como os funcionários deverão ou não usar a rede.

- Geral
  - Uso pessoal mínimo durante o horário comercial normal;
  - Nenhuma utilização da rede para atividades comerciais externas;
  - Acesso a recursos de Internet consistentes com as políticas de RH.

- Administrador de sistemas
  - Acesso responsável a informações sensíveis ou pessoais na rede;
  - Todo acesso especial é justificado por operações comerciais.

- Segurança
  - Acesso responsável a informações sensíveis ou pessoais na rede;
  - Todo acesso especial é justificado por operações comerciais ou segurança;
  - Uso de ferramentas de segurança apenas para objetivos comerciais legítimos.

- Contratado
  - Nenhum acesso pessoal a qualquer tempo;
  - Uso mínimo da rede e apenas por motivos específicos relativos a determinados contratos.

- Convidado
  - Nenhum uso da rede a qualquer tempo

Conseqüências

Descrever como é determinada a importância de uma violação da política e as categorias de conseqüências.

Penalidades

Descrever quais as penalidades de acordo com o nível do descumprimento de um item da política de segurança.

- Crítica
  - Recomendação para demissão;
  - Recomendação para abertura de ação legal

- Séria
  - Recomendação para demissão;
  - Recomendação para desconto de salário

- Limitada
  - Recomendação para desconto de salário
  - Repreensão formal por escrito
  - Suspensão não-remunerada

Para relaxar e refletir

- Na Alemanha: tudo é proibido, exceto aquilo que é permitido.
- Na França: tudo é permitido, exceto aquilo que é proibido.
- Em Cuba: tudo é proibido, inclusive aquilo que é permitido.
- No Brasil: tudo é permitido, inclusive aquilo que é proibido.

Estudo de Caso

Como avaliação parcial da disciplina, vamos analisar o estudo de caso.

Quais são as atitudes que sua empresa deve evitar na área de informática.

> Há menos de uma década, bastavam um cadeado, correntes reforçadas no portão e um cachorro feroz para manter a empresa e seus dados protegidos dos gatunos. Hoje, com a maior parte das informações digitalizadas, é preciso ir além. Não dá para deixar de investir em softwares de segurança e no treinamento dos funcionários para preservar os segredos da empresa. E não são poucas as ocorrências de espionagem industrial. A maioria dos 'piratas' conta com a ajuda dos funcionários da área de informática. Com bons conhecimentos técnicos, facilitam a vida da concorrência por meio da entrega de dados confidenciais da casa.
>
> Vejam abaixo quais são os sete pecados capitais da área

de tecnologia e confira se sua empresa comete alguns deles:

1. ORGULHO – Os administradores de rede acreditam que apenas os firewalls (softwares que barram a entrada e saída de e-mails) e os tradicionais antivírus são capazes de garantir total segurança aos arquivos da empresa. Descartam qualquer outra ação preventiva.

2. INVEJA – Profissionais que baixam programas espiões (*spyware*), usam brechas de segurança na rede para roubar dados confidenciais da empresa.

3. GULA – Os funcionários não resistem à fartura de banda e baixam arquivos pesados de vídeo e de música, possibilitando que a rede de acesso à Internet fique mais lenta.

4. LUXÚRIA – A combinação do acesso a sites de pornografia, à banda larga e à rede ponto-a-ponto facilita a captura de imagem para o computador pessoal. E, conseqüentemente, facilita também a troca de arquivos entre os funcionários, deixando vulnerável o acesso a informações sigilosas.

5. IRA – Ceder aos apelos dos momentos de fúria e cometer ataques à rede interna pode provocar perdas de dados e desperdício de recursos.

6. COBIÇA – A tentação de encher o computador do trabalho com arquivos em MP3 e DVDs funciona como uma porta de entrada para vírus e programas espiões (spyware).

7. PREGUIÇA – Ficar pendurado nos programas de mensagens instantâneas, jogos interativos e eventos de esportes ao vivo no ambiente de trabalho gera custos e mau uso do tempo. 90% dos gerentes de tecnologia da informação usam apenas antivírus para a proteção da rede

QUESTÃO

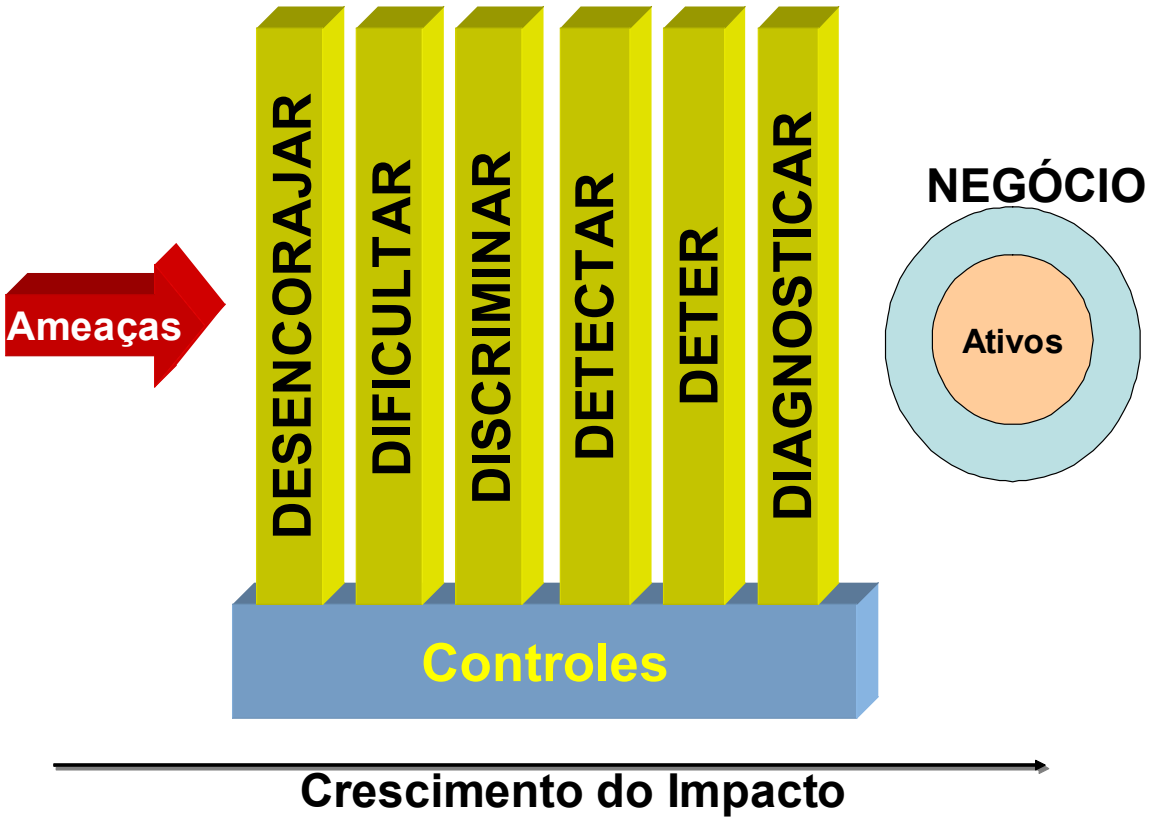
1) Escreva políticas de segurança para resolver os problemas detectados / apontados no texto. Para cada política escrita, você deve justificar a sua utilização e ilustrar / descrever uma possível falha de segurança que seria evitada se a sua política fosse seguida à risca. Lembre-se de escrever uma política no nível estratégico, tático e operacional.

CAPÍTULO VIII

Barreiras de Segurança

Conceitualmente, diante da amplitude e complexidade do papel da segurança, é comum estudarmos os desafios em camadas ou fases, particionando todo o trabalho para tornar mais claro o entendimento de cada uma delas. Chamamos esta divisão de barreiras.

Cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos, e por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita interação e integração, como se fossem peças de um único quebra-cabeça.



- **Barreira 1: Desencorajar** – Esta é a primeira das cinco barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas, já são efetivos nesta fase.

- **Barreira 2: Dificultar** – O papel desta barreira é complementar à anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Como exemplo, podemos citar os dispositivos de autenticação para acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, senhas, *smartcards* e certificados digitais, além da criptografia, firewall, etc.

- **Barreira 3: Discriminar** – Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites e acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e bancos de dados. Os processos de avaliação e gestão do volume de usos dos recursos, como e-mail, impressora, ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos das atividades desta barreira.

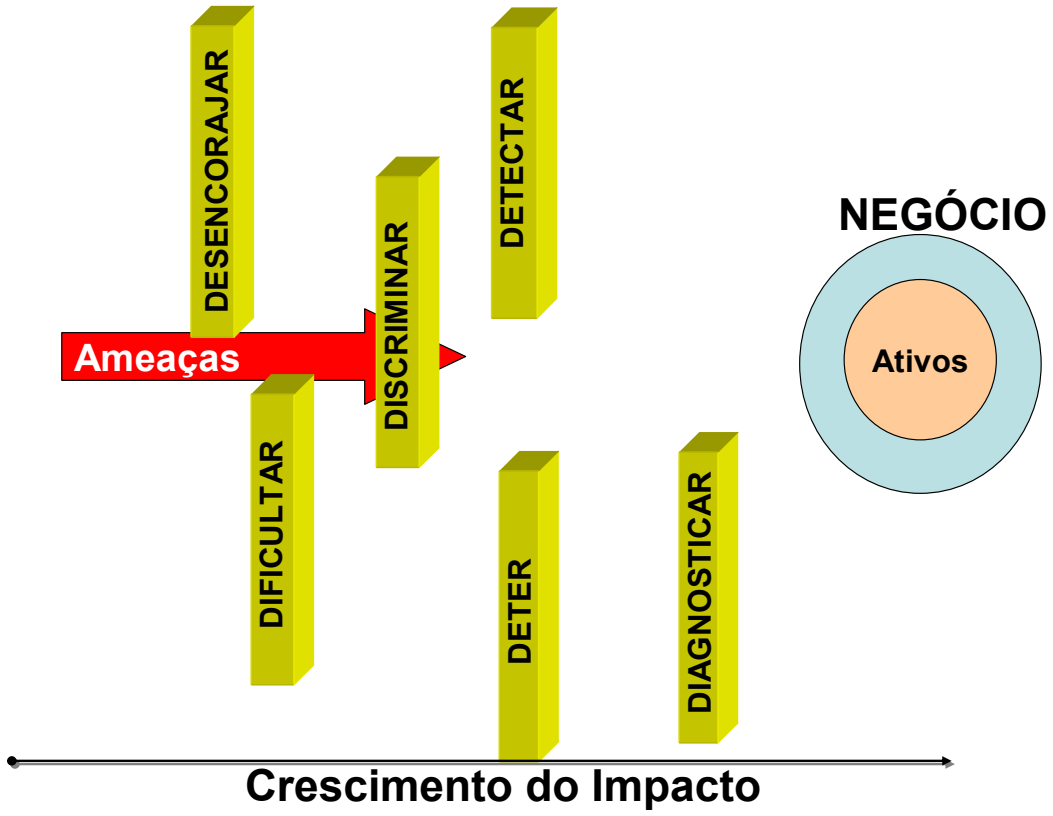
- **Barreira 4: Detectar** – Mais uma vez agindo de forma complementar às suas antecessoras, esta barreira deve munir a solução de segurança de dispositivos que sinalizem, alertem e instrumentam os gestores da segurança na detecção de situações de risco. Seja em uma tentativa de invasão, uma possível contaminação por vírus, o descumprimento da política de segurança da empresa, ou a cópia e envio de informações sigilosas de forma inadequada.
  Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e os sistema de detecção de intrusos, que reduziram o tempo de resposta a incidentes.

- **Barreira 5: Deter** – Representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.

- **Barreira 6: Diagnosticar** – Apesar de representar a última barreira no diagrama, esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança. Pode parecer o fim, mas é o elo de ligação com a primeira barreira, criando um movimento cíclico e contínuo. Devido a esses fatores esta é a barreira de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa.

É importante notar que um trabalho preliminar de diagnóstico mal conduzido ou executado sem metodologia e instrumentos que confiram maior precisão ao processo de levantamento e análise de riscos, poderá distorcer o

entendimento da situação atual de segurança e simultaneamente a situação desejada. Desta forma, aumenta a probabilidade de se dimensionar inadequadamente estas barreiras, distribuindo os investimentos de forma desproporcional, redundante muitas vezes, e pior, de forma ineficaz. O retorno sobre investimento não corresponderá às expectativas e a empresa não atingirá o nível de segurança adequado à natureza de suas atividades.



Cenário 1

Tome como exemplo uma grande loja de departamentos e 10 possíveis assaltantes (daqueles bem simples, que roubam somente roupas / perfumes / etc).

Vamos ver como funcionaria cada barreira. As 5 primeiras barreiras (se corretamente organizadas), poderia funcionar da seguinte forma:

- **DESENCORAJAR –** Ao entrar na loja, os assaltantes percebem um grande aviso na porta “Sorria, você está sendo filmado !!!”. Como este aviso, 2 assaltantes ficaram intimidados e desistiram do furto. Sobraram 8.
- **DIFICULTAR –** Nas peças de roupas que seriam roubadas, existe um dispositivo eletromagnético que impede a saída do produto da loja sem antes passar pelo caixa. Com isto, 2 assaltantes foram para outra loja. Sobraram 6.

- **DISCRIMINAR –** A loja dispõem de câmeras de vídeo posicionadas de forma a cobrir todos os pontos da loja. Estas câmeras possibilitam a identificação dos assaltantes. Ao perceberem as câmeras, 2 assaltantes ficaram receosos e desistiram. Sobraram 4.
- **DETECTAR –** Ao passar pela porta, os alarmes identificaram as peças de roupas com os dispositivos, soando um alarme sonoro. 2 assaltantes largaram as peças de roupas e fugiram. Não perca as contas, ainda sobraram 2.
- **DETER –** O armário, digo, vigia da loja, prende os 2 últimos assaltantes. Estes meliantes tão cedo não voltam a agir.
- **DIAGNOSTICAR –** Nesta fase, a equipe de segurança da loja irá fazer um balanço sobre eficácia dos métodos adotados. O ideal, seria que os assaltantes desistam ao encontrar a barreira DISCRIMINAR. Neste exemplo, se todos os 4 assaltantes ignorassem a barreira DETECTAR, o vigia (barreira DETER) teria dificuldades. Ou se os 2 últimos assaltantes estivessem armados, o vigia (barreira DETER) poderia não funcionar adequadamente (poderia haver troca de tiros, ocasionado em possíveis perdas humanas).

Um exemplo de melhoria poderia ser aplicado na barreira DISCRIMINAR, ao identificar suspeitos, através de algum software de reconhecimento de imagens interligado com o banco de dados da polícia, a polícia poderia ser chamada de forma a evitar maiores prejuízos para a loja e seus clientes.

Cenário 2

Num cenário bancário, a porta giratória com identificação de metais, pode ser classificado como um método de desencorajamento, dificuldade (não é fácil passar uma arma), discriminação (identifica uma arma) , detecção e deteção (pois o suspeito fica preso na porta).

Estudo de Caso

Rever as políticas de segurança criadas por vocês e verificar se as barreiras estão sendo aplicadas nas políticas;

CAPÍTULO IX

Gerenciamento de Risco

O risco não é um novo problema ou uma nova terminologia; os seres humanos sempre tiveram de enfrentar (ou encarar) os riscos no seu meio ambiente, embora seu significado tenha mudado, como tem mudado a sociedade e o próprio meio onde vive. No passado, a grande preocupação estava centrada nos desastres naturais (geológicos e climatológicos) na forma de inundações, secas, terremotos e tempestades.

Após a revolução industrial, os riscos naturais foram substituídos por aqueles gerados pelo próprio homem; nos Estados Unidos, os acidentes originados dos perigos tecnológicos, representam de 15 a 20% da mortalidade humana e tem ultrapassado significativamente daqueles naturais, em termos do impacto perante a sociedade, custo e importância (Leveson et al, 1997).

Uma das ferramentas mais poderosas no gerenciamento de riscos é o conhecimento. Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de grande parte das organizações, esta deve ser tratada como tal, sendo protegida nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade, seguindo a linha adotada pelo Governo Federal. Neste contexto, o gerenciamento de risco indica os caminhos e as informações que devem ser protegidas.

Conceitos Básicos

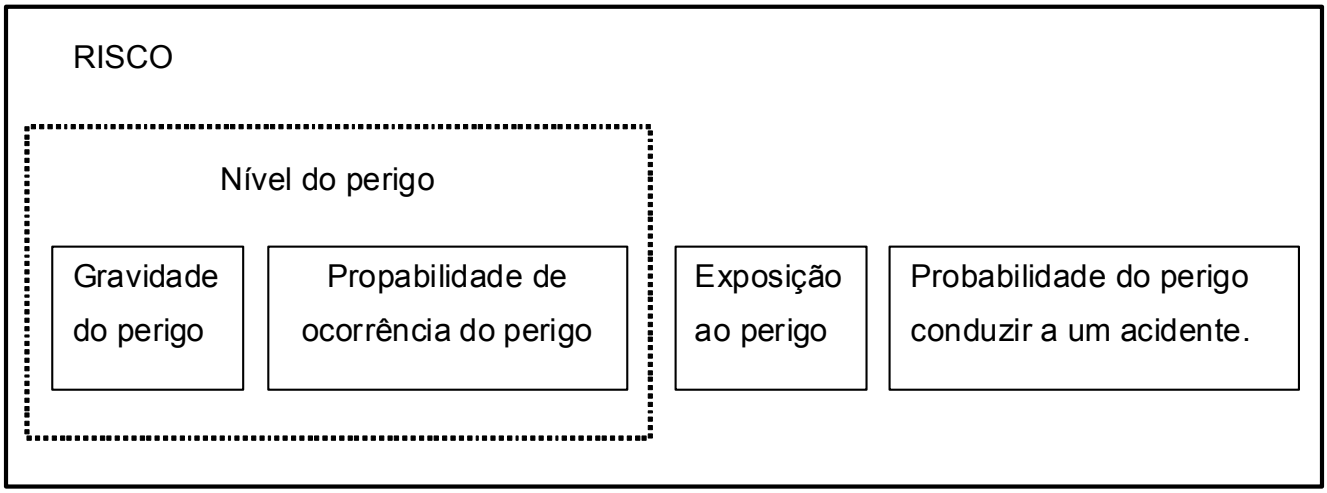
- **Risco**
  - Uma expectativa de perda expressada como a probabilidade de que uma ameaça em particular poderá explorar uma vulnerabilidade com um possível prejuízo;
  - Risco pode se definido como uma medida da incerteza associada aos retornos esperados de investimentos (Duarte Júnior, 2004);
  - Subentende-se por risco, o nível do perigo combinado com: (1) a probabilidade de o perigo levar a um acidente e, (2) a exposição ou duração ao perigo (algumas vezes denominado de latente); algumas vezes, o risco é limitado ao relacionamento entre o perigo e o acidente, ou seja, a probabilidade do perigo conduzir a um acidente, mas não da probabilidade do perigo ocorrer (Leveson et al, 1997);
  - Conforme (Scoy, 1992), risco não é ruim por definição, o risco é essencial para o progresso e as falhas decorrentes são parte de um processo de aprendizado.

- **Avaliação ou Análise de Risco** – Um processo que identifica sistematicamente recursos valiosos de sistema e ameaças a aqueles recursos, quantifica as exposições de perda (isto é, potencialidade de

ocorrer uma perda) baseadas em freqüências estimadas e custos de ocorrência, e (opcionalmente) recomenda como alocar recursos às contramedidas no para minimizar a exposição total.

