UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE
DEPARTAMENTO DE ADMINISTRAÇÃO

A AUDITORIA DE INFORMÁTICA FACE AO COMÉRCIO ELETRÔNICO ATRAVÉS DA INTERNET - UM ESTUDO NO SETOR FINANCEIRO

FERNANDO JOSÉ DE ARAUJO SILVA

Orientador Prof. Dr. Hiroo Takaoka

São Paulo

2000

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE
DEPARTAMENTO DE ADMINISTRAÇÃO

A AUDITORIA DE INFORMÁTICA FACE AO COMÉRCIO ELETRÔNICO ATRAVÉS DA INTERNET - UM ESTUDO NO SETOR FINANCEIRO

FERNANDO JOSÉ DE ARAUJO SILVA

Dissertação apresentada ao Departamento de Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, para obtenção do título de Mestre em Administração de Empresas.

Área de Concentração:
Métodos Quantitativos e Informática

Orientador:
Prof. Dr. Hiroo Takaoka

São Paulo

2000

REITOR DA UNIVERSIDADE DE SÃO PAULO

Prof. Dr. Jacques Marcovitch

DIRETOR DA FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE

Prof. Dr. Eliseu Martins

CHEFE DO DEPARTAMENTO DE ADMINISTRAÇÃO

Prof. Dr. Claudio Felisone de Angelo

Agradecimentos

Registrar o agradecimento é o mínimo que posso fazer como reconhecimento pela ajuda, compreensão e estímulo que recebi das pessoas com que convivi durante a elaboração desta dissertação.

Prof. Dr. Hiroo Takaoka, meu orientador, que estimulou, aconselhou, criticou e orientou de maneira segura este meu trabalho até sua conclusão, respeitando minha forma de trabalhar.

Os profissionais da organização pesquisada, meus colegas de trabalho, que participaram e contribuíram para o estudo de caso.

Meus familiares, em especial minha esposa, **Miriam,** e meus filhos, **Juliana** e **Eduardo**, por sua grande paciência, colaboração e incentivo à realização deste trabalho, mesmo nos momentos de maior dificuldade.

Fernando José de Araujo Silva

RESUMO

O comércio eletrônico praticado através da Internet vem crescendo significativamente e tem potencial para crescimento ainda mais elevado. Todavia, ao atuar na rede, as organizações podem tornar seu ambiente de processamento de informações vulnerável a ataques externos, comprometendo assim a integridade, disponibilidade e confidencialidade destas informações.

A função da auditoria de informática é avaliar os controles no ambiente de tecnologia da informação para auxiliar a organização a operar assumindo um nível de risco aceitável por sua administração. Com a atuação da organização na Internet, o ambiente de tecnologia da informação modificou-se e a auditoria de informática precisa adaptar-se para atuar nesta nova realidade.

Este trabalho tem como objetivo identificar os aspectos de segurança associados à prática do comércio eletrônico através da Internet e como a auditoria de informática pode avaliá-los para fornecer à administração da organização uma informação isenta e fundamentada dos riscos existentes. Sua realização envolveu pesquisa bibliográfica e estudo de caso focando atuação da auditoria de informática de uma instituição financeira onde se pratica o comércio eletrônico através da Internet.

ABSTRACT

The electronic commerce done by Internet has been increasing significantly and has potential to increase even more. Nevertheless, when in the Web, the organizations may make their technology information environment vulnerable for external attacks, jeopardizing the integrity, availability and confidentiality of the information.

The role of the system audit is to assess the controls within the information technology environment to help the organization operate taking a risk level acceptable by their management. With the organization operating in the Web, the information technology environment has changed and the system audit should adapt itself to act in this new reality.

This work intends to identify the security aspects related to making business through Internet and how the system audit can assess them to give the organization management reliable information about the real risks. Its accomplishment has involved a bibliographic survey and a case study addressing the role of the system audit in a financial institution where electronic commerce is practiced through the Web.