- **Gerenciamento de Riscos** – O processo de identificar, de controlar, os eventos incertos, eliminando ou minimizando os que podem afetar os recursos de sistema.

O perigo tem duas importantes características: a gravidade (algumas vezes denominada de dano) e a probabilidade da ocorrência. A próxima figura ilustra o conceito do risco e o seu relacionamento com o perigo (Leveson et al, 1997).



A gravidade do perigo é definida como o pior acidente possível de ocorrer, resultante do perigo dado pelo ambiente na sua condição menos favorável. A probabilidade de ocorrência do perigo pode ser especificada tanto quantitativamente como qualitativamente; infelizmente, quando o sistema está sendo projetado e os níveis de perigo estejam sendo avaliados e pontuados, para a eliminação dos riscos potenciais, as informações necessárias para a sua avaliação nem sempre estão disponíveis; neste caso, utiliza-se de banco de dados de alguns projetos que estejam disponíveis ou ainda, baseando-se em avaliações puramente qualitativas. A combinação da gravidade somada a probabilidade de ocorrência é freqüentemente denominada de nível do perigo. A exposição ou duração de um perigo é uma componente do risco; desde que um acidente envolve uma coincidência de condições, na qual o perigo é justamente um deles, quanto maior o estado de perigo existir maiores são as chances de que outras condições ocorram, ou seja, a coincidência de condições necessárias para um acidente pode ter estatisticamente, uma baixa probabilidade, mas a probabilidade da coincidência pode dramaticamente ser aumentada, caso o perigo esteja presente por longos períodos de tempo.

Importância da Informação

Para que o processo de classificação possa ser guiado com êxito, não dependendo exclusivamente da avaliação do consultor de segurança, faz-se

necessário o envolvimento dos criadores, gestores, curadores e usuários da informação. Estes devem estar habilitados a responder aos seguintes questionamentos.

A. Qual a utilidade da informação ?

Aparentemente simples, a resposta para esta pergunta deve ser consolidada base a uma visão holística - a informação é parte de um todo muitas vezes indecomponível. A informação que suporta o departamento comercial tem diferente utilidade quando confrontada com as informações provenientes da engenharia. Quando justificar utilidade, lembre sempre dos fins: suporte, operação, estratégia, etc.

B. Qual o valor da informação ?

Existem diferentes métodos para a valoração da informação. São abordagens qualitativas, quantitativas e mistas; algumas compostas de cálculos e fórmulas herméticas - por vezes tão confusas que causam suspeita aos homens de espírito prático. Acredito que tão ou mais eficiente que o aparato analítico informatizado seja a avaliação pessoal do dono da informação. Ele saberá qualificar sua munição: qual o prejuízo caso esta informação seja revelada ou comprometida? Caso haja dificuldade em compor o resultado através de um indicador financeiro preciso, vale também a descrição através de escalas de classificação.

C. Qual a validade da informação ?

Salvo exceções justificadas, toda informação deve possuir um período de validade - manter informações desatualizadas, redundantes ou de integridade duvidosa, quando não por imposição legal, significa espaço em disco, leia-se “custo adicional”.

D. Quem é responsável pela manutenção da classificação da informação ?

Em algumas organizações, o criador da informação é responsável pela sua classificação inicial nos quesitos da tríade da segurança - confidencialidade, integridade e disponibilidade. Esta classificação deve ser acompanhada pela definição de grupos, perfis ou usuários individuais com permissão para o acesso.

Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de grande parte das organizações, esta deve ser tratada como tal, sendo protegida nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade, seguindo a linha adotada pelo Governo Federal.

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

De ataques de hackers a epidemias de vírus, sobrecarga de sistemas a utilização indevida por parte dos funcionários, uma variedade de ameaças exige uma abordagem sistemática para identificar, quantificar, tratar e monitorar os riscos a que o negócio está sujeito.

Como analisar riscos sem estudar minuciosamente os processos de negócio que sustentam sua organização? Como classificar o risco destes processos sem antes avaliar as vulnerabilidades dos componentes de tecnologia relacionados a cada processo? Quais são os seus processos críticos? Aqueles que sustentam a área comercial, a área financeira ou a produção? Você saberia avaliar quantitativamente qual a importância do seu servidor de web? Para cada pergunta, uma mesma resposta: **conhecer para proteger**.

Vale a pena proteger tudo ?

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. É um jogo que não pára. A cada novo investimento as empresas devem tornar os resultados palpáveis, expressando-os em números.

Mas como fazer isso? 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.

É preciso conhecimento do negócio para definir o modelo que melhor se adapte a cada situação. Conhecimento do negócio – este é o ponto chave de qualquer Gerenciamento de Riscos.

Proteger contra o quê ?

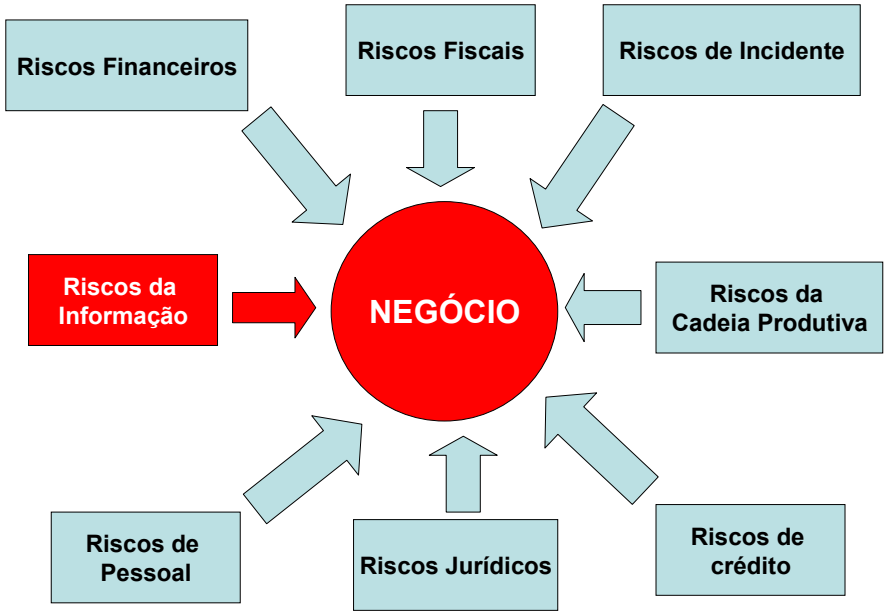
O objetivo da segurança da informação é protegê-la contra riscos. Em linhas gerais, riscos são eventos ou condições que podem ocorrer e, caso realmente ocorram, podem trazer impactos negativos para um determinado ativo (no caso, a informação).

Como pode ser percebida através da leitura da afirmação acima, a incerteza é a questão central do risco. Estamos trabalhando com hipóteses: a probabilidade de ocorrência de uma situação e o grau do dano (severidade) decorrente de sua concretização.

Mas vamos a questões mais práticas: uma vez quantificado o valor de uma informação, devem ser levantados os meios em que esta se encontra, tanto armazenado quanto em trânsito, e delimitado o escopo de atuação. Escopos infinitos caracterizam um dos erros mais comuns cometidos durante

um Gerenciamento de Riscos.

Cabe aqui a ressalva de que nosso objetivo é proteger a informação, não o ativo que a contém. De que adianta investir na proteção de um servidor de rede, por exemplo, que não armazena nenhuma informação crítica ao negócio? Os esforços devem ser concentrados no que realmente é significativo para a empresa.



Mas como proteger uma informação ?

Inicialmente, faz-se necessário uma definição do que seja Gerenciamento de Riscos propriamente dito. Este é um processo que objetiva identificar os riscos ao negócio de uma empresa e, a partir de critérios de priorização, tomar ações que minimizem seus efeitos. É caracterizado, sobretudo, por ter uma abordagem mais estruturada e científica.É dividido em 4 (quatro) etapas básicas:

1. Identificação dos Riscos: Como o próprio nome já diz, nessa etapa são identificados os riscos a que o negócio (o foco sempre deve ser este) está sujeito.

O primeiro passo é a realização de uma Análise de Riscos, que pode ser tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – quanto qualitativa – baseada em know-how, geralmente realizada por especialistas, que têm profundos conhecimentos sobre o assunto.

Devido a sua agilidade, geralmente as empresas tendem a adotar os

modelos qualitativos, que não requer cálculos complexos. Independentemente do método adotado, uma Análise de Riscos deve contemplar algumas atividades, como o levantamento de ativos a serem analisadas, definições de uma lista de ameaças e identificação de vulnerabilidades nos ativos.

2. Quantificação dos Riscos: Nessa etapa é mensurado o impacto que um determinado risco pode causar ao negócio.

Como é praticamente impossível oferecer proteção total contra todas as ameaças existentes, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços e os gastos com segurança.

Uma das ferramentas existentes no mercado é o BIA, do inglês *Business Impact Analysys*. Esta técnica consiste, basicamente, da estimativa de prejuízos financeiros decorrentes da paralisação de um serviço.

Você é capaz de responder quanto sua empresa deixaria de arrecadar caso um sistema estivesse indisponível durante 2 horas? O objetivo do BIA é responder questões desse tipo.

3. Tratamento dos Riscos: Uma vez que os riscos foram identificados e a organização definiu quais serão tratados, as medidas de segurança devem ser de fato implementadas.

Definições de quais riscos serão tratadas ? Isso mesmo. O ROI e o BIA servem justamente para auxiliar nesta tarefa. Alguns riscos podem ser eliminados, outros reduzidos ou até mesmo aceitos pela empresa, tendo sempre a situação escolhida documentada. Só não é permitido ignorá-los.

Nessa etapa ainda podem ser definidas medidas adicionais de segurança, como os Planos de Continuidade dos Negócios – que visam manter em funcionamento os serviços de missão-crítica, essenciais ao negócio da empresa, em situações emergenciais – e *Response Teams* – que possibilitam a detecção e avaliação dos riscos em tempo real, permitindo que as providências cabíveis sejam tomadas rapidamente.

4. Monitoração dos Riscos: O Gerenciamento de Riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes.

Mas como realizar uma monitoração de segurança? O ideal é que este trabalho seja norteado por um modelo de Gestão de Segurança, que defina atribuições, responsabilidades e fluxos de comunicação interdepartamentais. Só que a realidade costuma ser bem diferente... Não são todas as empresas que possuem uma estrutura própria para tratar a segurança de suas informações.

Então a monitoração de riscos pode ocorrer numa forma mais *light*,

digamos. Não é necessário todo o formalismo de uma estrutura específica, mas devem ser realizadas algumas atividades importantes, tais como:

- Elaboração de uma política de segurança, composta por diretrizes, normas, procedimentos e instruções, indicando como deve ser realizado o trabalho, e
- Auditoria de segurança, a fim de assegurar o cumprimento dos padrões definidos e, conseqüentemente, medir a eficácia da estratégia de segurança adotada.

Um efetivo gerenciamento de riscos necessita de alguns requisitos básicos que devem ser de conhecimento de todos os envolvidos nesse assunto. Esse conhecimento, inclusive, é uma outra dificuldade a ser vencida. Normalmente apenas algumas pessoas ficam sabendo do processo de gerenciamento de riscos. O desejável é que todos os envolvidos tenham acesso às informações desse gerenciamento, considerando, evidentemente, a questão da confidencialidade da informação: acesso parcial, acesso somente de leitura, acesso para atualização, etc... Neste caso o uso de uma ferramenta adequada e com inteligência para tratar todas as informações geradas é fundamental.

Como requisitos básicos para o gerenciamento de riscos, consideramos que devam existir:

Objetivos de negócio – Antes de qualquer análise de riscos, devem existir os objetivos de negócio relativos à organização ou à área organizacional em estudo. Somente podemos falar em riscos, se existem os objetivos de negócio. Cada objetivo deve ser o mais explícito possível. "Crescer o faturamento em 15% em relação ao ano passado" é muito melhor do que um genérico "aumentar o faturamento". "Garantir um tempo de resposta no ambiente computacional de no máximo três segundos" é muito melhor do que "ter um tempo de resposta que deixe o usuário satisfeito".

Riscos – Para cada objetivo de negócio definido, devem ser identificados os riscos que podem impedir que esse objetivo seja alcançado. Em uma primeira análise pode se fazer uma listagem completa de todos os riscos possíveis e imagináveis. Depois podem ser selecionados os riscos mais significativos para que o trabalho de gerenciamento de risco tenha um custo / benefício adequado.

Ações – Para cada risco selecionado e definido como significante para o processo de gerenciamento de riscos, devemos identificar ações que possam minimizar a ocorrência desse risco. Essas ações podem já existir ou não.

Na medida em que esses elementos forem sendo identificados em um número crescente, temos a necessidade de avaliar a prioridade e importância de todo esse material. Mas, que parâmetros devemos tomar por base ? Quais as avaliações que devemos fazer ? Para cada um dos elementos sugerimos que sejam analisados:

- Importância para o negócio – Cada objetivo deve ser avaliado sobre a sua importância para o negócio da organização.
- Probabilidade de ocorrência – Os riscos devem ser analisados sob a probabilidade de sua ocorrência. Impacto no negócio – Cada ocorrência de risco traz impactos diferentes para o negócio da organização. Identificar o grau desse impacto será um dado importante para a priorização desse processo.
- Grau de minimização do risco – As ações definidas para minimizar um risco possuem um grau de eficácia. Quanto mais eficazes forem, maior o poder de minimização do risco.
- Esforço a ser gasto – O esforço associado para que a ação possua uma boa eficácia é um parâmetro a ser considerado. Muito esforço em ações que minimizem riscos de pequeno impacto no negócio significa um ponto de atenção.

Para se chegar aos valores desses parâmetros a serem julgadas, as organizações necessita de um processo que expresse verdadeiramente a avaliação das pessoas envolvidas. Este processo pode ser desde um simples questionário até sessões de trabalho conduzidas por facilitadores e com apoio de softwares de decisão de grupo.

Muitos erros podem ser cometidos nesse processo de gerenciamento de riscos. Uma forma de minimizar esses erros é considerar como fatores críticos de sucesso:

- A definição do escopo da área a ser trabalhada;
- A definição explícita dos objetivos de negócio;
- A existência de uma abordagem metodológica;
- O acesso à informação por todos os envolvidos.

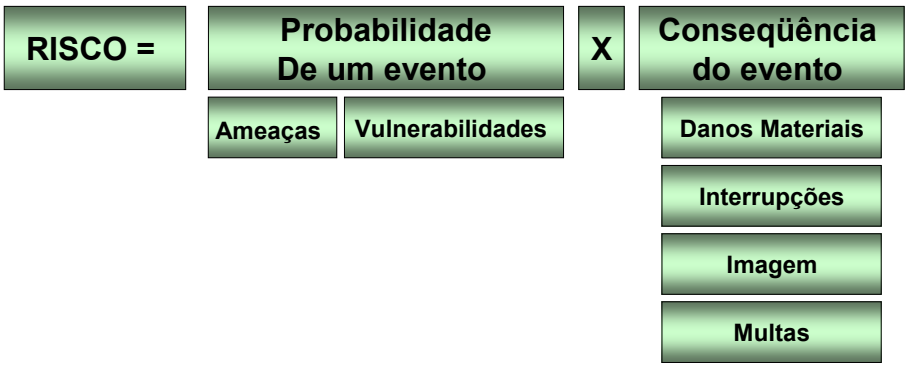
A Análise

A análise de risco consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios.

Através da aplicação deste processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela organização. Proporciona também informações para que se possa identificar o tamanho e o tipo de investimento necessário de forma antecipada aos impactos na Organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio. Sem um processo como este não são possíveis identificar a origem das vulnerabilidades, nem visualizar os riscos.

Utiliza-se como métrica as melhores práticas de segurança da

informação do mercado, apontadas na norma ISO/IEC 17799. A partir destas informações faz-se possível à elaboração do perfil de risco, que segue a fórmula: (Ameaça) x (Vulnerabilidade) x (Valor do Ativo) = RISCO. Atenção: a ISO/IEC 17799 não ensina a analisar o risco, serve apenas como referência normativa.



A - Por que fazer uma análise de risco ?

Durante o planejamento do futuro da empresa, a Alta Administração deve garantir que todos os cuidados foram tomados para que seus planos se concretizem. A formalização de uma Análise de Risco provê um documento indicador de que este cuidado foi observado. O resultado da Análise de Risco dá à organização o controle sobre seu próprio destino – através do relatório final, pode-se identificar quais controles devem ser implementados em curto, médio e longo prazo. Há então uma relação de valor; ativos serão protegidos com investimentos adequados ao seu valor e ao seu risco.

B - Quando fazer uma análise de riscos ?

Uma análise de riscos deve ser realizada — sempre — antecedendo um investimento. Antes de a organização iniciar um projeto, um novo processo de negócio, o desenvolvimento de uma ferramenta ou até mesmo uma relação de parceria, deve-se mapear, identificar e assegurar os requisitos do negócio. Em situações onde a organização nunca realizou uma Análise de Risco, recomendamos uma validação de toda a estrutura.

C - Quem deve participar da análise de riscos ?

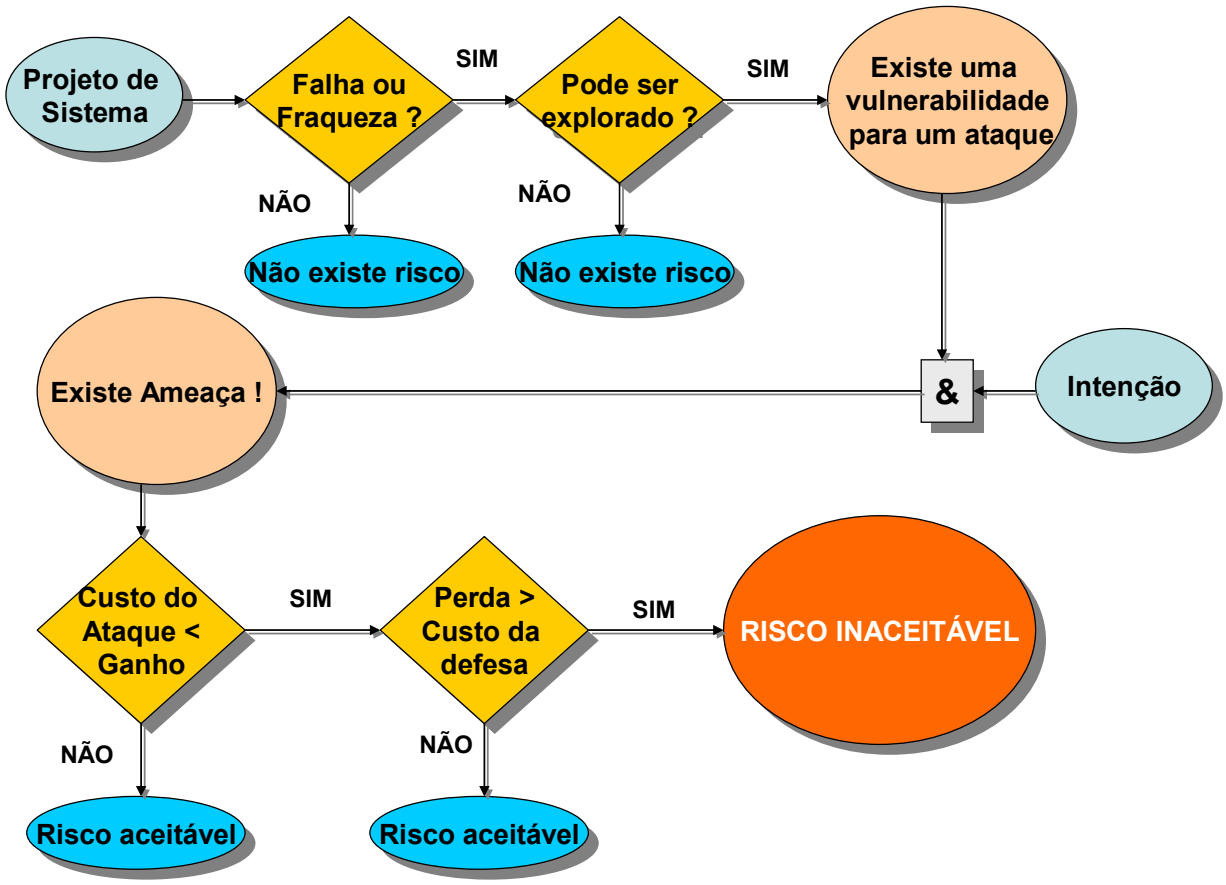
O processo de análise de riscos deve envolver especialistas em análise de riscos e especialistas no negócio da empresa — esta sinergia possibilita o foco e a qualidade do projeto. Um projeto de Análise de Risco sem o

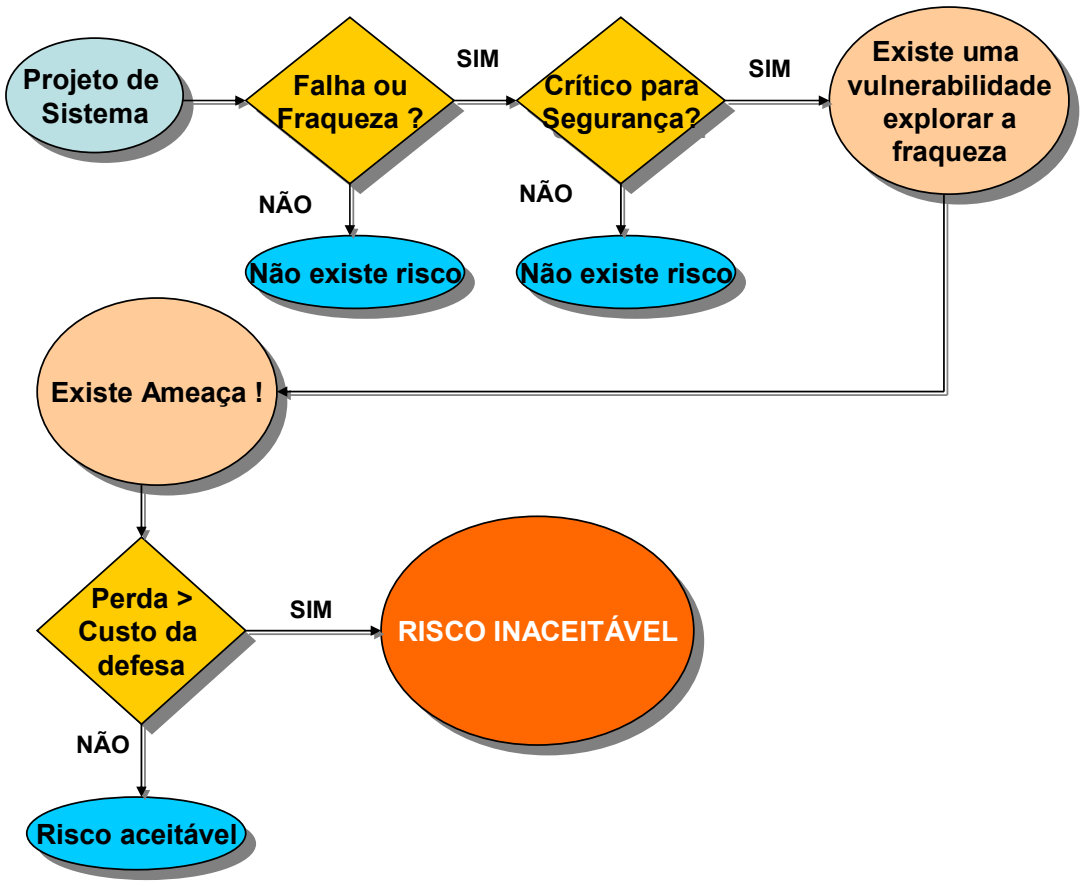
envolvimento da equipe da empresa, muito dificilmente retratará a real situação da operação.

D - Quanto tempo o projeto deve levar ?

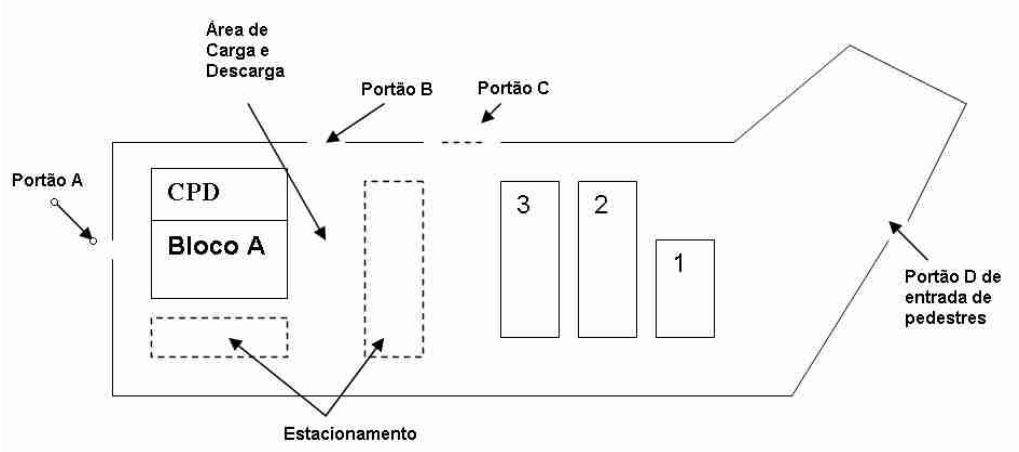
A execução do projeto deve ser realizada em tempo mínimo. Em ambientes dinâmicos a tecnologia muda muito rapidamente. Um projeto com mais de um mês — em determinados ambientes —, ao final, pode estar desatualizado e não corresponder ao estado atual da organização.

Conforme (Stoneburner, 2001), a forma para descobrir se existe algum risco em um projeto e se o mesmo é aceitável, é apresentada na próxima figura:





Estudo de Caso



Descrição:
O desenho acima mostra o site de uma empresa que abrigará um novo CPD.
O terreno é cercado por grades (aprox. 2 metros), com 4 portões:
Portão A: entrada para o bloco A
Portão B: entrada de funcionários e de caminhões para carga e descarga
Portão C: atualmente desativado (portão grande)
Portão D: entrada de pedestres(portão pequeno)

O terreno contém 4 construções:

Bloco A:
No subsolo, há 3 depósitos distintos:
1. papelaria e material de expediente;
2. móveis usados;
3. equipamentos de informática reutilizável.

No térreo funcionam uma gráfica, um estoque de atacado e a rampa de carga e descarga.
No primeiro andar funcionará o CPD e um novo setor com um grande volume de cheques. Separados do CPD por uma parede corta-fogo estarão a gráfica plana, o escritório e o laboratório da gráfica, que contém materiais altamente inflamáveis.

Existem 2 entradas para o CPD. A principal, pelo portão A e uma outra pela área de carga e descarga.

Pavilhão 1: documentos de microfilmagem e papéis
Pavilhão 2: Setorial de transporte, estoque de papel da gráfica e lanchonete
Pavilhão 3: móveis e equipamentos obsoletos

Tendo em vista a segurança física:

1. Quais são os riscos com relação a acesso, incêndio, inundação, etc?
2. Quais ações/soluções vocês recomendariam?

CAPÍTULO X

Contingência ou Plano de Continuidade de Negócios

Num mundo de negócios competitivo como o de hoje, as empresas simplesmente não podem mais ficar indisponível para seus clientes mesmo que tenham problemas com seus processos de negócios, recursos e / ou dados e informações. Velocidade de processamento e de decisões, altíssima disponibilidade, flexibilidade e foco em produtos de acordo com o mercado são requisitos fundamentais para "sobrevivência e sucesso". Porém, se não houver Planejamento para Segurança e Contingência adequados, alguns ou até todos requisitos estarão ameaçados e, conseqüentemente, a empresa ameaçada.

Definições

- **Plano de Contingência** – Um plano para a resposta de emergência, operações backup, e recuperação de após um desastre em um sistema como a parte de um programa da segurança para assegurar a disponibilidade de recursos de sistema críticos e para facilitar a continuidade das operações durante uma crise.

- **Disponibilidade** – A propriedade que e um sistema ou um recurso de sistema de estarem acessíveis e utilizáveis sob demanda por uma entidade autorizada pelo o sistema, de acordo com especificações de desempenho projetadas para o sistema; isto é, um sistema que está disponível para fornecer serviços de acordo com o projeto do sistema sempre que pedido por seu usuário.

- **Confiabilidade** – A habilidade de um sistema de executar uma função requerida sob condições indicadas por um período de tempo especificado.

- **Sobrevivência** - A habilidade de um sistema de continuar em operação ou existindo apesar das condições adversas, inclui as ocorrências naturais, ações acidentais, e ataques ao sistema.

Conceitos[10]

Diferentemente do que se pensava há alguns anos sobre definição de Continuidade de Negócio, quando o conceito estava associado à sobrevivência das empresas – principalmente através das suas estratégias comerciais, redução de custos com produtividade e fortalecimento da marca –, observa-se atualmente uma mudança que cria um novo conceito associado a um modelo de gestão mais abrangente, onde todos os componentes e processos essenciais ao negócio tenham os seus risco de inoperância ou paralisação minimizadas por Planos de Continuidade de Negócios atualizados,

[10] (Plachta, 2001)

documentados e divulgados corretamente.

Na época em que o antigo conceito era usado, todas as preocupações referentes a inoperabilidade dos componentes (sejam estes de suporte à tecnologia ou aos processos) eram tratadas isoladamente por cada gestor ou técnico responsável que, como não possuíam uma visualização necessária de todas as interdependências existentes, não orientavam a implementação às atividades fins da empresa.

Em um primeiro momento imagina-se que Planos de Continuidade visam permitir que os negócios sejam mantidos da mesma forma durante o regime de contingência. Este tipo de raciocínio é restrito. O que devemos levar em conta é "o que é que nossos clientes precisam ?" E assim considerar "a continuidade de que serviços (ou da oferta de que produtos) nossos clientes esperam de nós ?".

Seria necessário então criar uma solução onde todas as áreas pudessem ter uma visão global dos seus inter-relacionamentos e, com isto seria possível definir critérios referentes ao custo de recuperação, de inoperância ou de impacto refletidos na atividade fim da empresa.

Quando se enumerava os grandes vilões responsáveis pela indisponibilidade e o caos nas empresas, pensava-se em desastres como as ameaças naturais, terremotos, inundações e outros similares. Porém, estes fatores perderam terreno para as vulnerabilidades herdadas pelas empresas em decorrência do aumento desenfreado, e necessárias, das novas tecnologias.

Com isso, o **conceito de desastre**, antes atrelado ao caos gerado por fatores naturais, vem sendo substituído pelo **conceito de evento**, que é a concretização de uma ameaça previamente identificada, podendo ser seguido ou não de um desastre.

Por exemplo, o recebimento de um vírus por um usuário de e-mail identifica-se como um evento até que o programa seja executado, resultando na perda de dados, o que seria um desastre, considerando o valor das informações atingidas.

Nos dias de hoje, após os atentados nos Estados Unidos, intensifica-se um conceito de estado de alerta para o Plano de Continuidade de Negócios denominado Plano de Administração de Crise, onde todas as medidas para o estado de vigilância e ações de resposta emergenciais devem estar documentadas e destinadas às equipes de plantão responsáveis pela sua execução.

Através destas medidas, observamos cada vez mais que a continuidade dos processos e negócios está atrelada não somente à recuperação ou ao contingenciamento dos processos vitais, mas também à vigilância contínua dos eventos.

Sendo assim, quando é possível a identificação imediata da probabilidade da ocorrência de um evento que ocasionará a indisponibilidade de um processo crítico ou vital, este deverá ser tratado como uma situação de crise – aplicando-se o plano de controle e administração para a redução do risco desta ocorrência.

Justificando

Mesmo sem ter planos formais de contingência, através dos questionamentos abaixo um alto executivo pode saber se a sua organização está preparada para o inevitável:

- Quais são os principais negócios da minha empresa ?
- Quais são os fatores de risco operacionais que podem afetar seriamente os negócios da empresa ?
- Qual seria o impacto nas receitas geradas pelo negócios da empresa se um ou mais fatores de risco se manifestasse ?
- Como a empresa está preparada para lidar com o inevitável ou o inesperado ?

Para cada questão não respondida ou respondida insatisfatoriamente, cresce a vulnerabilidade da empresa frente a fatos cuja ocorrência esteja fora de seu controle, sendo a ponderação dessa vulnerabilidade maior quanto maior a ordem da questão não respondida.

Estratégias de Contingência[11]

- **Estratégia de Contingência Host-site** – Recebe este nome por ser uma estratégia "quente" ou pronta para entrar em operação assim que uma situação de risco ocorrer. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto. Se a aplicássemos em um equipamento tecnológico, um servidor de banco de dados, por exemplo, estaríamos falando de milessegundos de tolerância para garantir a disponibilidade do serviço mantido pelo equipamento.

- **Estratégia de Contingência Warm-site** – Esta se aplica a objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade. Tomemos, como exemplo, o serviço de e-mail dependente de uma conexão. Vemos que o processo de envio e recebimento de mensagens é mais tolerante que o exemplo usado na estratégia anterior, pois poderia ficar indisponível por minutos, sem, no entanto, comprometer o serviço ou gerar impactos significativos.

- **Estratégia de Contingência Cold-site** – Dentro do modelo de classificação

[11] (Sêmola, 2003)

nas estratégias anteriores, esta propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infra-estrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto, aplicável à situação com tolerância de indisponibilidade ainda maior.

- **Estratégia de Contingência de Realocação de Operação** – Como o próprio nome denuncia, esta estratégia objetiva desviar a atividade atingida pelo evento que provocou a quebra de segurança, para outro ambiente físico, equipamento ou link, pertencentes à mesma empresa. Esta estratégia só é possível com a existência de "folgas" de recursos que podem ser alocados em situações de crise. Muito comum essa estratégia pode ser entendida pelo exemplo que se redireciona o tráfego de dados de um roteador ou servidos com problemas para outro que possua folga de processamento e suporte o acúmulo de tarefas.

- **Estratégia de Contingência Bureau de Serviços** – Considera a possibilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado; portanto, fora dos domínios da empresa. Por sua própria natureza, em que requer um tempo de tolerância maior em função do tempo de reativação operacional da atividade, torna-se restrita a poucas situações. O fato de ter suas informações manuseadas por terceiros e em um ambiente fora de seu controle, requer atenção na adoção de procedimentos, critérios e mecanismos de controle que garantam condições de segurança adequadas à relevância e criticidade da atividade contingenciada.

- **Estratégia de Contingência Acordo de Reciprocidade** – Muito conveniente para atividades que demandariam investimentos de contingência inviáveis ou incompatíveis com a importância da mesma, esta estratégia propõe a aproximação e um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes a sua, e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional. Estabelecem em conjunto as situações de contingência e definem os procedimentos de compartilhamento de recursos para alocar a atividade atingida no ambiente da outra empresa. Desta forma, ambas obtêm redução significativa dos investimentos. Apesar do notório benefício, todas as empresas envolvidas precisam adotar procedimentos personalizados e mecanismos que reduzam a exposição das informações que, temporariamente, estarão circulando em ambiente de terceiros. Este risco se agrava quando a reciprocidade ocorre entre empresas pseudoconcorrentes que se unem exclusivamente com o propósito de reduzir investimentos, precisando fazê-lo pela especificidade de suas atividades, como por exemplo, no processo de impressão de jornais.

- **Estratégia de Contingência Auto-suficiência** – Aparentemente uma estratégia impensada, a auto-suficiência é, muitas vezes, a melhor ou única estratégia possível para determinada atividade. Isso ocorre quando

nenhuma outra estratégia é aplicável, quando os impactos possíveis não são significativos ou quando estas são inviáveis, seja financeiramente, tecnicamente ou estrategicamente. A escolha de qualquer uma das estratégias estudadas até o momento depende diretamente do nível de tolerância que a empresa pode suportar e ainda depende do nível de risco que seu executivo está disposto a correr. Esta decisão pressupõe a orientação obtida por uma análise de riscos e impactos que gere subsídios para apoiar a escolha mais acertada.

Planos de Contingência

São desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencentes ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência. É acertadamente subdividido em três módulos distintos e complementares que tratam especificamente de cada momento vivido pela empresa.

- **Plano de Administração de Crise** – Este documento tem o propósito de definir passo-a-passo o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano.

- **Plano de Continuidade Operacional** – Tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, conseqüentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à Internet, exemplificam os desafios organizados pelo plano.

- **Plano de Recuperação de Desastres** – Tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processo de negócio, a fim de restabelecer o ambiente e as condições originais de operação.

É fator crítico de sucesso estabelecer adequadamente os gatilhos de acionamento para cada plano de contingência. Estes gatilhos de são parâmetros de tolerância usados para sinalizar o início da operacionalização da contingência, evitando acionamentos prematuros ou tardios. Dependendo das características do objeto da contingência, os parâmetros podem ser: percentual de recurso afetado, quantidade de recursos afetados, tempo de indisponibilidade, impactos financeiros, etc.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Principais fases de elaboração do Plano de Contingência Corporativo

O Plano de Contingência Corporativo provê a avaliação de todas as funções de negócio, juntamente com a análise do ambiente de negócios em que a empresa se insere, ganhando-se uma visão objetiva dos riscos que ameaçam a organização. Com o Plano de Contingência, ela poderá se assegurar de que possui o instrumental e treinamento necessários para evitar que interrupções mais sérias em sua infra-estrutura operacional possam afetar sua saúde financeira.

A metodologia do Programa do Plano de Contingência consiste de 6 passos:

1 Avaliação do projeto: escopo e aplicabilidade;
2 Análise de risco;
3 Análise de impacto em negócios;
4 Desenvolvimento dos planos de recuperação de desastres;
5 Treinamento e teste dos planos;
6 Implementação e manutenção;

Riscos Envolvidos

São vários os riscos envolvidos na criação e análise de um Plano de Contingência. Observe a figura abaixo.

Mais Informações

O NIST – *National Institute of Standards and Technology* (http://www.nist.gov/) criou um documento intitulado *Contingency Planning Guide for Information Technology Systems* que demonstra os conceitos já explicados aqui e métodos / exemplos de como aplicar e realizar um Plano de Continuidade de Negócios.

Estudo de Caso

Os desastres acontecidos não envolvem computação. Entretanto, eles testaram o gerenciamento e ambos os negócios teriam se convertido em grandes perdas caso os mesmos não tivessem sido administrados efetivamente.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005

Caso Tylenol:estudo de caso.

A única coisa necessária para que o mal triunfe é a de que homens de bem não façam nada.
Edmund Burke

A humanidade não consegue tolerar muito a realidade.
T. S. Eliot

ADULTERAÇÃO, O MAL VINDO DE FORA: O CASO TYLENOL

Talvez, nem um outro caso recente tenha um impacto tão grande como a grande tragédia ocorrida com os eventos associados ao Tylenol. Um artigo publicado na conhecida revista de negócios Forbes revela um lado sinistro do caso como um todo. Uma premonição funesta estava no ar antes que os atos hediondos que logo seriam associados ao Tylenol tivessem ocorrido. No começo de setembro de 1982, no retiro estratégico de planejamento de três dias da Johnson e Johnson, a empresa controladora da McNeil, o Presidente da J & J's James Burke meditou sobre como tinham sorte em estarem numa indústria que tinha tantas marcas extremamente lucrativas. Entretanto, ele refletiu em voz alta, "E se algo acontecesse a um deles [aos seus principais produtos], como o Tylenol?" "Nada," ele observou, "é impenetrável." Ninguém poderia aparecer com algo que poderia diminuir o ímpeto do que parecia ser um negócio extremamente bem sucedido, mas Burke "riu de si mesmo...por estar se preocupando com coisas as quais ele não tinha por que se preocupar."