SUMÁRIO

APÊNDICES

Capítulo 1

INTRODUÇÃO

1.1 O comércio e a evolução tecnológica

O comércio (considerado dentro do conceito de troca, de compra e venda de bens, serviços ou valores) é uma atividade intrínseca à natureza humana porque, através dela, as pessoas obtêm satisfação de suas necessidades e desejos. Está associado à história humana desde seu início e a maneira como é realizado avança acompanhando o desenvolvimento da civilização, aproveitando as inovações tecnológicas.

Ilustrando a evolução experimentada pelo comércio, pode-se comparar o início dos tempos e a fase em que as técnicas de navegação já tinham sido dominadas. Se, no início, a prática comercial envolvia apenas negociação direta entre fornecedor e consumidor, já que ambos estavam no mesmo ambiente, quando o homem aprendeu a transitar pela água, expandiu-se, até vencer os limites continentais.

A estreita ligação entre o desenvolvimento tecnológico e a forma de realizar a arte do comércio ainda é uma realidade no presente. Os recursos da eletrônica, particularmente nas áreas de computação e telecomunicações, permitiram o surgimento do comércio eletrônico, isto é, como define Albertin (1999) "a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio" .

Os avanços tecnológicos também permitiram o surgimento da Internet: uma rede que, criada inicialmente com objetivos militares, foi adotada no meio acadêmico e, passou a ser utilizada pelo público, de maneira geral. A velocidade com que esta rede se expande é significativa, conforme revela estudo citado por Santos e Gimenez (1998), apresentado na Tabela 1.1:

Tabela 1.1 *Mídia e Tempo Gasto para se Alcançar 50 Milhões de Habitantes*

MÍDIA	*ANOS*
Rádio	*38*
TV	*14*
TV a Cabo	*10*
Internet	*5*

Fonte: Santos e Gimenez (1998), citando Morgan Stanley Technology Research.

O comércio eletrônico efetuado através da Internet tem um potencial de crescimento bastante significativo, podendo-se afirmar que existe um efeito semelhante ao experimentado quando as técnicas de navegação foram dominadas: as possibilidades de comércio romperam os limites locais, passando a ser globais.

possibilidades de comércio romperam os limites locais, passando a ser globais. Matéria publicada na revista Exame (nº12, 16/junho/1999, p. 151), citando pesquisa da Forrester Research, dá uma idéia do volume já negociado e do potencial de crescimento, conforme demonstrado na Tabela 1.2.

Tabela 1.2 - Comércio através da Internet (em US$ bilhões)

Ano	Comércio no Mundo	Nos Estados Unidos
1998	80	51
1999	170	127
2000	390	284
2001	970	551
2002	2.000	919
2003	3.200	1.439

Fonte:"Explosão do Comércio Eletrônico" Revista Exame, nº 12, 16/06/99, p. 151, citando pesquisa da Forrester Research

Esta mesma matéria destaca a evolução das operações no Brasil, citando duas empresas nacionais: o Grupo Pão de Açúcar, e o Bradesco, conforme apresentado na Tabela 1.3.

Tabela 1.3 - Uso da Internet em empresas nacionais

Período	Pedidos feitos pela Internet no Pão de Açúcar (em % sobre total de encomendas	Clientes que usam o Internet Banking, do Bradesco (em % sobre total de clientes)
1996	4	0,5
1997	8	2,5
1998	16	7,0
até maio/99	24	9,5

Fonte: "Explosão do Comércio Eletrônico" Revista Exame, nº 12, 16/06/99, p. 151, citando as empresas como fonte

A evolução da quantidade de usuários da Internet pode explicar este crescimento acelerado no tamanho do mercado através da rede. Este crescimento pode ser visualizado na Tabela 1.4, também extraída da Revista Exame.

Tabela 1.4 - Quantidade de usuários da Internet (em milhões de pessoas)

Ano	No Brasil	Na América Latina	No Mundo
1997	1,2	2,2	87
1999	3,8	7	196
2002	7,7	16	399

Fonte: "Sucesso.com" Revista Exame, nº 15, 28/07/99, p. 74, citando pesquisa da International Data Corporation

A realidade trazida pela nova tecnologia mudou significativamente os antigos métodos de realizar negócios. O deslocamento físico não é imprescindível, a validação para confirmar identidade do parceiro deixou de ser visual ou baseada em documentos físicos, a velocidade em que as transações são efetivadas é praticamente instantânea. Juntamente com a ampliação das possibilidades comerciais trazidas pela Internet, se vê também a ampliação dos riscos aos quais os negócios estão expostos. Salvaguardas que existiam anteriormente, como barreiras físicas de acessos aos centros de processamento de dados e usuários previamente conhecidos não são mais suficientes na nova realidade.

1.2 Formulação da situação problema

Apesar de todo potencial representado pelo universo que se abre frente às empresas com o comércio eletrônico através da Internet, ele ainda padece de desconfiança tanto do ponto de vista da empresa quanto dos clientes. Esta desconfiança existe em três eixos principais:

- **Acesso ao interior das empresas**

  Ao se colocar na rede, as empresas podem abrir seu interior para a visita de pessoal indesejável: os "hackers" e a versão maligna deste grupo: os "crackers". De acordo com o jargão existente no meio, os "hackers" são os invasores de sistemas que têm uma abordagem mais "romântica": invadem sistemas apenas movidos pelo espírito de aventura, de desafio, sem intenção deliberada de causar danos; caso estes ocorram, terá sido mero "acidente de trabalho". Os "crackers", pelo contrário, têm intenção de trazer prejuízo à instituição invadida, seja pela apropriação indevida de informações internas de natureza confidencial (para comercialização), seja para danificar suas informações e sistemas internos.

- **Acesso às informações que transitam na rede**

  As informações ao transitarem na rede podem ser interceptadas e utilizadas de maneira indevida. Esta ameaça paira sobre cada parte envolvida no negócio. Como exemplo de informações que se tornam vulneráveis quando em trânsito pode-se destacar, dentre outras, número e característica do cartão de crédito que está sendo utilizado para pagamento, dados de operações que uma empresa realiza com seus parceiros comerciais, movimentações realizadas entre uma instituição financeira e seus clientes, etc.

- **Autenticação das partes envolvidas em negócios através da rede**

  As movimentações efetuadas devem permitir garantia às partes envolvidas no negócio que o parceiro é autêntico e que não exista repúdio indevido (uma das partes alegar que não era de seu conhecimento a transação efetuada em seu nome)

Zboray (1998) comenta que muitos participantes do GartnerGroup's U.S. Symposium, realizado em outubro/97, tinham como grande preocupação a habilidade para negociar com segurança através da Internet. Empresas do setor financeiro, educacional, varejista, químico, e de seguro-saúde expressaram preocupação sobre o estabelecimento de comunicações seguras com seus clientes e parceiros comerciais. Os pontos vulneráveis compreendem desde a ferramenta de acesso do usuário ("user browser") até os recursos internos da empresa que permitem tornar o serviço disponível (arquivos e aplicativos internos).

Além dos controles específicos para as operações realizadas através da rede, não se deve ignorar o risco que a empresa tem com seus usuários internos. É importante destacar também este ângulo porque, independentemente da empresa ter excelentes controles para supervisionar suas operações através da rede, se seu ambiente interno for vulnerável, o risco de desvios é significativo. Para destacar a importância que deve ter a atenção com o ambiente interno, pode-se citar dados obtidos no levantamento efetuado pela Módulo (empresa de consultoria especializada em segurança para redes) junto a 148 executivos representantes de instituições financeiras, grandes indústrias e órgãos públicos. Neste levantamento, "5ª Pesquisa Nacional sobre Segurança de Informação", efetuado em setembro/99 e divulgado na íntegra em fevereiro/2000, identificou-se que 30% das empresas brasileiras sofreram algum tipo de invasão nos últimos dois anos, sendo que metade destes ataques ocorreram nos 6 meses anteriores à pesquisa. Os autores dos ataques em 35% dos casos foram os próprios funcionários da empresa, contra 17% causados por hackers, conforme pode ser visualizado na Tabela 1.5.