Então o impensável aconteceu.

No dia 29 de setembro de 1982, dois irmãos, Adam e Steven Janus, e Mary Kelleran, de dois diferentes subúrbios fora de Chicago, morreram por terem tomado cápsulas de Tylenol Extra-Forte. Um veneno mortal, cianeto, havia sido injetado nas cápsulas. Um dia depois, Mary Reiner e Mary McFarland , também dos subúrbios de Chicago, morreriam de envenenamento por cianeto. Tylenol fora identificado como o culpado em todos os casos. Mais especificamente, as cápsulas venenosas foram rastreadas até o número do lote 1910 MD e MC 2738. O pior havia acontecido. Não só Tylenol havia sido envenenado mas o desastre tinha sido ampliado a diversos lotes. Ninguém sabia como diversos lotes diferentes haviam sido infectados.

J & J reagiu prontamente. Todos os 93.400 frascos do lote número MC 2880 foram imediamente recolhidos. Um dia depois todos os 171.000 frascos do lote número 1910 MD foram também recolhidos.

Em 4 de outubro de 1982, o FDA (Federal Drug Administration, o órgão americano responsável pelo controle de remédios) ordenou que seus 19 laboratórios começassem a testar as cápsulas de Tylenol Extra-Forte. As cápsulas foram recolhidas numa amostra aleatória das prateleiras em todo o país.

Naquele mesmo dia, a viuva de Adam Janus entrou com uma ação de $15 milhões de dólares por danos contra a J & J. Duas outras ações foram movidas mais tarde no valor de $ 35 milhões. Porém a mais grave de todas, uma quarta ação estava para ser movida exigindo a restituição a qualquer pessoa no país que houvesse comprado Tylenol naquele ano! As estimativas de custos potenciais daquela ação chegavam a $ 600 milhões.

Em 5 de outubro, no dia seguinte, o envenenamento havia se espalhado por toda a nação. Três frascos de Tylenol Extra-Forte contendo uma quantidade de estriquinina foram achados em Oroville, Califórnia.

Em 6 de outubro, J & J enviou mensagens via telex para aproximadamente 15,000 revendedores e distribuidores. As mensagens pediam para que eles removessem todos os 11 milhões de frascos do Tylenol normal e do Extra-Forte de suas prateleiras.

O custo inicial para a J & J foi calculado em mais do que dólares simplesmente. A tragédia cobrou o seu preço em impacto psicológico do mesmo modo que o fizera em dólares. Isto afetou a confiança e a segurança que os executivos da J & J tinham em seus próprios produtos do mesmo modo que afetou o público. A melhor analogia é a de que para os executivos da J & J e da McNeil fora como se alguém da família houvesse morrido. A essência, o alicerce, do negócio de analgésicos foram construídos sobre uma palavra chave: confiança. As pessoas tomavam Tylenol porque era recomendado por médicos ou porque lhes fora dado em hospitais. Elas o tomavam porque, nas palavras de Burke, "elas não estavam bem e estavam num estado altamente emotivo." As perguntas agora, segundo o autor do artigo publicado na Forbes, Thomas More, colocara, eram: se a emotividade fora responsável pela ingestão inicial de Tylenol e a subsequente identificação da marca com este fato, aquelas mesmas emoções se voltariam contra Tylenol porque as pessoas não arriscariam com um produto cujo nome fora carregado emocionalmente de maneira negativa? Se o nome Tylenol fora inicialmente associado com a epítome da desconfiança e do mal? Quem culparia o público por não estar disposto a dar uma nova chance?

Mesmo que o dólar não fosse suficiente para calcular o impacto total de tal tragédia, a quantidade era impressionante de qualquer modo. Esta quantidade era tudo menos desprezível ou trivial. Em 1975, a McNeil começou a promover o Tylenol agressivamente como uma alternativa de analgésico para aqueles que sofriam do estômago ou de outros efeitos colaterais da aspirina. Em 1982, Tylenol tinha 35% do mercado de $ 1 bilhão de dólares do analgésico. Como uma prova da significância de Tylenol para a J & J, ele representava uma estimativa de 7% das vendas mundiais e algo em 15% ou 20% de seus lucros totais em 1981. Antes dos envenenamentos, os executivos da McNeil previam confiantemente que Tylenol obteria 50% do mercado, ou mais, até 1986.

Em suma, J & J recolheu uns 31 milhões de frascos com um valor de revenda de mais de $ 100 milhões. Como resultado, os seus ganhos do terceiro quadrimestre caíram de 78 centavos a ação em 1981 para 51 centavos em 1982. Os analistas de segurança projetaram uma queda de 70% em $ 100 milhões em vendas de balcão dos produtos Tylenol no quarto quadrimestre. Em 1983, previa-se que o Tylenol obteria meio bilhão de dólares em vendas. Depois da tragédia, os analistas previram que J & J teria sorte se ganhasse metade disto.

A tragédia do Tylenol é o nosso primeiro e talvez mais proeminente exemplo do tipo de ato trágico impensável que pode acontecer a qualquer organização. Um produto (ou serviço) central, de suporte do qual a organização obtém uma quantia significante de sua renda e razão pela qual o público tem um reconhecimento e lealdade consideráveis em relação à marca, foi criado

para fazer o bem. As propriedades do produto (serviço) então são alteradas, de maneira drástica, pela injeção de substâncias estranhas. O produto (serviço) é então convertido em um agente para se fazer mal a seus consumidores insuspeitos. Como resultado, tanto os consumidores como os fabricantes do produto (serviço) sofrem uma perda considerável. Toda organização agora está vulnerável a este tipo de perda, tragédia, e ameaça.

Quando dizemos que este tipo de coisa é impensável, nós o fazemos em dois sentidos distintos. Um, é inacreditável -totalmente impensável- que alguém poderia de fato perpetrar tal ato contra outros seres humanos. A maioria de nós acha difícil imaginar que tipo de mente realmente poderia fazer tais coisas. Não está além de nossa imaginação pensar em atos violentos. Na verdade nós o fazemos a todo o momento sem estar plenamente consciente. Porém estaria além da normalidade se nossos impulsos violentos cruzassem a barreira, não importando quão frágil que ela possa ser, da mera fantasia para a sua atuação de fato.

Dois, além de medidas preventivas de embalagem, é difícil se não impossível saber-se o que alguém poderia ter feito anteriormente para prever tais tragédias. Numa nação de aproximadamente 226.500.000 de pessoas, parece ser claramente impossível prever quais indivíduos fariam tal coisa a ponto de se poder isolá-los e determinar sua exata localização e momento de atacar.

Em ambos relatos nós nos sentimos totalmente bloqueados. Nos sentimos desamparados, à mercê de um ambiente incontrolável e imprevisível. Como um autor escrevera comentando sobre o que a tragédia do Tylenol significou para ele: "Um homem na Califórnia ameaçou envenenar potes de picles nas lojas Safeway (modo seguro, em inglês) a menos que recebesse uma enorme quantia de dinheiro.

Na verdade, a mim parece um pouco assustador viver num mundo onde sequer potes de picles sejam seguros...."

A crise do Tylenol em 1982 é vista como um caso clássico de neutralização eficiente de crise. O sucesso da Johnson e Johnson é principalmente atribuído a sua resposta rápida e as suas ações, sua agressividade, suas extensas e eficientes relações públicas e à campanha na mídia, sua abertura, e sua disposição em divulgar informações relacionadas à crise para o público. A repetição da crise em fevereiro de 1986 certamente não mudou a sua imagem. A experiência de 1986 foi caracterizada pelas mesmas qualidades básicas; J&J foi rápida, agressiva, e aberta.

Uma crise é uma situação fora da situação normal. As condições da crise podem evocar uma decisão de se fazer uma substituição total da diretoria por uma nova equipe, que poderia trazer uma nova perspectiva e um novo quadro. O argumento é o de que os executivos atuais são arquitetos das práticas e políticas existentes, defensores do status quo, e conseqüentemente relutantes em iniciar e instituir o tipo de mudanças necessárias para o controle efetivo da crise. Obviamente, soluções extremas talvez não sejam necessárias. No entanto, uma crise cria uma nova situação que não pode ser trabalhada com normas antigas.

A urgência de uma resposta rápida é também uma característica da maioria das situações críticas. Uma crise é uma situação crítica e sensível que uma vez sendo negligenciada ou tratada inadequadamente, pode causar o colapso de toda a organização, pois o tempo disponível para formular e implantar uma resposta é geralmente limitado. Uma situação de crise apresenta um dilema. A resposta tem de ser sonora e efetiva bem como rápida e vigorosa. No caso do Tylenol contaminado, acredita-se que a resposta rápida e agressiva da J&J tenha sido significante para a solução da crise, para se re-adquirir o mercado perdido, e para o fortalecimento da credibilidade da companhia junto aos consumidores. Diferentemente, em setembro de 1985 quando a rede estatal canadense de rádio e TV (Canadian Broadcasting Corporation) acusou a subsidiária canadense da Star-Kist Foods, Inc. de enviar exportar um milhão de latas de atum "rançoso e em decomposição", a companhia preferiu fazer pouco e se manter de boca fechada, assumindo que o tempo automaticamente tomaria conta do problema. As semanas seguintes a esta inatividade, causou uma queda de 90% na receita canadense da Star-Kists, prejudicou seriamente a credibilidade do público na Star-Kist Foods e na sua firma controladora H.J. Heinz Co, e colocou seriamente o futuro da Star-Kist Foods Inc em dúvida no Canadá.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Western Petroleum Transportation Inc. :Estudo de Caso

Os nomes desta companhia e dos funcionários foram mudados neste estudo de caso:estudo de caso.

PROJETO DE ORGANIZAÇÃO PARA ACIDENTES QUÍMICOS PERIGOSOS

A temperatura estava em uns 20 graus negativos em West City, fora do escritório central da Western Petroleum Transportations, Inc. A western Petroleum (WPT) opera um sistema extenso de oleodutos que transporta mais de 50 tipos de produtos petroquímicos (hidrocarbonos líquidos) dos centros de produção de West City para os mercados do leste. Em 1984, mais de 200.000 metros cúbicos por dia de hidrocarbonos foram despejados no sistema.

A WPT tem sido uma operação lucrativa, com uma renda descontada de impostos de mais de $ 100 milhões de dólares. Os dados sobre segurança da WPT também são invejáveis; em 40 anos, a WPT teve apenas um grande acidente fatal.

Nesta manhã em particular, vários membros da Equipe de Manutenção de Oleodutos da WPT estavam pintando, inspecionando equipamentos, e fazendo um inventário do terminal central da WPT na "Refinary Row" nos arredores de West City. Três membros foram enviados para a área de Three Creeks, 100 km distante do trabalho de rotina em uma estação bombeadora. Estas tarefas eram condizentes com os deveres da equipe, as quais incluíam a manutenção do oleoduto, a localização de vazamentos e de problemas, a reparação da linha, e o transporte de equipamento tanto de ida para como de vinda dos locais de trabalho.

O piloto da companhia estava no ar em um vôo de inspeção de rotina sobre a linha preferencial do oleoduto. Nesta manhã, nenhum problema fora observado e o oleoduto parecia estar intacto.

Ao meio dia, a sala de controle no terminal recebeu uma ligação telefônica de um fazendeiro de Three Creeks avisando sobre um provável vazamento de gás na área. Embora os instrumentos da controle não indicassem quaisquer irregularidades na linha, até mesmo grandes vazamentos de substâncias como gases liquefeitos naturais (GNLs) não são detectados pelos instrumentos da sala de controle. Mesmo assim todos os oleodutos paralelos da WPT foram imediatamente fechados.

O terminal ligou para Mel Ginter, o chefe de seção da equipe de manutenção para avisá-lo do vazamento suspeito. O Gerente Assistente do Distrito recebeu a ligação e notificou o Gerente do Distrito. Simultaneamente, o chefe de seção da Equipe de Manutenção chegou no escritório já sabendo da situação. Depois de informar outros membros da equipe para ficarem aguardando por outras instruções no rádio. Ginter e um membro da equipe partiu imediatamente para o local na camionete equipada com rádio de Ginter.

O Gerente e seu assistente argumentaram sobre o vazamento, ligaram para a polícia para solicitar segurança para a área do vazamento, e enviaram um avião da companhia para monitorar o vazamento. Os trabalhadores da WPT foram dirigidos para assegurar que uma válvula de fechamento corrente acima tivesse sido ativada para parar o fluxo do vazamento de produtos químicos para o segmento de linha. E o Gerente Assistente foi enviado para supervisionar o local de vazamento.

A polícia ergueu barreiras no norte e no sul, e em seguida foi dispensada pelos membros da equipe de manutenção na barreira do sul. O chefe de seção chegou na barreira do norte às 14:30 e observou que a área de vazamento era no campo de um fazendeiro, a um quilômetro da residência mais próxima e muitos quilômetros distante da cidade mais próxima.

O chefe de seção (Mr. Ginter) e um membro da equipe inspecionaram a área de vazamento. Caminhando próximo a uma coluna de gás, eles confirmaram um vazamento de gás liquefeito natural e usaram um detetor de gás para estabelecer uma localização aproximada. A localização exata seria difícil de determinar; o vazamento de gás toma o caminho de menor resistência para chegar à superfície, portanto o gás pode aparecer com uma certa distância da origem do vazamento.

De volta à camionete, Ginter se comunicou via rádio para West City para consertar o equipamento e avisou ao Gerente que uma linha estava vazando gases liquefeitos naturais. As outras duas (intactas) foram reabertas.

O Gerente Assistente chegou à barreira do norte e então começaram os contatos via rádio entre o Gerente em West City , o Assistente e o Chefe de Seção no local. A polícia fora dispensada na barreira do norte assim que os membros da equipe e equipamentos começaram a chegar mais ou menos às 15:30. A área de vazamento foi inspecionada repetidamente.

Às 16:00 o Gerente Assistente e o Chefe de Seção concordaram que eles estavam enfrentando um grande vazamento de gases liquefeitos naturais. Os gases liquefeitos naturais são uma mistura de propano, butano, e condensados levados sob pressão à temperaturas muito aquém de zero. Com uma volatilidade alta, os GLNs podem ser inflamados com uma centelha, e podem ter efeitos intoxicantes quando inalados. "A Ignição controlada" ou ignição controlada é um procedimento comum para vazamentos de GNLs e é efetuado para se evitar uma ignição não planejada de nuvens erráticas de gás durante os esforços.

O Gerente Assistente e o Chefe de Seção disseram ao gerente que "nós temos de considerar seriamente a operação de efetuar a ignição controlada". O Gerente endossou a decisão pela ignição controlada "apenas se fosse 100% segura," e propiciou a instalação de uma válvula-rolha 300 metros corrente acima do vazamento para isolar uma seção pequena da linha. Uma vez que GLNs em pouco mais de um quilômetro e meio de linha poderia valer milhões de dólares, a ignição controlada seria cara; o fogo poderia queimar por 36 horas, atrasando os reparos e destruindo condensados que poderiam ser recuperados mais tarde.

Às 17:30 o assistente e o chefe de seção concordaram em não efetuar a ignição controlada: estava escuro agora e a ignição controlada poderia ser muito perigosa devido as dificuldades de monitoramento visual da coluna de gás.

Mais membros da equipe chegaram, trazendo um sistema de iluminação usado para iluminar locais de trabalho à noite. Dois detetores de gás estavam no local, embora as suas baterias estivessem se acabando. Um trailer com o grosso do equipamento de reparo e suprimentos estava a caminho, incluindo detetores de gás, e roupas próprias para a proteção contra o efeito congelante de GNLs. A roupa protetora contra fogo não estava disponível, apesar do perigo de uma ignição não planejada.

Às 19:15, o Gerente Assistente estava só na barreira do norte e um membro da equipe estava assegurando a barreira do sul. O sistema de iluminação a diesel não dava partida na barreira do sul. Ele foi rebocado com outro equipamento para um local a umas poucas centenas de metros contra o vento a partir do vazamento onde o chefe de seção, quatro outros membros da equipe de manutenção e um funcionário contratado estavam localizados.

O sistema de iluminação finalmente "deu partida", apenas para voltar a parar. Os odores de gás e as nuvens de gás que chegavam à altura dos joelhos se moviam pela área e fizeram com que os membros da equipe ficassem mais preocupados, e às 20:20 dois trabalhadores foram desligar as máquinas de seu equipamento. De repente uma chama que tinha o tamanho de vários campos de futebol irrompeu. Um membro da equipe correu para o campo e escutou gritos dos funcionários a medida que o fogo os queimava.

O Gerente Assistente viu o fogo e tentou inutilmente estabelecer contato via rádio com a equipe. Um fazendeiro que se dirigia para a barreira do norte foi deixado para compor a barreira enquanto o assistente seguiu ao local de trabalho. Logo em seguida, o caminhão de equipamento de West City chegou à barreira do norte.

O membro da equipe que havia escapado do fogo retornou para o local de trabalho e achou outros companheiros seriamente queimados, gritando em agonia e dor. Ele correu em direção à barreira do norte e relatou os ferimentos causados ao Gerente Assistente. Eles enviaram esta mensagem via rádio para os quartéis da WPT, e então se dirigiram para ajudar os homens feridos.

Os executivos da companhia a caminho do vazamento escutaram o relatório e chamaram uma ambulância para levar os feridos a um pequeno hospital local. O fogo no oleoduto queimou descontroladamente por três dias.

Os homens feridos foram mais tarde transferidos para a unidade de queimados de um hospital importante onde o chefe de seção e um trabalhador morreram duas semanas depois. Três outros trabalhadores permaneceram hospitalizados por diversos meses.

CAPÍTULO XI

Auditoria em Informática

Introdução

O crescente uso dos computadores nas empresas bem como a sua importância estratégica, vem fazendo com que as empresas se preocupem em aumentar o controle sobre os departamentos de processamento de dados, já que estes controlam informações vitais à empresa.

Este controle é feito através de um processo de Auditoria, que visa descobrir as irregularidades em tais departamentos (caso seja feito em microcomputadores) ou nos centros de processamento da empresa. A Auditoria também identifica os pontos que irão desagradar a alta administração para que estes possam ser corrigidos.

Como no passado, a base da investigação era restrita ao setor da finanças, as empresas não viam o porquê de manter um departamento somente de auditores, preferindo contratar empresas prestadoras deste serviço. Atualmente com a proliferação do comutador, já é necessário manter um departamento de auditoria interna.

A prática deste tipo de auditoria iniciou-se nos Estados Unidos e na Europa na década de 80. Como as técnicas de processamentos e as maneiras de burlar os controles vêem evoluindo de maneira rápida, os auditores devem estar sempre atentos a tais mudanças.

A Auditoria de processamento de dados deve abranger todas as áreas de um departamento de processamento de dados:

- Coordenação de Problemas
- Coordenação de Mudanças
- Sistemas em Processamento “Batch” (em série)
- Recuperação de desastre
- Capacidade dos Sistemas
- Desempenho dos Sistemas
- Desenvolvimento de Sistemas
- Sistemas em Processamento On-Line (linha por linha)
- Sistemas Financeiros
- Rede de Telecomunicações
- Segurança de informação
- Centro de computação
- Microcomputador
- Distribuição dos Custos

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005

Perfil do Profissional Auditor em Informática

O auditor é aquela pessoa, ou departamento, que foi designado pela alta administração da empresa para avaliar, examinar e descobrir os pontos falhos e a devida eficácia dos departamentos por ela vistoriados. Logicamente auditado é aquela pessoas ou setor que sofre a investigação da auditoria.