Tabela 1.5
Responsáveis por ataques a informações internas da empresa

Responsável	*%*
Funcionários	*35*
Hackers	*17*
Fornecedores ou Prestadores de Serviço	*9*
Clientes	*6*
Concorrentes	*2*
Outros	*6*
Origem não identificada	*25*

Fonte: 5ª Pesquisa Nacional sobre Segurança da Informação, efetuada pela Módulo, disponível (em março/2000) no site www.modulo.com.br

O prejuízo destes ataques é preocupante embora não tenha sido perfeitamente quantificado. Apenas 19% das empresas atacadas apuraram suas perdas e, em 13% destas organizações, o prejuízo ultrapassou R$ 1 milhão.

A mesma pesquisa da Módulo citava o registro pelo FBI de US$ 123 milhões em prejuízos decorrentes de crimes de informática nos Estados Unidos em 1999. Este número contabilizava apenas as empresas que conseguiram calcular suas perdas (31% do total), com um prejuízo médio de US$ 227 mil por ocorrência.

1.3 Objetivo do estudo

Este trabalho está assumindo como premissa que as informações da organização devem atender três exigências básicas:

- **integridade**

  As informações não podem ter sido corrompidas

- **disponibilidade**

  As informações devem estar disponíveis no formato e no momento oportuno para serem utilizadas no processo comercial

- **confidencialidade**

  Supõe-se que nenhuma entidade, seja pessoa física ou jurídica, se sente confortável ao tomar conhecimento que suas informações relevantes estão vulneráveis a serem expostas a fontes não autorizadas.

A implementação de controles que permitam à organização assegurar que estas exigências estejam sendo atendidas já era muito importante quando esta operava em um ambiente com fronteiras perfeitamente definidas. Com a introdução do fator atuação na Internet no processo comercial, estes controles passaram a ser fundamentais pois, no caso de não cumprirem seu papel, podem até mesmo comprometer a sobrevivência da organização que se propõe a praticar o comércio eletrônico através da rede.

A avaliação dos controles existentes para assegurar que as empresas operem correndo um risco compatível com o aceito por seus proprietários é uma responsabilidade histórica da Auditoria. Attie (1983) define que os profissionais desta área têm a missão de zelar para que "todos os procedimentos internos e as rotinas de trabalho estejam sendo habilmente executados e de forma tão boa quanto aquela exercida pelo próprio dono". Paula (1999) particulariza esta responsabilidade na auditoria interna ao afirmar que:

> *A Auditoria Interna é responsável pela avaliação da eficiência e da eficácia da entidade e, portanto, co-responsável pelo seu resultado.*
>
> *Fornecer informações que subsidiem os gestores da companhia no cumprimento cada vez melhor de sua missão é a tarefa mais importante da Auditoria Interna.*

A atuação do auditor no ambiente informatizado requer dele conhecimentos específicos de tecnologia de informações. Tal necessidade fez surgir o auditor de informática ou de sistemas, cuja atuação, como define Gil (1999) é "de correlação e comprovação da funcionalidade e da efetividade dos sistemas de informações computadorizados".

O assunto Comércio Eletrônico é relativamente novo e ainda pouco estudado na comunidade acadêmica. Mesmo estes trabalhos não enfocam especificamente a atuação da auditoria nesta nova realidade. O desafio que este ambiente representa para o auditor e os novos riscos organizacionais trazidos pela nova tecnologia ainda carecem de pesquisa e é nesse sentido que se realiza este trabalho. Buscou-se, através dele, obter resposta às seguintes questões:

1. O que é a Internet?
2. Quais os riscos que a organização se expõe ao atuar na Internet e quais os mecanismos que podem mitigar estes riscos?
3. O que é auditoria e como ela contribui para administração de uma organização?
4. Como é a atuação da auditoria de informática em organização financeira onde se pratica o comércio eletrônico através da Internet?
5. Como uma organização desenvolve habilidade para efetuar auditoria em ambiente onde se pratica comércio eletrônico através da Internet?
6. Quais são as competências exigidas do auditor de informática para atuar neste novo ambiente?