O auditor deve ser um profissional de grande conhecimento da área de processamento de dados e todas as suas fases. Deve ter objetividade, discrição, raciocínio lógico e principalmente um sentimento real de independência, ou seja, em seus relatórios sejam eles intermediários ou finais, devem possuir personalidade e até mesmo os fatos incorretos na administração do auditado.

Posicionamento da Auditoria dentro da organização

Este setor deve ser totalmente independente dos outros setores a fim de que não tenha influências no seu desempenho. Deve estar ligado diretamente à alta administração da empresa.

Outro ponto importante é a existência de um planejamento prévio, no nível de datas, de quando e como irão ocorrer as auditorias. O sigilo deste planejamento é importante para que não hajam acertos de última hora que irão resultar em relatórios não condizentes com a realidade, prejudicando o desempenho da organização.

Importância da Auditoria e suas fases

Como já foi dito a auditoria dentro de um departamento, principalmente na área de processamento de dados, é de vital importância para empresa, já que através desta a alta administração deverá ditar os rumos da empresa, além

de evitar fraudes e garantir o bom desempenho dos setores auditados. Este processo é composto de: Pré-Auditoria, Auditoria e Pós-Auditoria.

Pré-Auditoria

Nesta fase é enviado ao departamento a ser auditado um anúncio, através de um notificação formal do setor de auditoria ou pelo setor de Controle Interno da empresa. Este anúncio deve ser feito com até duas semanas de antecedência e deverá especificar quais serão as áreas a ser auditadas, com seus respectivos planos de trabalho.

Ainda destro desta fase, serão feitas as primeiras reuniões da alta administração com os auditores visando esclarecer os pontos e planos de trabalho.

Nesta fase o grupo Auditor deve preparar as atividades administrativas necessárias para a realização da auditoria, definir as áreas a auditar, orientar o grupo de auditores quanto a estratégia a ser adotada, preparar o documento de anúncio e anunciar o setor da Auditoria.

O setor a ser auditado deve preparar as atividades administrativas de apoio ao Grupo Auditor, educar o pessoal do setor quanto ao processo que será utilizado, deliberar (resolver após examinar) quais informações são necessárias ao processo e fazer uma revisão final no setor.

Auditoria

Terminadas as reuniões iniciais e após definir as ações que serão tomadas, inicia-se a auditoria. O Auditor-chefe fará as solicitações por escrito e com data de retorno do representante do setor auditado.

De acordo com as datas preestabelecidas (na pré-auditoria) serão feitas reuniões onde os fatos identificados serão expostos e é entregue um relatório destes fatos ao representante do setor auditado para que este emita, por meio de outro relatório as razões de estar em desacordo.

Se tais razões não forem aceitas pelo grupo Auditor, elas farão parte do relatório denominado Sumário Executivo, que é apresentado à alta diretoria da empresa. Dentro deste mesmo relatório constará uma Avaliação Global da situação da área de informática que está sendo auditada. Geralmente a auditoria dura cerca de seis semanas.

Nesta fase, o Grupo Auditor deve avaliar os Controles (ou seja, como a área auditada funciona); documentar os desvios encontrados (falhas); validar as soluções, preparar o relatório final e apresentá-lo para a Presidência.

O Setor auditado deve prover as informações necessárias ao trabalho da auditoria, analisar a exposição dos desvios encontrados, entender os desvios encontrados, desenvolver planos de ação que solucionarão os desvios encontrados, corrigir as exposições e revisar o Sumário Executivo.

Pós-Auditoria

Terminada a auditoria, o grupo auditor emite um relatório final detalhando as suas atividades. Este relatório conterá o objetivo da Auditoria, as

áreas cobertas por ela, os fatos identificados, as ações corretivas recomendadas e a avaliação global do ambiente auditado.

Este relatório é enviado a todas as linhas administrativas, começando pela presidência e terminando no representante do setor auditado.

Nesta fase, o Setor Auditado deve solucionar os desvios encontrados pela auditoria, preparar resposta ao Relatório Final e apresentar para a Presidência, administrar conclusão dos desvios e manter o controle para que os erros não se repitam e a eficácia seja mantida.

O Grupo Auditor deve distribuir o Relatório Final, revisar resposta recebida (soluções e justificativas apresentadas), assegurar o cumprimento do compromissado e analisar a tendência de correção.

Inter-Relação entre auditoria e segurança em informática

Resumindo, podemos dizer que a segurança e a auditoria são interdependentes, ou seja, uma depende da outra para produzirem os efeitos desejáveis à alta administração.

Enquanto a segurança tem a função de garantir a integridade dos dados, a auditoria vem garantir que estes dados estejam realmente íntegros propiciando um perfeito processamento, obtendo os resultados esperados.

Com isso, concluímos que para que uma empresa continue competitiva no mercado, ela deve manter um controle efetivo sobre as suas áreas e isso é feito através do processo de auditoria.

A atividade de auditoria em segurança de informação

A auditoria tem como verificar se os requisitos para segurança da informação estão implementados satisfatoriamente, mantendo a segurança nos dados da empresa e verificando se os seus bens estão sendo protegidos adequadamente.

Inicialmente o auditor deve revisar o plano aprovado, ou seja, verificar se o método utilizado para proteção de informações é o melhor ou se precisa sofrer alguma atualização, sempre relacionado com o esquema de trabalho a seguir dentro da área que está sendo auditada.

Depois de terminado o estudo do plano, o auditor solicita os procedimentos necessários para descrever as diversas atividades que exige uma Segurança em Informática. Esses procedimentos serão confrontados com a realidade do dia-a-dia dentro do departamento, ou seja, verificando se todos os procedimentos necessários à Segurança em Informática são corretamente utilizados no departamento que está sendo auditado.

Na investigação o Auditor deverá revisar os seguintes itens, verificando se:

- O proprietário (aquele que tem permissão para acessar um certo conjunto de informações), periodicamente faz uma revisão em todos os dados que ele possui acesso para verificar se houver perdas, alterações, ou outras problemas de qualquer natureza. O Centro de Computação deve ser avisado sobre os resultados obtidos através da revisão tanto quando eles forem favoráveis (os dados estão corretos) ou quando for encontrado alguma irregularidade.
- Todos os proprietários estão identificados, ou seja, os que possuem acesso a um conjunto de informações específicas;
- Os inventários são realizados conforme requerido, padronizados e periodicamente;
- Os dados possuem a proteção necessária para garantir sua integridade, protegendo-os contra acessos e alterações indevidas;
- As documentações necessárias devem ser avaliadas pelas áreas competentes, garantindo que estas demonstrem o que realmente ocorre dentro da área a que se está referindo as documentações;
- Quando ocorrem desastres desde um erro de digitação até a perda total dos dados de um banco de dados, existe um plano de recuperação em caso de desastre que são testados conforme requerido. Por exemplo, existem os sistemas de *backup* e *recovery*, isto é, os dados mais importantes devem possuir cópias evitando transtorno em caso de acontecimentos inesperados, verificando sempre se essas cópias estão seguras evitando problemas;
- Os programas críticos, ou seja, os programas de sobrevivência da empresa mais importantes, são seguros o suficiente que qualquer tentativa de fraude não consiga alterar o sistema;
- Um terminal tem acesso somente as informações inerente àqueles que irão manipulá-lo, ou seja, um terminal no setor de Finanças só proverá informações ligadas a este setor e seus processos, não terá acesso às informações relacionadas ao setor de Recurso Humanos. Por sua vez, estes terminais podem possuir senhas próprias, podendo ser acessado somente pelos envolvidos a este setor que estejam autorizados a possuírem tais informações, estando protegido assim, contra acessos não autorizados, ou utilizado outros métodos, pois depende de que área encara como segurança da informação;
- As senhas devem possuir suas trocas automáticas garantidas, pois é muito arriscado para uma empresa, principalmente empresas de grande porte, manter uma mesma senha por um grande período;
- O processo de auto-avaliação desta área foi feito e concluído com sucesso;
- Todos os usuários estão autorizados para o uso do computador, isto é, qualquer pessoa não autorizada a manipular dados dentro do sistema possa obter informações sem influenciar o sistema. Ex.: alterações.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005


A auditoria não serve somente para apontar os defeitos e problemas encontrados dentro de uma organização, o processo de auditoria deve ser considerada uma forma de ajuda aos negócios da empresa.

Outro documento importante sobre o processo de auditoria em sistemas de informação é o *A Guide to Understanding Audit in Trusted Systems* publicado pela *National Computer Security Center* (hoje o atual NIST).

CAPÍTULO XII

Legislação

Legislação Brasileira e Instituições Padronizadoras

A segurança de informações, em função de sua grande importância para a sociedade modera, deu origem a diversos grupos de pesquisa, cujos trabalhos muitas vezes são traduzidos em padrões de segurança, e a projetos legislativos que visam tratar do assunto sob o aspecto legal, protegendo os direitos da sociedade em relação a suas informações e prevendo sanções legais aos infratores.

Em geral, os padrões de segurança são utilizados no âmbito internacional, enquanto as leis e normas são normalmente estabelecidas em caráter nacional, podendo haver, entretanto, similaridade entre as legislações de países diferentes.

Para implantar segurança de informações, é recomendável, portanto, que a instituição pesquise e sempre se mantenha atualizada quanto à legislação aplicável e aos padrões de segurança estabelecida por organismos nacionais e internacionais.

A nossa legislação, com relação à segurança de informações, não está tão consolidada como a legislação americana, porém já existem alguns dispositivos legais sobre assuntos relativos à informática, direitos autorais e sigilo de informações:

- Projeto de lei do Senador Renan Calheiros, de 2000 – define e tipifica os delitos informáticos;
- Projeto de lei nº 84, de 1999 – dispõe sobre os crimes cometidos na área de informática e suas penalidades;
- Lei nº 9.609, de 19 de fevereiro de 1998 – dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no país;
- Lei nº 9.610, de 19 de fevereiro de 1998 – altera, atualiza e consolida a legislação sobre direitos autorais;
- Lei nº 9.296, de 24 de julho de 1996 – regulamenta o inciso XII, parte final, do artigo 5º, da Constituição Federal. O disposto nessa lei aplica-se a interceptação do fluxo de comunicações em sistemas de informática e telemática;
- Projeto de Lei do Senado nº 234, de 1996 – dispõe sobre crime contra a inviolabilidade de comunicação de dados de computador;
- Projeto de Lei da Câmara dos Deputados nº 1.713, de 1996 – dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores;

- Decreto nº 96.036, de 12 de maio de 1988 – regulamenta a Lei nº 7.646, de 18 de dezembro de 1987, revogada pela Lei nº 9.609, de 19 de fevereiro de 1998;
- Decreto nº 79.099, de 06 de janeiro de 1977 – aprova o regulamento para salvaguarda de assuntos sigilosos.

Você pode acompanhar todas as leis referentes a internet no site Internet Legal (http://www.internetlegal.com.br/legis/) mantido pelo advogado Omar Kaminski. Garanto que vale a pena a visita ao site. Outro site com artigos interessantes sobre a legitimidade dos documentos digitais é o do advogado Aldemario Araújo Castro (http://www.aldemario.adv.br/dinformatica.htm), mantido pelo próprio. Esta referência (http://www.estig.ipbeja.pt/~ac_direito/dinfhome.html) veio lá de Portugal, oferecido pelo amigo e professor Manuel David Masseno.

Considerações[12]

A Internet é a mídia mais segura, e a mais insegura, que existe. Já é, estatisticamente, onde ocorre a maioria das fraudes, invasões de privacidade, e outros ilícitos cíveis e criminais. Por outro lado, tecnicamente, é a que oferece maiores condições de garantia de integridade, procedência e autenticidade nas comunicações. Como se situa a lei, entre esses dois pólos ?

Em primeiro lugar, cabe lembrar que bem antes da Internet, essa questão já se apresentava, em face da armazenagem eletrônica, das transmissões de dados em redes fechadas, do intercâmbio eletrônico de dados (EDI), etc., sem que existissem leis de assinatura digital, contratos eletrônicos, e semelhantes. Como, então, o Direito dava conta dessas situações ?

Simples: fazendo uso de dois princípios fundamentais, o da autonomia da vontade ("o contrato é lei entre as partes") e o da responsabilidade civil ("quem causa um dano ilicitamente, deve repará-lo"). Por exemplo, em contratos de EDI se estipulava obrigação de sigilo em relação a senhas, e reconhecimento da validade de mensagens eletrônicas para fins de prova documental. E o fabricante de computadores ficava sujeito a consertar ou indenizar qualquer defeito.

Porém, havia, e continua a haver, um detalhe. É que a alta sofisticação da informática, e a dependência que ela gera, são associadas as maiores responsabilidades, tanto para os fornecedores de soluções de informática, quanto para os que dela se utilizam para oferecer bens ou serviços a terceiros. Nos EUA, chegaram até a tentar criar a expressão "*computer malpractice*", para elevar o nível de responsabilidade do setor equiparando-o à severidade dos erros médicos, denominados "*medical malpractice*". No mundo inteiro, os prejuízos da informática geram indenizações maiores, e o uso de computadores costuma ser classificado como agravante no julgamento de crimes.

[12] (Almeida, 2001)

Assim, como minimizar essa responsabilização mais grave? Resposta básica: atentando no dever de escolher um bom fornecedor ou funcionário (“*culpa in eligendo*”), no de exercer um mínimo de vigilância (“*culpa in vigilando*”), no de não omitir informações relevantes (“*culpa in omittendo*”) e no de contratar em termos adequados (“*culpa in contraendo*”). Resumindo, trata-se de contratar um fornecedor bem reputado e que possua o “estado da arte”, acompanhar seu trabalho, assegurar as informações importantes, e fazer um contrato bem estruturado. Isto significa haver tomado as precauções esperáveis no limite das possibilidades, o que isenta de maiores responsabilidades, na medida em que ninguém é culpado pelo impossível.

Lógico, as leis que estão vindo para regular a Internet, nas áreas de privacidade (“cookies” e “spam”), assinatura digital, concorrência, consumidor, e outras, reforçarão as proteções asseguradas pelo Direito. Mas como o ritmo do Legislativo, em qualquer país, é mais lento que a evolução contínua da Internet, sempre haverá déficit legislativo, portanto os princípios tradicionais do Direito continuarão necessários.

Aí é que a lei e a técnica se juntam, transformando a responsabilidade em oportunidade. É que o conhecimento especializado de ambas permite tirar o melhor partido da aplicação dos princípios antigos, atualizando-os frente a novas realidades. Além de diferencial competitivo, este know-how propicia, para os que o utilizam, que a Internet seja, de fato e de direito, a mais segura das mídias.

Crime digital[13]

O crime digital em todas as suas formas é um Crime de Meio, um crime corriqueiro que é cometido através do uso do computador, e não uma nova modalidade de crime nunca visto antes. Logo, a questão de se punir os criminosos digitais não é tanto pela falta de leis que o permitam, mas também pelo despreparo do poder de polícia em lidar contra os atos ilegais com as ferramentas que se encontram disponíveis na jurisdição brasileira.

É um fato conhecido de que a justiça brasileira é lenta tanto em processar quanto legislar, porém com a existência da “tipificação dos crimes” já na legislação, e apenas a necessidade de se utilizar os ditos tipos de crimes no âmbito da informática ajuda a agilizar eventuais processos contra criminosos digitais.

Os crimes que podemos analisar então são aqueles cujo fim está coberto pelo âmbito da legislação já vigente, divididos entre crimes contra a pessoa, crimes contra o patrimônio, crimes contra a propriedade imaterial, crime contra os costumes, crimes contra a incolumidade pública, crimes contra a paz pública e outros crimes menos comuns. Será exemplificado, a seguir, formas digitais da ocorrência destes crimes.

[13] Fonte: (Ravanello, Hijazi e Mazzorana, 2004)

Crimes contra a pessoa

São crimes que visam a vida e a integridade física dos seres humanos:

- **Homicídio**: Ticio invade um sistema de controle de semáforos, deixando o sinal no estado "verde" tanto para o pedestre quanto para o veículo que vem no sentido contrário, causando o atropelamento do pedestre; neste caso, respondem tanto o motorista e o invasor por homicídio, o motorista responde por homicídio culposo por não ter pretendido matar um pedestre e o invasor por homicídio doloso, por ter deliberadamente causado um evento capaz de tirar vidas.
- **Crimes contra a honra**: Uma pessoa mal intencionada publica em uma página web informações de cunho calunioso ou informações que não se pode provar; Uma pessoa envia para mais de uma pessoa um e-mail expondo a sua opinião negativa acerca de outra pessoa de maneira caluniosa, com informações acerca da pessoa que quem enviou o e-mail não consegue provar a veracidade.
- **Indução, Estímulo ou Auxílio ao Suicídio**: Ticio encontra Mévio em uma sala de bate-papo, onde Mévio revela à Ticio seu desejo de extinguir a sua vida. Então Ticio passa a estimular Mévio a cometer o suicídio, e caso Mévio venha a ter sucesso neste ato, a prova material da influência de Ticio na morte de Mévio é exatamente o computador e os eventuais logs de conversas entre Ticio e Mévio. A título de exemplo, na data de 18/03/1999, o jornal "O Tempo", de Belo Horizonte, publicou o endereço de um site americano que encorajava o suicídio como solução final dos problemas, e pedia que os suicidas publicassem suas cartas de despedida no site. Pelo menos 3 pessoas das que postaram suas cartas de despedida no site foram encontradas mortas e uma quarta não teve sucesso na tentativa de suicídio e foi internada para tratamento psicológico;

Crimes contra o patrimônio

- **Furto**: Ticio entra em um site de algum operador financeiro e passa a manipular os centavos de diversas contas, transferindo-os para uma conta própria.
- **Estelionato**: Ticio envia e-mails fazendo correntes e pedindo que sejam efetuados depósitos monetários em uma conta corrente específica; ou ainda: a mesma pessoa utiliza um software criado para gerar números falsos de cartão de crédito e de CPF, fazendo compras então com estes números falsos. O crime de estelionato é o mais comum pela Internet, e é o que mais gera processos criminais.

Crimes contra a propriedade imaterial

- **Violação de Direito Autoral**: Ticio cria um site que permite que outras pessoas façam download de programas completos ou

músicas sem pagar nada por isso.

- **Concorrência Desleal**: o dono da Empresa MevioTronic publica em um site que o produto produzido pela sua concorrente, a empresa TicioTronic, é altamente nocivo para a saúde, segundo uma pesquisa americana.
- **Usurpação de nome ou pseudônimo alheio**: Ticio invade o site de um famoso escritor Mévio e lá publica um conto de sua autoria, e um comentário assinado pelo escritor dizendo que nele baseou alguma obra qualquer.

Crimes contra os costumes

- **Pedofilia**: Publicar, gerar, transmitir ou acessar imagens de crianças e adolescentes mantendo relações sexuais.
- **Favorecimento à prostituição**: Ticio constrói um site que contém links para fotos e números de telefone de prostitutas, ou ainda uma Mévio que envia mensagens (e-mail, celular, torpedo), convidando mulheres a se cadastrarem e oferecerem seus serviços em dado site.
- **Rufianismo**: no mesmo site acima, uma opção para se contratar as mulheres e se pagar com o cartão de crédito diretamente no site.

Crimes contra a incolumidade pública

- **Tráfico de Drogas e de Armas com ou sem Associação para**: Ticio anuncia em um leilão pela Internet drogas ou armas com entrega em domicílio.

Crimes contra a paz pública

- **Incitação ao Crime**: Ticio, preconceituosa faz um site com comentários racistas e com a possibilidade de outras pessoas também "expressarem sua opinião".
- **Formação de Quadrilha ou bando**: Ticio, Mévio e Licio combinam, em um chat pela Internet a invasão de um site de um grande banco, com o objetivo de dividir os espólios entre suas contas.

Outros crimes menos comuns

- **Ultraje a culto ou prática religiosa**: Ticio constrói um site apenas para maldizer uma prática religiosa e todos os seus seguidores.
- **Crime eleitoral**: Ex-candidato Ticio, desprovido de direitos eleitorais por ter sido caçado anteriormente, envia mensagens às pessoas, pedindo votos para seu aliado, o candidato Mévio.

Legislação específica para o meio digital[14]

A lei 9.296/96 é a primeira lei específica para o meio digital e trata, basicamente do sigilo das transmissões de dados, segundo a qual é vedado a qualquer pessoa ou entidade o direito de interceptação de mensagens digitais ou telefônicas, bem como quaisquer comunicações entre 2 computadores por meios telefônicos, telemáticos ou digitais.

A interpretação mais recente desta lei observa exatamente esta ultima parte da lei, "comunicação entre 2 computadores" e a aplica a furto de dados de bancos de dados, invasão e espionagem ou *sniffing* da rede e outros delitos que envolvam a manipulação de um terceiro à um conjunto de dados pertencente a outros computadores.

Ainda a lei 9.983/00 prevê como crime a ação de divulgação de segredo, inclusive por meio da Internet tanto a sua transmissão quanto sua descoberta, sendo considerado como segredo, para efeitos da lei, senhas, dados de clientes ou quaisquer outras informações que não possam ser obtidas senão através da invasão do site. Esta lei também inclui como crime ações que englobam mas não se limitam à inserção proposital de dados inválidos em bancos de dados e da construção e modificação de sistemas sem a autorização do proprietário.

Ainda circula pela câmara dos deputados um Projeto de lei, de número 89/04 que prevê condutas tipicamente do meio digital, como disseminação de vírus, invasão e pichação de sites, entre outros.

Prova de autoria e dificuldades técnicas que atrapalham a captura de criminosos virtuais[15]

Visto que há legislação capaz de atender muitas das ocorrências de crimes digitais, podemos afirmar que não é apenas a incapacidade de se processar um crime digital que impede que o Brasil tenha um número tão grande de ocorrências de invasões sem punição.

A principal dificuldade encontra-se em efetuar a “prova da autoria” de um crime digital, prova esta que é a evidência irrefutável de que uma pessoa utilizou um computador para efetuar um crime.

A legislação brasileira compara o computador, nos casos de crime digital, à uma ferramenta, à arma do crime. Se em um homicídio nós temos a figura da vítima, o ato (perfurações por arma de fogo) e a arma que foi usada, em um crime digital existe a mesma estrutura, que é a vítima que teve sua perda moral ou material, o ato (modificação de dados, exclusão, cópia indevida) e a arma que foi usada para tal, no caso o computador.

Em um crime real, no entanto, existe a necessidade em se ligar a arma

[14] Fonte: (Ravanello, Hijazi e Mazzorana, 2004)
[15] Fonte: (Ravanello, Hijazi e Mazzorana, 2004)

de um crime a uma pessoa que o tenha cometido. Esta ligação pode ser efetuada por testemunhos, por análises forenses laboratoriais ou por provas materiais como fotos e filmagens, por exemplo.

No mundo digital, no entanto, há uma complicação a isso: como garantir que uma pessoa realmente utilizou tal computador para efetuar um crime? As técnicas forenses são utilizadas para determinar com exatidão qual computador foi utilizado e quais as ações do criminoso digital, porém é difícil de se ligar uma pessoa ao ato criminoso. Esta é exatamente a maior dificuldade em se reprimir o crime digital. Para poder autuar um criminoso digital, é necessário um conjunto muito grande de provas circunstanciais ou então de uma autuação em flagrante delito; dadas às dimensões da Internet, onde o crime pode ser cometido em qualquer lugar do mundo e a partir de qualquer outro lugar do mundo, o flagrante instantâneo de mostra difícil de se obter, logo é necessária sempre uma investigação profunda na qual se permite que o delito seja praticado às vezes até mais de uma vez, para que se possa obter uma autuação em flagrante.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br
01/06/2005

CAPÍTULO XIII

Segregação de Ambiente e Funções

Introdução

Um dos muitos itens que constam na norma é a segregação de função. A segregação de função pode ser explicada com um exemplo simples: um DBA cria a base dados, um programador irá criar os programas que trabalham com esta base, mas será o usuário que irá popular a base. Nem o DBA e nem o programador poderá ter permissões para alterar as informações cadastradas pelo usuário do sistema.

A segregação de ambientes, consiste em trabalhar com pelo menos 3 ambientes idênticos em termos de configuração de máquina (ou no mínimo, em termos de funcionalidade) e software, estes ambientes são chamados popularmente de Desenvolvimento, Homologação e Produção. Teoricamente, o programador somente tem acesso total no ambiente de desenvolvimento. O processo de transferência de software de um ambiente para outro, deve ser realizada por uma pessoa ou área específica e deve estar o mais bem documentado possível.

A proteção destes ambientes é simples, o desenvolvedor somente tem acesso ao ambiente de desenvolvimento (baseando em autenticação do próprio sistema operacional, com login e senha) e ele não pode ter o domínio de nenhuma chave de acesso aos ambientes de homologação e produção (não pode ter acesso ao sistema operacional e nem ao banco de dados destes ambientes). Caso exista a necessidade de um acesso, deve ser criada uma chave temporária de acesso e todas as informações (comandos de sistema operacional e banco de dados) devem ser registradas.

A empresa deve ter uma norma rígida para tentativas de acesso indevidas e detectadas. Deve-se estabelecer uma política clara e que deve ser cumprida. Uma sugestão de punição é uma multa para o funcionário infrator com possível demissão no caso de re-incidência.

Vamos ver os conceitos a seguir, extraídos diretamente da norma.

Segregação de Funções

A segregação de funções é um método para redução do risco de mau uso acidental ou deliberado dos sistemas. Convém que a separação da administração ou execução de certas funções, ou áreas de responsabilidade, a fim de reduzir oportunidades para modificação não autorizada ou mau uso das informações ou dos serviços, seja considerada.

As pequenas organizações podem considerar esse método de controle

difícil de ser implantado, mas o seu princípio deve ser aplicado tão logo quanto possível e praticável. Onde for difícil a segregação, convém que outros controles, como a monitoração das atividades, trilhas de auditoria e o acompanhamento gerencial sejam considerados. É importante que a auditoria da segurança permaneça como uma atividade independente.

Convém que sejam tomados certos cuidados para que as áreas nas quais a responsabilidade seja apenas de uma pessoa não venha a ser alvo de fraudes que não possam ser detectadas. Recomenda-se que o início de um evento seja separado de sua autorização. Recomenda-se que os seguintes controles sejam considerados:

- É importante segregar atividades que requeiram cumplicidade para a concretização de uma fraude, por exemplo, a emissão de um pedido de compra e a confirmação do recebimento da compra.
- Se existir o perigo de conluios, então é necessário o planejamento de controles de modo que duas ou mais pessoas necessitem estar envolvidas, diminuindo dessa forma a possibilidade de conspirações.

Separação dos ambientes de desenvolvimento e de produção

A separação dos ambientes de desenvolvimento, teste (homologação) e produção são importantes para se alcançar à segregação de funções envolvidas. Convém que as regras para a transferência de software de desenvolvimento para produção sejam bem definidas e documentadas.

As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações não autorizadas total ou parcialmente de arquivos ou do sistema. Convém que seja avaliado o nível de separação necessário entre o ambiente de produção e os ambientes de teste e de desenvolvimento, para prevenir problemas operacionais. Convém que uma separação semelhante também seja implementada entre as funções de desenvolvimento e de teste. Nesse caso, é necessária a existência de um ambiente confiável e estável, no qual possam ser executados os testes e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento.

Quando o pessoal de desenvolvimento e teste possui acesso ao ambiente de produção, eles podem introduzir códigos não testados ou autorizados, ou mesmo alterar os dados reais do sistema. Em alguns sistemas essa capacidade pode ser mal utilizada para a execução de fraudes, ou introdução de códigos maliciosos ou não testados. Esse tipo de código pode causar sérios problemas operacionais. O pessoal de desenvolvimento e os encarregados dos testes também representam uma ameaça a confidencialidade das informações de produção.

As atividades de desenvolvimento e teste podem causar modificações não intencionais no software e a informação se eles compartilham o mesmo ambiente computacional. A separação dos recursos de desenvolvimento, de teste e operacionais é dessa forma bastante desejável para a redução do risco

de modificação acidental ou acesso não autorizado ao software operacional e dados dos negócios. Recomenda-se que os seguintes controles sejam considerados:

- Convém que o software de desenvolvimento e o software de produção sejam, sempre que possível, executados em diferentes processadores, ou diferentes domínios ou diretórios.
- Convém que as atividades de desenvolvimento e teste ocorram de forma separada, tanto quanto possível.
- Convém que compiladores, editores e outros programas utilitários não sejam acessíveis a partir do ambiente de produção, quando isso não for uma necessidade.
- Convém que o processo de acesso ao ambiente de produção seja diferente do acesso de desenvolvimento para reduzir a possibilidade de erro. Convém que os usuários sejam incentivados a usar diferentes senhas para esses ambientes e as telas de abertura exibam mensagens de identificação apropriadas.

Convém que o pessoal de desenvolvimento receba senhas para acesso ao ambiente de produção, e de forma controlada e apenas para suporte a sistemas no ambiente de produção. Convém que sejam utilizados controles que garantam que tais senhas seja alteradas após o uso.

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

CAPÍTULO XIV

A Questão Humana na Segurança da Informação

Os avanços tecnológicos, principalmente na área dos computadores, têm permitido a automação de muitos processos e trabalhos antes manuais, em uma variedade de aplicações, em geral com foco no aspecto econômico e relacionado ao aumento da produtividade, na redução dos custos, além de outros objetivos como a redução da fadiga e de tempo em processos repetitivos, precisão no manuseio de informações, etc. Contudo, os equipamentos de automação agregam um alto valor monetário no processo, como os custos dos equipamentos, dos custos decorrentes da própria operação, manutenção e de treinamento aos operadores; por outro lado, em determinadas aplicações, é necessário à aplicação da redundância nos equipamentos para que os níveis de confiabilidade sejam garantidos (Leveson et al, 1997).

De que adianta toda a proteção tecnológica ?

Algumas tarefas realizadas por humanos necessitam de precisão de uma máquina eletrônica, mas são os homens que criam as especificações para estas máquinas e muitas destas especificações contêm inconsistências e indefinições (Martin, 1991). Antigamente, a atenção sobre a segurança da informação estava focada para a tecnologia. Hoje, o desafio é construir uma relação de confiabilidade com clientes e parceiros.

Conforme (Rezende e Abreu, 2000), as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório para ambas as partes, com objetivos comuns.

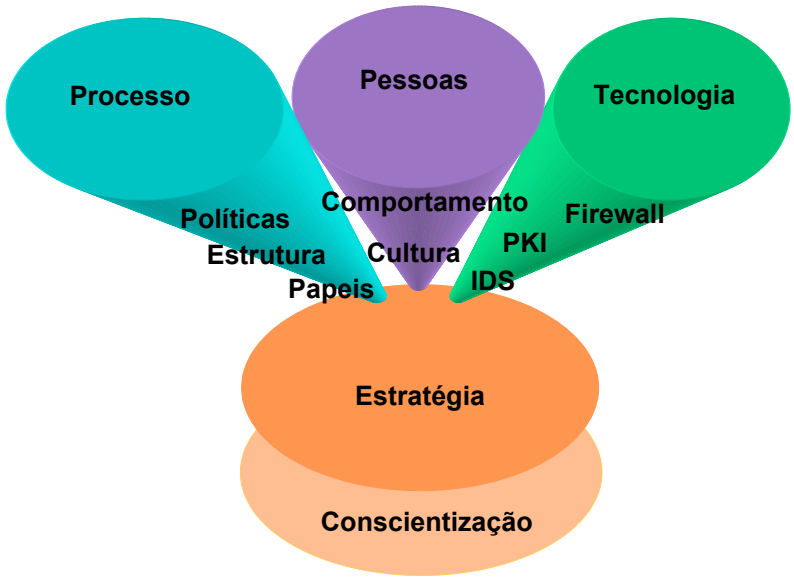
Atualmente, os negócios de uma empresa estão atrelados a 3 itens importantes:

- **Processos** – Conjunto de atividades que produzem um resultado útil para o cliente interno ou externo.

- **Pessoas** – Grupos que visam alcançar seus objetivos e atender as suas necessidades (Rezende e Abreu, 2000). Na realidade, são as pessoas que projetam e executam os diversos processos dentro de uma empresa.

- **Tecnologia** – Toda e qualquer ferramenta utilizada pelas pessoas da empresa para que seja realizada.

Conforme a figura abaixo demonstra, os processos, as pessoas e tecnologias devem atender a uma estratégia da empresa, pode-se afirmar que a estratégia da empresa é obter o lucro para seus administradores e acionistas. Para que a estratégia seja alcançada, é necessária a conscientização de todas as partes envolvidas.



Relação dos componentes de uma empresa.

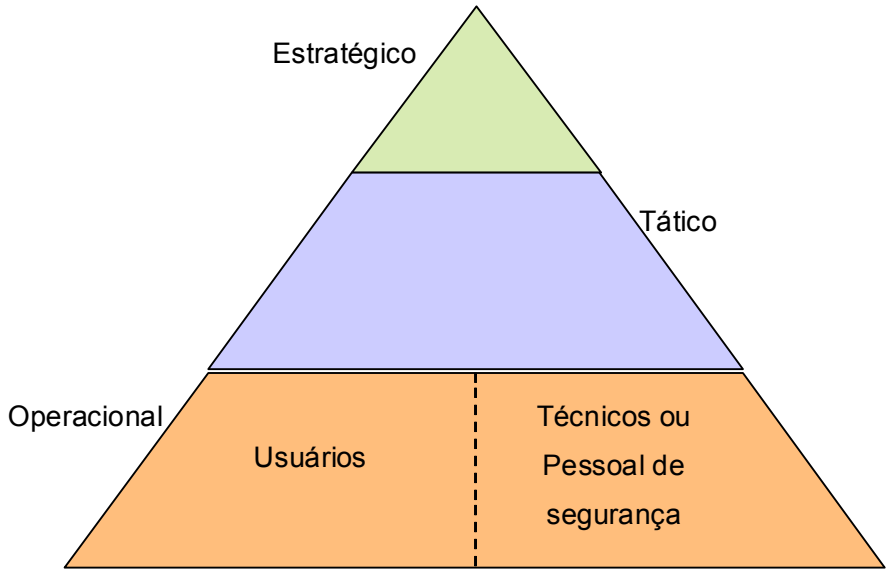
Conforme (DeMarco e Lister, 1990), os principais problemas de uma empresa não são de natureza tecnológica, mas sim sociológica. Partindo deste princípio, pode-se afirmar que o elo mais fraco de um processo de segurança é a pessoa (ou grupos de pessoas).

No planejamento estratégico das informações, é vital a participação do Analista ou Gestor do Negócio, pois somente ele pode mensurar a importância da informação (Feliciano Neto, Furlan e Higo, 1988). Se um processo não funciona adequadamente, é por que alguma pessoa a projetou errada ou escolheu a tecnologia inadequada. Caso alguma das tecnologias venha a falhar ou não atender as necessidades da empresa, a culpa é da pessoa que

configurou ou mesmo definiu aquela tecnologia. Vale lembrar que falhas da tecnologia por outros fatores, como por exemplo, a ausência de eletricidade, também pode ser atribuída à pessoa. Afinal, ela deveria ter-se preocupado em garantir a continuidade das operações da empresa.

Os fatores de sucesso críticos para empresa são decompostos em fatores de sucesso críticos para os departamentos e então relacionados às motivações dos executivos (Martin, 1991). Os produtos e serviços são criados dentro de um ambiente extremamente dinâmico. O desafio está em inovar, ousar, agilizar e controlar, identificando e gerenciando os riscos para as partes envolvidas.

A divulgação das informações pelas pessoas que participam da organização constitui-se em uma falta ética e moral grave. Semelhantemente, na economia do conhecimento a divulgação de dados ou informações organizacionais pode acarretar em perdas econômicas ou danos quanto a possibilidades de inserção privilegiada para a organização ou seus produtos e / ou serviços no mercado (danos estratégicos). Conforme a próxima figura demonstra (baseando-se na tradicional pirâmide de níveis dentro de uma empresa), o nível operacional é caracterizado por 2 lados: Quem precisa implantar a segurança e as pessoas que precisam utilizar os recursos da empresa.



Neste contexto, alguns cuidados devem ser tomados com relação às pessoas, processos e tecnologias de uma empresa (DeMarco e Lister, 1990):

- Ensinar aos seus funcionários a ler sobre o desenvolvimento do seu trabalho;
- É possível obter qualidade sem ferramentas “maravilhosas”;
- Não existe técnicos ou ferramentas que tragam a qualidade de uma hora para outra;
- Constantes modificações são inimigas da qualidade;
- Não construa sistemas que querem prever e tratar todas as possibilidades

altere somente quando o caso raríssimo ocorrer;
- Uma metodologia funciona, quando toda a equipe conhece, entende e compreende o significado da mesma;
- Os melhores testes são feitos por outros técnicos que não participaram na confecção do software. Mais importante, os técnicos que realizam os testes conhecem tanto da área de negócios como da área tecnológica;

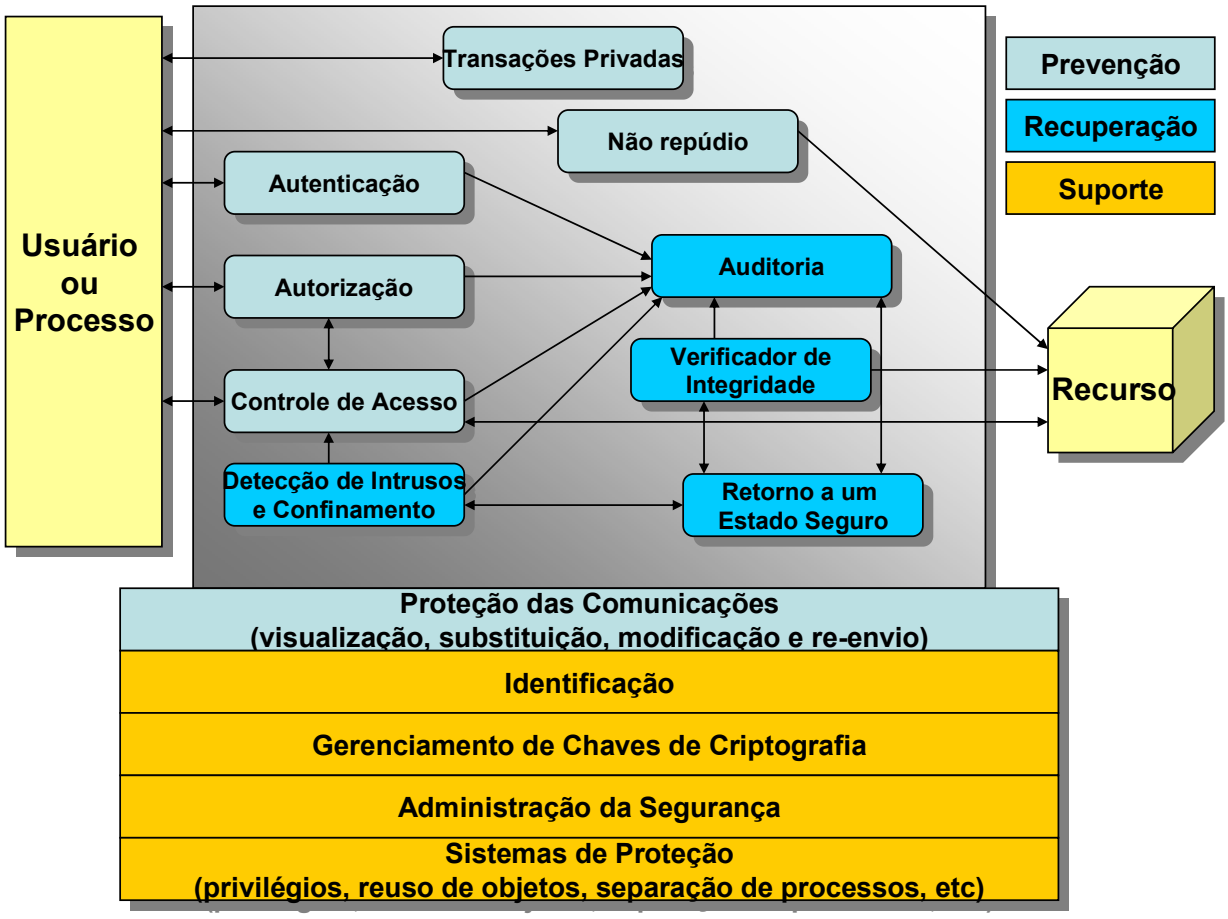
Todas informações (ou quase) têm a interferência de um ser humano no processo ou tecnologia, neste caso é necessário garantir a confiabilidade humana nas partes envolvidas.No contexto da engenharia, a confiabilidade humana é a probabilidade de que um humano execute corretamente uma tarefa designada em um tempo especificado, durante um período de tempo definido em um ambiente também especificado (Lasala, 1998).