A busca às respostas das questões 1 a 3 foi conduzida através de pesquisa em bibliografia especializada e em instituições de auditoria e segurança. A resposta à questão 4 foi buscada também em pesquisa bibliográfica, complementada com um estudo de caso em uma instituição que pratica o comércio eletrônico através da Internet. As respostas às questões 5 e 6 foram buscadas através do estudo de caso. O objeto deste estudo de caso foi uma instituição financeira nacional de grande porte.

Este trabalho tem seu foco dirigido para validação da tecnologia que proporciona controles para as operações realizadas através da Internet. Não estão sendo contemplados outros aspectos ligados à auditoria (como auditoria fiscal, de crédito, operacional, etc.), mesmo que envolvam auditoria de comércio eletrônico através da Internet.

1.4 Plano do Trabalho

Este trabalho está organizado em 8 capítulos, conforme sucintamente detalhado a seguir:

No capítulo 1 - "Introdução" - são apresentados os objetivos do trabalho, as justificativas para a escolha do tema e o plano de trabalho.

O capítulo 2 - "O Contexto da Auditoria no Comércio Eletrônico Através da Internet" - apresenta o modelo de referência utilizado para estudo do assunto e descreve o ambiente Internet, destacando os aspectos externos e organizacionais envolvidos na prática de comércio através deste ambiente.

No capítulo 3 - "Ambiente Tecnológico" - são destacados os aspectos do ambiente tecnológico que podem prover segurança ao ambiente.

No capítulo 4 - "Ambiente de Auditoria" - descreve-se como é a atuação da auditoria de maneira geral e da auditoria de informática em particular.

No capítulo 5 - "Auditoria no Comércio Eletrônico através da Internet" - são apresentadas abordagens para auditoria no novo ambiente.

No capítulo 6 - "Metodologia" - são apresentados os critérios que orientaram a pesquisa.

No capítulo 7 - "A Pesquisa" - está descrita a instituição pesquisada e apresentadas as observações efetuadas durante o estudo do caso.

No capítulo 8 - "Conclusão" são apresentadas as conclusões finais do trabalho, suas limitações, recomendações e perspectivas para a realização de novas pesquisas no futuro.