CAPÍTULO XV

Um modelo para Implantação da Segurança

Conforme (Stoneburner, 2001), o modelo de segurança é descrito na próxima figura que mostra os serviços preliminares e os elementos usados para suportar e executar a segurança da tecnologia de informação, junto com seus relacionamentos preliminares. O modelo classifica também os serviços de acordo com sua finalidade preliminar como segue:

- **Suporte** – Serviços genéricos para a maioria das atividades na segurança da informação.
- **Prevenção** – Estes serviços focalizam em impedir que ocorra uma falha na segurança.
- **Detecção e Recuperação** – Focalizam na detecção e recuperação no caso de uma falha na segurança.



Definição dos Serviços ou Mecanismos

Os serviços de suporte são, por sua natureza, persuasivos e inter-relacionados com muitos outros serviços:

- **Identificação** – Para que sejam executados outros serviços, é necessário que os assuntos e objetos sejam identificados. Este serviço fornece a capacidade para identificar usuários, processos e recursos.

- **Gerenciamento de Chaves de Criptografia** – As chaves de criptografia devem ser seguramente gerenciadas, para prover funções criptográficas implementadas em outros serviços.

- **Administração da Segurança** – As diversas camadas de segurança precisam de administradores para instalações específicas e controles do ambiente operacional.

- **Sistemas de Proteção** – Representam a qualidade das implementações de segurança adotadas. São à base de confiança do sistema de segurança.

Os serviços de prevenção, visam impedir que ocorram quebras na segurança:

- **Proteção das Comunicações** – Em sistemas distribuídos, os objetivos de segurança somente são obtidos se os sistemas de comunicação são altamente confiáveis. A proteção das comunicações garante os serviços de integridade, disponibilidade e confidencialidade das informações em trânsito.

- **Autenticação** – Este serviço provêm os meios para verificar a identidade de um sujeito ou objeto.

- **Autorização** – Especifica e habilita o gerenciamento das ações que podem ser realizadas dentro de um sistema.

- **Controle de Acesso** – Verificar as permissões que um determinado sujeito ou objeto têm sobre o sistema.

- **Não repúdio** – Este serviço é executado tipicamente no ponto da transmissão ou da recepção, pois o objetivo é assegurar de que os remetentes não possam negar de ter emitido a informação e os receptores não podem negar a de ter recebido-as.

- **Transação Privada** – Protege contra a perda da privacidade no que diz respeito às transações que estão sendo executadas por um indivíduo.

Como nenhum conjunto de medidas de prevenção é perfeito, é necessário que falhas de segurança sejam identificadas e possam ser tomadas

ações reduzir seu impacto:

- **Auditoria** – A auditoria é importante para a segurança, pois é através dela que será possível detectar e recuperar as informações após a realização de algum ato indesejado.

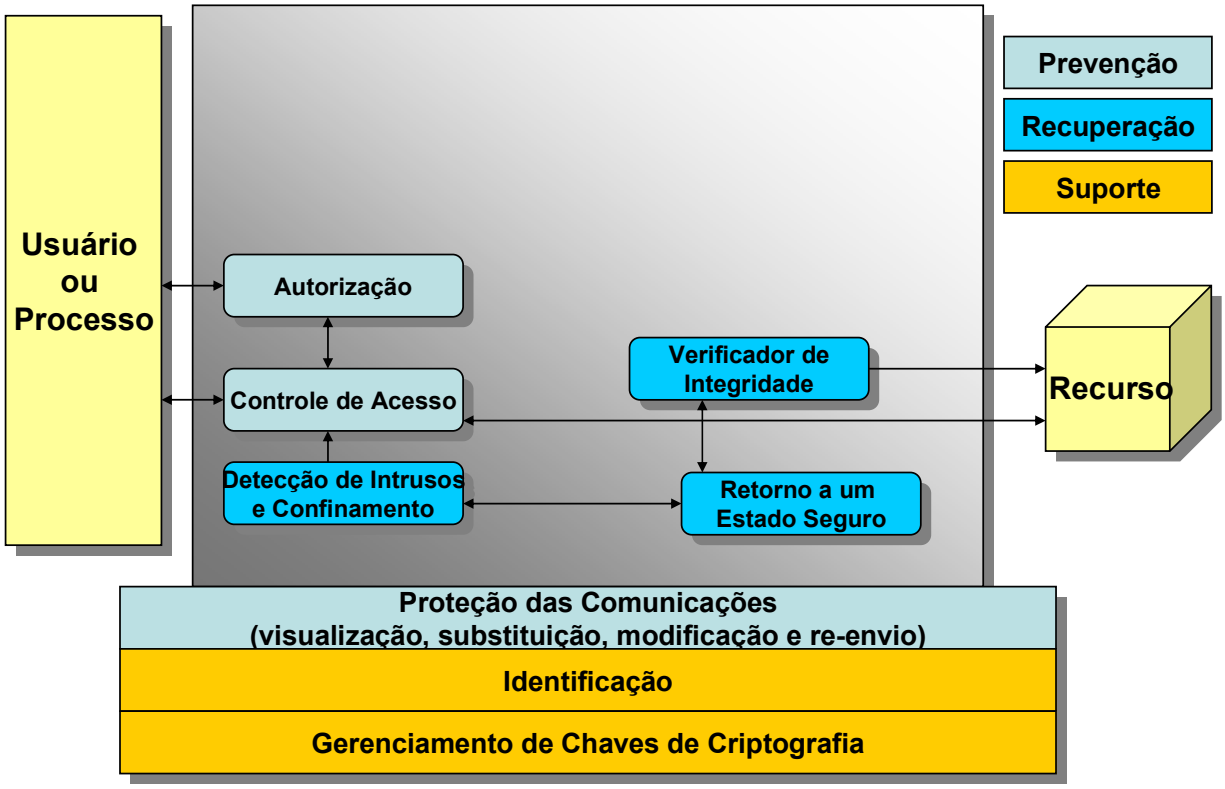
- **Detecção de Intrusão e Confinamento** – A detecção de situações inseguras é essencial para respostas oportunas. Se uma falha de segurança não for detectada, não será possível iniciar os procedimentos de resposta e confinamento de forma eficaz.

- **Verificador de Integridade** – Essencial para identificar uma potencial corrupção da informação ou sistema.

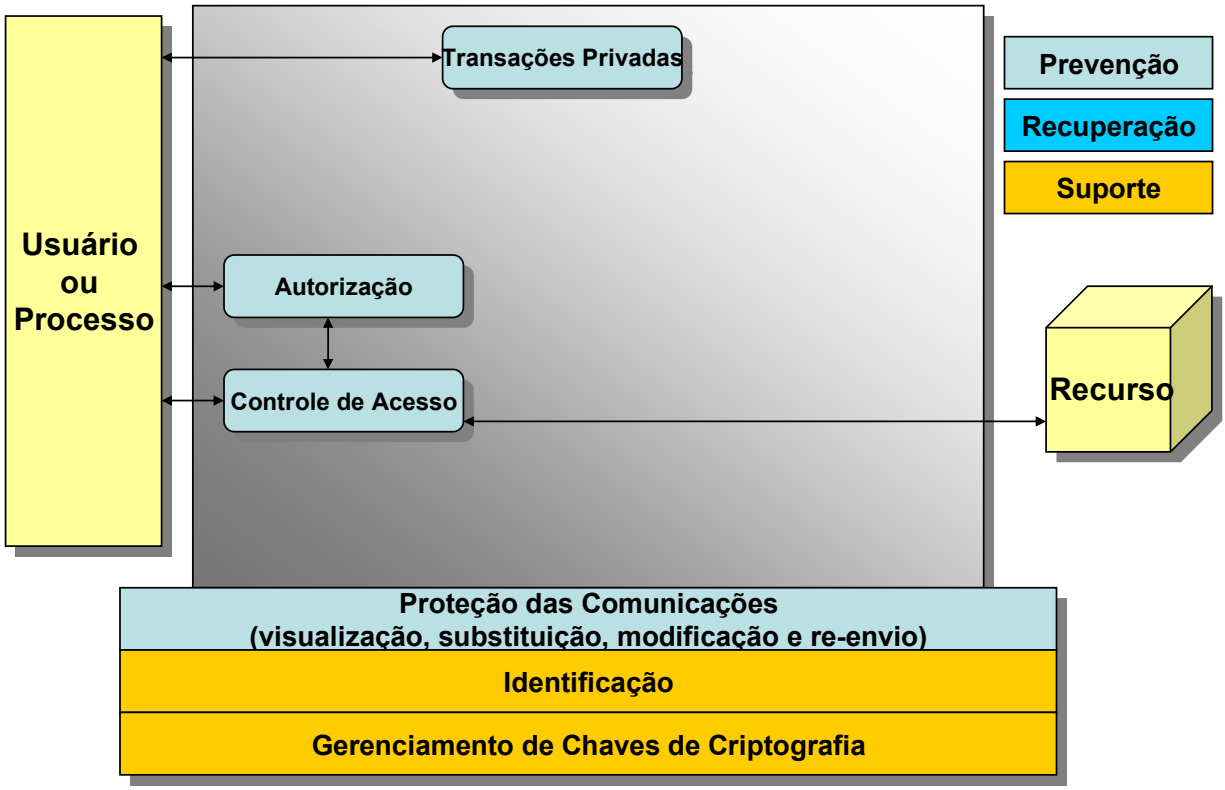
- **Retorno a um estado seguro** – Capacidade do sistema retornar (*rollback*) a um estado salvo caso tenha havido uma falha de segurança.

O modelo conforme os princípios da segurança

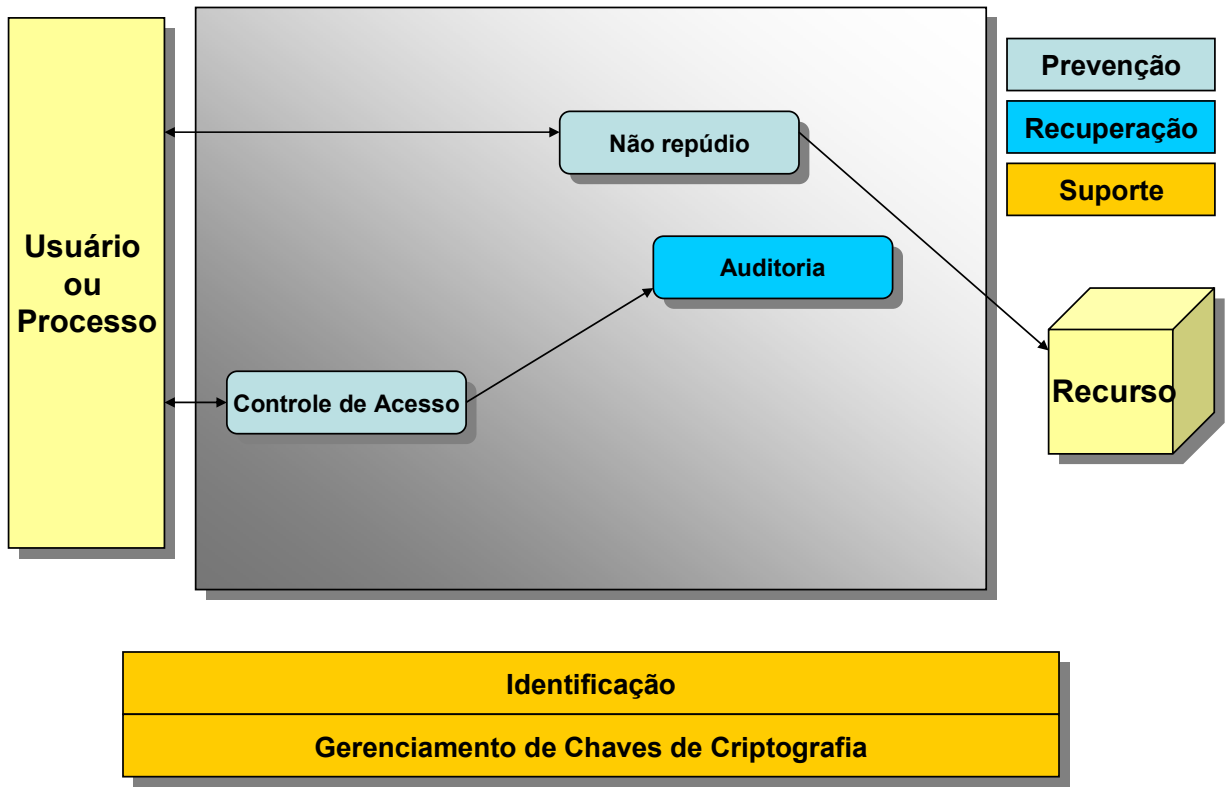
A implementação da **disponibilidade** e da **integridade** são obtidas através do controle e identificação das pessoas e alterações não autorizadas, e a capacidade do sistema ser recuperado.



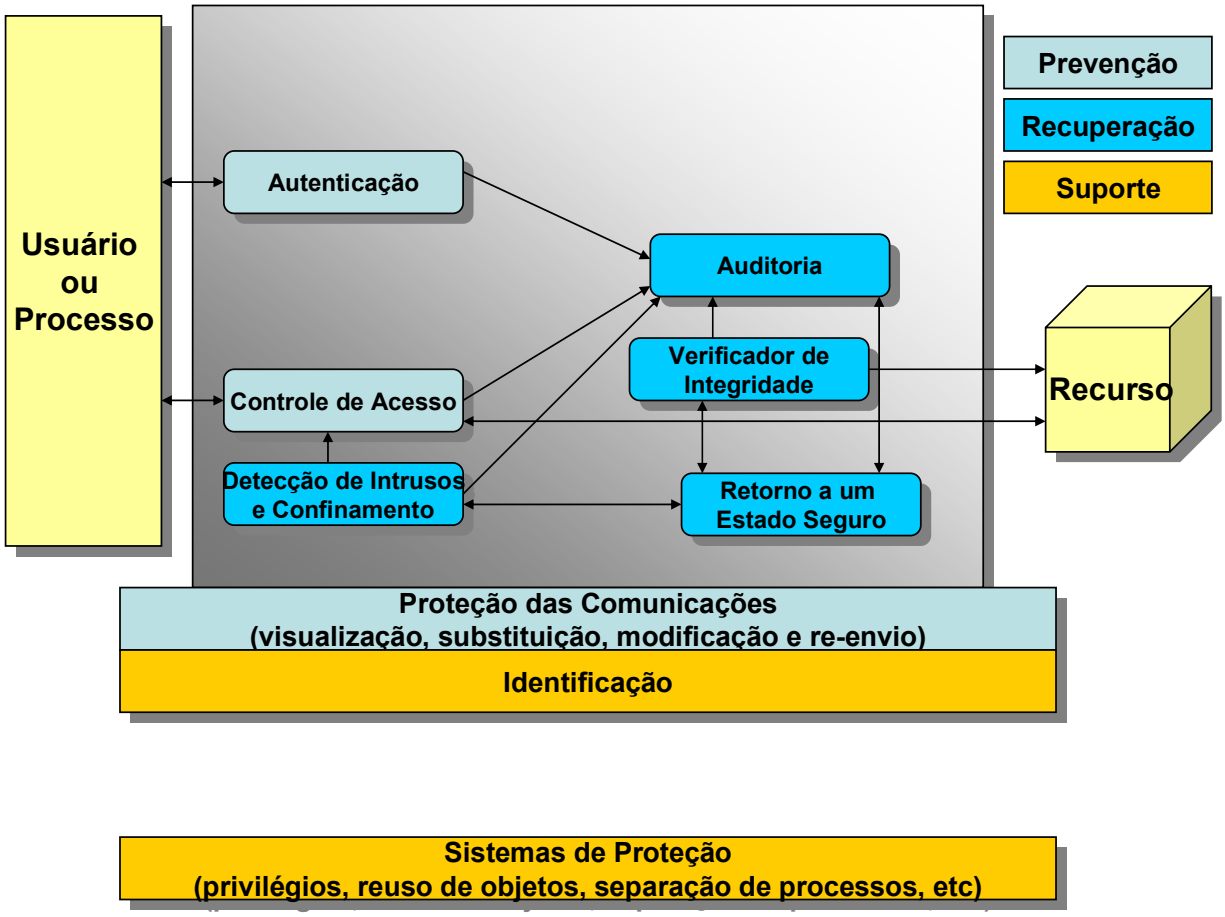
A **confidencialidade** é obtida através da proteção das comunicações, do controle de acesso e do uso eficaz dos mecanismos de privacidade (de forma a manter a confidencialidade).



A **auditoria** do sistema é necessária para manter a rastreabilidade das ações e o não-repúdio das transações efetuadas no sistema.



E finalmente, é possível obter a garantia (qualidade) segurança de um sistema de informação, se alguns dos serviços citados forem implementados. Esta garantia é dependente da forma e dos objetivos do sistema.


Usuário
ou
Processo
Autenticação
Auditoria
Controle de Acesso
Verificador de
Integridade
Detecção de Intrusos
e Confinamento
Retorno a um
Estado Seguro
Recurso
Prevenção
Recuperação
Suporte
Proteção das Comunicações
(visualização, substituição, modificação e re-envio)
Identificação
Sistemas de Proteção
(privilégios, reuso de objetos, separação de processos, etc)

CAPÍTULO XVI

Instituições Padronizadoras e Normas de Segurança

Pequeno histórico sobre o surgimento das Normas de Segurança[16]

Desde o início da civilização humana há uma preocupação com as informações e com os conhecimentos atrelados a elas. Inicialmente, esta atenção especial pode ser observada no processo de escrita de alguns povos, como é o caso da antiga civilização egípcia, na qual somente as castas "superiores" da sociedade tinham acesso aos manuscritos da época, e menos pessoas ainda ao processo de escrita dos mesmos. Assim a escrita, por meio de hieróglifos do Egito antigo, representa uma das várias formas utilizadas pelos antigos de protegerem e, ao mesmo tempo, perpetuarem o seu conhecimento.

Contudo, somente na sociedade moderna, com o advento do surgimento dos primeiros computadores, houve uma maior atenção para a questão da segurança das informações. De início, esta preocupação era ainda muito rudimentar, porém com o passar do tempo este processo mudou.

A questão da segurança no âmbito dos computadores ganhou força com o surgimento das máquinas de tempo compartilhado, também conhecidas como computadores "time-sharing", ou seja, que permitiam que mais de uma pessoa, ou usuário, fizesse uso do computador ao mesmo tempo, processo comum na atualidade, mas que até então não era possível.

O "time-sharing" permitiu que vários usuários pudessem acessar as mesmas informações, contudo este acesso não gerenciado poderia gerar efeitos indesejáveis, tal como: um estagiário pode ter acesso aos dados do presidente da firma. Logo, nasce à necessidade da implementação de ferramentas que implementem o fornecimento de mecanismos para minimizar o problema do compartilhamento de recursos e informações de forma insegura.

Neste período foi então caracterizado o que ficara conhecido como o "problema clássico de computadores", o qual pode ser resumido na seguinte questão: "Como fazer com que usuários autorizados possam ter acesso a determinadas informações, ao mesmo tempo em que os usuários não autorizados não possam acessá-las ?".

Todavia, a resposta para a pergunta acima não era, e ainda não é, trivial. A primeira resposta, sugerida na época para solucionar o problema foi à construção de um Sistema Operacional (S.O.) melhor, mais aprimorado.

[16] (Gonçalves, 2003)

Contudo, a sociedade ainda não possuía o conhecimento de como construí-lo.

Assim, em outubro de 1967, nasceu nos Estados Unidos o primeiro esforço para solucionar tal situação. Isto se deu com a criação de uma "força tarefa", que resultou em um documento intitulado "*Security Control for Computer System: Report of Defense Science Boad Task Force on computer Security*" [este documento foi editado por W. H. Ware], e representou o início do processo oficial de criação de um conjunto de regras para segurança de computadores, que mais tarde chegaria ao seu cume com a publicação da uma norma internacional de segurança da informação no ano de 2000, que como o nome afirma é de âmbito mundial.

Porém, este esforço não se deu somente por parte do Departamento de Defesa dos Estados Unidos (*United States Department of Defese* - DoD); a Agência Central de Inteligência (*Central Inteligency Agency*) também comprou esta briga, e iniciou o desenvolvimento do primeiro Sistema Operacional que implementava as políticas de segurança do DoD, que foi o ADEPT-50.

Em outubro de 1972, J. P. Anderson escreve um relatório técnico denominado: "*Computer Security Technologs Planning Study*", no qual ele descreve "todos" os problemas envolvidos no processo de se fornecer os mecanismos necessários para salvaguardar a segurança de computadores.

Este documento, combinado com os materiais produzidos por D.E. Bell e por L. J. La Padula, e denominados "*Secure Computer Systens: Mathematical Fundations*", "*Mathemathical Model*" e "*Refinament of Mathematical Model*", deram origem ao que ficou conhecido como "*Doctrine*", esta por sua vez seria a base de vários trabalhos posteriores na área de segurança.

Paralelamente o Coronel Roger R. Schell, da Força Aérea americana, que na época trabalhava na Divisão de Sistemas Eletrônicos - EDS (*Eletronic System Division - Air Force Systems Command*) iniciou o desenvolvimento de várias técnicas e experimentações que levariam ao surgimento do que ficou conhecido como "*Security Kernels*", que nada mais é do que os componentes principais para o desenvolvimento de um Sistema Operacional "Seguro".

Em 1977, o Departamento de Defesa dos Estados Unidos formulou um plano sistemático para tratar do Problema Clássico de Segurança, o qual daria origem ao "*DoD Computer Security Initiative*", que, por sua vez, desenvolveria a um "centro" para avaliar o quão seguro eram as soluções disponibilizadas.

A construção do "Centro" gerou a necessidade da criação de um conjunto de regras a serem utilizadas no processo de avaliação. Este conjunto de regras ficaria conhecido informalmente como "*The Orange Book*", devido a cor da capa deste manual de segurança, e o Coronel Roger Shell foi o primeiro diretor deste centro.

O processo de escrita do "*Orange Book*", conhecido oficialmente como "*Trusted Computer Evaluation Criteria* – DoD 5200.28-STD", teve o seu início

ainda no ano de 1978. No mesmo ano, a publicação da primeira versão "Draft", ou rascunho, deste manual, entretanto somente no dia 26 de dezembro de 1985 foi publicada a versão final e atual deste documento.

Graças às operações e ao processo de criação do Centro de Avaliação e do "*Orange Book*" foi possível a produção de uma larga quantidade de documento "técnicos", que representaram o primeiro passo na formação de uma norma coesa e completa sobre a segurança de computadores. A série de documentos originados pelo esforço conjunto dos membros do centro é reconhecida pelo nome de "*The Rainbow Serie*", cujos documentos continuam sendo atualizados largamente, tais documentos são distribuídos gratuitamente pela internet.

Mesmo que o "*Orange Book*" seja considerado, atualmente, um documento "ultrapassado", podemos considerá-lo como o marco inicial de um processo mundial e contínuo de busca de um conjunto de medidas que permitam a um ambiente computacional ser qualificado como seguro.

Esta norma de segurança permitiu e continua permitindo a classificação, por exemplo, do nível de segurança fornecido pelos sistemas operacionais atualmente utilizados, como são os casos do OpenBSD, do FreeBSD, do NetBSD, do Solaris, do AIX, do QNX, dos vários "sabores" de Linux e até mesmo das várias versões do Windows. Com a classificação realizada pelo "Centro" ficou mais fácil comparar as soluções fornecidas pela indústria, pelo mercado e pelo meio acadêmico de uma forma geral, o que não era possível até então.

Outro fator a ser lembrado é que o "*Orange Book*", dentro de sua "formalidade", permite, de uma maneira simples e coesa, especificar o que deve ser implementado e fornecido por um software, para que ele seja classificado em um dos níveis de "segurança" pré-estipulados, permitindo assim que este também seja utilizado como fonte de referência para o desenvolvimento de novas aplicações e para o processo de atualização ou refinamento de aplicações já existentes e em uso.

Logicamente podemos concluir que o processo de busca de soluções para os problemas de segurança em ambientes computacionais envolve a necessidade do desenvolvimento de padrões, os quais serão tanto utilizados no apoio à construção de sistemas computacionais "seguros" como para a avaliação dos mesmos. A existência de uma "Norma" permite o usuário tomar conhecimento do quão protegidas e seguras estarão as suas informações, possibilitando ao mesmo uma ferramenta que irá auxiliar a escolha de uma solução. Do ponto de vista dos profissionais técnicos, eles passarão a possuir uma ferramenta comum de trabalho, evitando assim que cada equipe tenha para si um padrão desconexo das demais equipes, dificultando aos clientes a melhor escolha.

O "*The Orange Book*" representou o marco "zero", do qual nasceram vários padrões de segurança, cada qual com a sua filosofia e métodos

proprietários, contudo visando uma padronização mundial. Houve um esforço para a construção de uma nova norma, mais atual e que não se detivesse somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação.

Este esforço foi liderado pela "*International Organization for Standardization* (ISO)". No final do ano de 2000, o primeiro resultado desse esforço foi apresentado, que é a norma internacional de Segurança da Informação ISO/IEC-17799:2000, a qual já possui uma versão aplicada aos países de língua portuguesa, denominada NBR ISO/IEC-17799.

Normas Existentes sobre Segurança

A segurança dos sistemas e informações foi um dos primeiros itens a ter padrões definidos. Esta necessidade de segurança é particularmente verdade nas transações via Internet. A gerência de segurança da informação visa identificar os riscos e implantar medidas que de forma efetiva tornem estes riscos gerenciáveis.

Uma das primeiras normas definidas foi a BS7799 - *Code of Practice for Information Security Management*. Após um trabalho intenso de consulta pública e internacionalização, em primeiro de dezembro de 2000 a norma foi aceita como um padrão internacional ISO/IEC 17799:2000.

A aderência ao ISO/IEC 17799 permite que as empresas demonstrem publicamente que foi feito um investimento no sentido de proteger a Confidencialidade, Integridade e Disponibilidade das informações. O padrão define 127 controles que permitem identificar as necessidades de segurança apropriadas para o ambiente definido como escopo do sistema de gerência de segurança a ser implantado. A norma ISO/IEC 17799 apresenta controles de segurança para implantação e administração de sistemas e redes, guias para implantação de Políticas de Segurança, planos de continuidade de negócio e aderência à legislação.

A origem da ISO/IEC 17799 remonta ao final da década de 80. Em 1987, no Reino Unido, o DTI (*Department Of Trade Centre*) criou o CCSC (*Comercial Computer Security Centre*) com o objetivo de auxiliar as companhias britânicas que comercializavam produtos para segurança de Tecnologia da Informação através da criação de critérios para avaliação da segurança.

Outro objetivo do CCSC era a criação de um código de segurança para os usuários das informações. Com base nesse segundo objetivo, em 1989 foi publicado a primeira versão do código se segurança, denominado PD0003 - Código para Gerenciamento da Segurança da Informação.

Em 1995 esse código foi revisado e publicado como uma norma britânica (BS), a BS7799:1995. Em 1996, essa norma foi proposta ao ISO para homologação mas essa foi rejeitada. Uma segunda parte desse documento foi criada posteriormente e publicada novembro de 1997 para consulta pública e

avaliação.

Em 1998 esse documento foi publicado como BS7799-2:1998. Nesse ano, a lei britânica, denominada Ato de Proteção de Dados, recomendou a aplicação da norma na Inglaterra, o que viria a ser efetivado em 1o de março de 2000.

Em maio de 2000 o BSI homologou a primeira parte da BS7799. Em outubro do mesmo ano, na reunião do comitê da ISO em Tóquio, a norma foi votada e aprovada pela maioria dos representantes. Os representantes dos países ricos, excetuando a Inglaterra, foram todos contra a homologação, mas, sob votação, venceu a maioria e a norma foi homologada em 1o. de dezembro como ISO/IEC 17799:2000.

Em abril de 2001 a versão brasileira da norma ISO foi posta em consulta pública. Em setembro de 2001, a ABNT homologou a versão brasileira da norma, denominada NBR ISO/IEC 17799.

A atual norma inglesa BS7799 não se limita a aspectos meramente técnicos de processamento, IT e redes, mas abrange todos os aspectos de segurança da organização. Os itens são:

1 Política de Segurança;
2 Organização da Segurança;
3 Gestão de Ativos;
4 Segurança de Pessoal;
5 Gestão da Segurança Física;
6 Procedimentos de Operação de Processamento de Dados e de Rede;
7 Controle de Acesso;
8 Procedimentos de Desenvolvimento e Manutenção de Sistemas;
9 Gestão da Continuidade de Negócios;
10 Aderência à Legislação.

COBIT

O CobiT (*Control Objectives for Information and related Technology*) pode ser traduzido como Objetivos de Controle para a Informação e Tecnologia relacionada. Publicado pela ISACA (*Information Systems Audit and Control Foundation*) em 1996, o CobiT está em sua terceira edição, marcando sua transferência para o *IT Governance Institute*, e acrescentando em sua estrutura as guias de gerenciamento requeridas pela governança corporativa.

O CobiT foi desenvolvido com base no consenso de especialistas de todo o mundo no que concerne as melhores práticas e metodologias, tais como códigos de conduta (Conselho Europeu, OECD, ISACA etc.) critérios de qualificação para os sistemas e processos de TI (ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria etc.), padrões profissionais para controle interno e auditoria (COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO etc.), práticas de mercado e requerimentos legais, governamentais e específicos dos

mercados que dependem fortemente de tecnologia, tais como os setores financeiro e de telecomunicações.

O grande diferencial do CobiT é sua orientação para negócios, o que vem atender as seguintes demandas:

1 Da administração e gerência, visando equilibrar os riscos e os investimentos em controles no ambiente dinâmico de TI.
2 Dos usuários, que dependem dos serviços de TI e seus respectivos controles e mecanismos de segurança para realizar suas atividades.
3 Dos auditores, que podem utilizá-lo para validar suas opiniões ou para recomendar melhorias dos controles internos à administração.

As atividades de TI são apresentadas pelo CobiT de forma lógica e estruturada, relacionando riscos de negócios, necessidades de controles e questões técnicas. O CobiT pode ser usado independentemente da plataforma tecnológica adotada pela organização e se aplica também a qualquer segmento de indústria.

O CobiT agrupa os processos de TI em 4 domínios abrangentes:
1 Planejamento e Organização
2 Aquisição e Implementação
3 Entrega e Suporte
4 Monitoramento

O CobiT contém 34 Objetivos de Controle de alto nível e 318 objetivos detalhados para os processos de TI. Esses Objetivos de Controle são suportados pelos Guias de Auditoria que possibilitam aos auditores e gerentes revisarem os processos específicos de TI assegurando que os controles sejam suficientes ou que necessitam de melhorias. O terceiro principal componente do CobiT são os Guias de Gerenciamento.

TESTES E EXERCÍCIOS

Relacione os dez recursos de informática mais importantes de sua organização e as dez ameaças de maior gravidade e justifique.

Estruture um *check list*, com as dez questões principais que, em sua opinião, devam ser contempladas para auditoria da segurança de um sistema aplicativo.

QUESTÕES A CONSIDERAR

Quais os eventos determinantes do ciclo administrativo (planejamento, execução, controle, auditoria), em cada nível administrativo (operacional, tático, estratégico), da segurança em informática de sua organização ?

Por que segurança em informática é um elemento básico da qualidade em informática ?

Quais as práticas de gestão estratégica e tática vigentes em sua organização ?

Referências Bibliográficas

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. Editora Atlas. São Paulo, 2000.

-------. **NBR ISO/IEC 17799 – Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2003.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Axcel Books. Rio de Janeiro, 2000.

WADLOW, Thomas. **Segurança de Redes**. Editora Campus. Rio de Janeiro, 2000.

ABREU, Dimitri. **Melhores Práticas para Classificar as Informações**. Módulo e-Security Magazine. São Paulo, agosto 2001. Disponível em www.modulo.com.br. Acessado em: 17/03/2004.

DeMARCO, Tom e LISTER Timothy. **Peopleware – Como Gerenciar Equipes e Projetos Tornados-os mais Produtivos**. Editora McGraw-Hill. São Paulo, 1990.

SHIREY, R. **RFC 2828 – Internet Security Glossary**. The Internet Society, 2000. Disponível em: http://www.ietf.org/rfc/rfc2828.txt?number=2828. Acessado em: 08/04/2004.

KRAUSE, Micki e TIPTON, Harold F. **Handbook of Information Security Management**. Auerbach Publications, 1999.

LAUREANO, Marcos Aurelio Pchek. **Uma Abordagem Para a Proteção de Detectores de Intrusão Baseadas em Máquinas Virtuais**. Dissertação de Mestrado apresentado ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná, 2004.

KATZAM JR, Harry. **Segurança de em Computação**. Editora LTC. Rio de Janeiro, 1977.

MARTIN, James. **Engenharia da Informação – Introdução**. Editora Campus. Rio de Janeiro, 1991.

SYNNATT, William R. **The Information Weapon – Winning Customers and Markets with Tecnhonology**. Editora John Wiley & Sons, 1987.

FELICIANO NETO, Acácio; FURLAN, José Davi e HIGO, Wilson. **Engenharia da Informação – Metodologia, Técnicas e Ferramentas**. Editora McGraw-Hill. São Paulo, 1988.

BORAN, Sean. **IT Security Cookbook**, 1996. Disponível em http://www.boran.com/security/. Acessado em: 17/03/2004.

STONEBURNER, Gary. **Underlying Technical Models for Information Technology Security**. NIST Special Publication 800-33, 2001.

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. **Segurança no Desenvolvimento de Software – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408**. Editora Campus. Rio de Janeiro, 2002.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma visão Executiva**. Editora Campus. Rio de Janeiro, 2003.

CROSBY, Philip B. **Qualidade é Investimento**. José Olympio Editora. 5ª Edição, Rio de Janeiro, 1992.

SANDHU, Ravi S. e SAMARATI, Pierangela. **Authentication, Acess Control, and Intrusion Detection**. IEEE Communications, 1994.

DUARTE Júnior, Antonio Marcos. **A importância do Gerenciamento de Riscos Corporativos**. UNIBANCO – Global Risk Management. Disponível em: http://www.risktech.com.br/. Acessado em: 11/04/2004.

LEVESON, Nancy G. et al. **Analyzing Software Specifications for Mode Confusion Potential**. Workshop on Human Error and System Development, 1997.

LASALA, Kenneth P. **Human Performance Reliability: A Historical Perspective**. IEEE Transactions on Reliability, vol 47, 1998.

------. **BS 7799-2 – Code of Practice for Information Security Management – Part 2: Specification for Information Security Management Systems**. British Standards Institute, Londres – UK, 2002.

SCOY, Roger. L. **Software Development Risk: Opportunity, Not Problem**. Technical Report CMU/SEI-92-TR-30. Carnegi Melon University, 1992.

AHMAD, David R. Mirza e RUSSEL, Ryan. **REDE SEGURA NETWORK**. Alta Books, 2002.

CULP, Scott. **10 Immutable Laws of Security. Microsoft TechNet**. Disponível em: http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx. Acessado em 20/09/2004.

ABREU, Dimitri. **Política de Segurança - Definir para implementar**. Módulo Security Magazine, 2002. Disponível em:

http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=287&pagecounter=0&idiom=0. Acessado em: 21/09/2004
LAUDON, Kenneth C. e LAUDON, Jane P. **Sistemas de Informação Gerenciais**. Prentice Hall; São Paulo, 2004.

LAUREANO, Marcos Aurelio Pchek. **Firewall com IPTABLES no LINUX**, 2002. Disponível em: http://www.ppgia.pucpr.br/~laureano/guias/GuiaFirewallIptables.htm. Acessado em: 24/09/2004.

ALMEIDA, Gilberto Martins de. **Internet, segurança e leis Como o Direito lida com questões de informática ?**, 2001. Disponível em: http://www.radiobras.gov.br/ct/artigos/2001/artigo_220601.htm. Acessado em: 30/09/2004.

RAVANELLO, Anderson Luiz; HIJAZI, Houssan Ali; MAZZORANA, Sidney Miguel. **Honeypots e Aspectos Legais**, 2004. Dissertação de Especialização em Redes e Segurança – Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática Aplicada. Curitiba - PR.

PLACHTA, Claudio. **Plano de Continuidade de Negócios - Garantindo a sobrevivência**, 2001. Módulo Security Magazine. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=249&pagecounter=0&idiom=0. Acessado em: 01/02/2004.

GONÇALVES, Luís Rodrigo de Oliveira. **Pequeno histórico sobre o surgimento das Normas de Segurança**, 2003. Módulo Security Magazine. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=344&pagenumber=0&idiom=0. Acessado em: 30/03/2004.

CHIN, Liou Kuo. **Rede Privada Virtual - VPN**, 1998. Boletim bimestral sobre tecnologia de redes. RNP – Rede Nacional de Ensino e Pesquisa, 1998. Vol. 2, Nº 8. Disponível em: http://www.rnp.br/newsgen/9811/vpn.html. Acessado em: 16/10/2004.