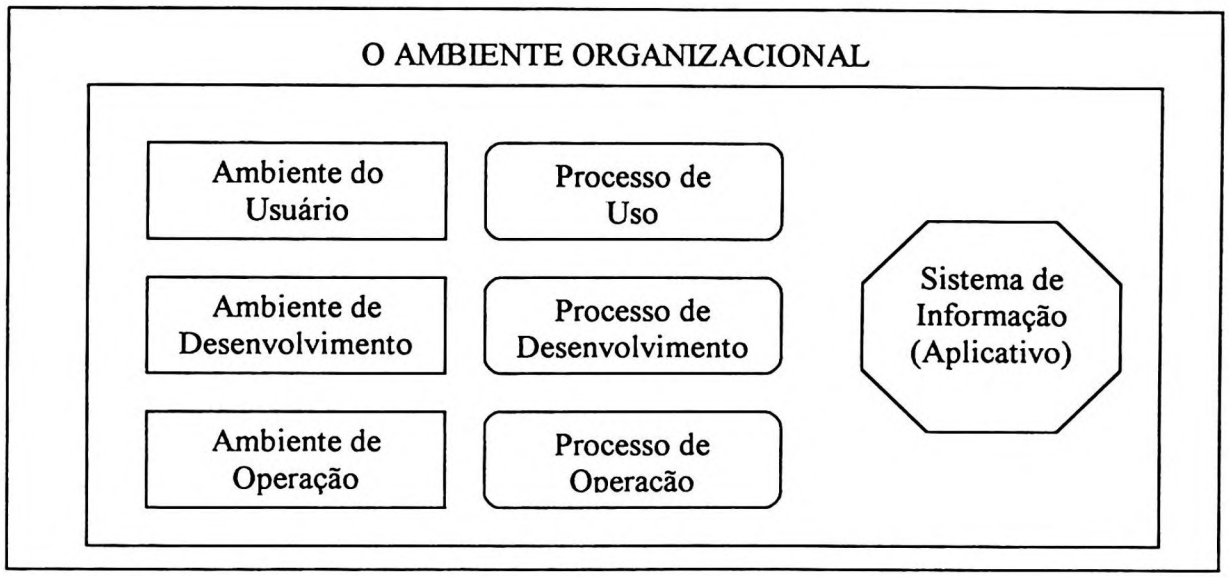
Capítulo 2

O CONTEXTO DA AUDITORIA NO COMÉRCIO ELETRÔNICO ATRAVÉS DA INTERNET

2.1 O Modelo de Referência

Este trabalho baseou-se em um modelo teórico proposto por Ives et al. (1980), no qual o sistema aplicativo é afetado pelo ambiente externo, pelo ambiente organizacional e por características internas à organização associadas ao ambiente do sistema e ao seu processo, conforme demonstrado na Figura 2.1.

Figura 2.1 - Um modelo para pesquisa de sistema de informação



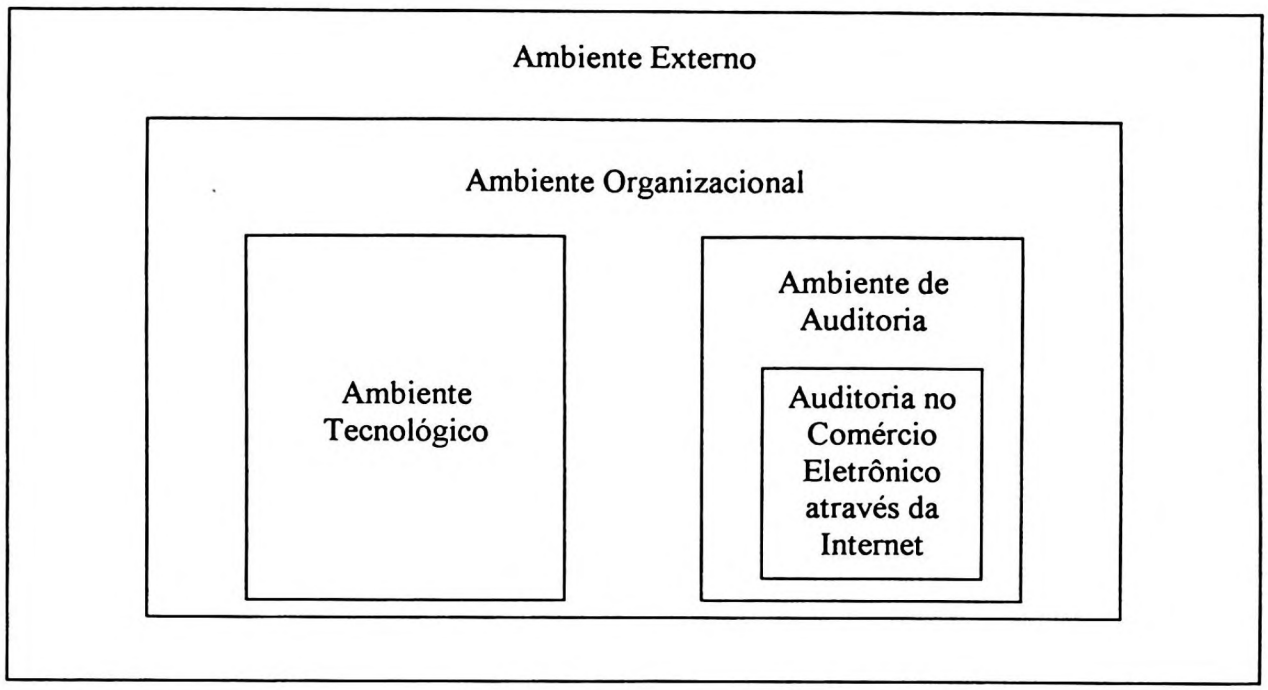
Fonte: Ives et al. (1980)

O ambiente externo compreende considerações legais, sociais, políticas, culturais, econômicas, educacionais e de recursos. O ambiente organizacional envolve metas organizacionais, atividades, estrutura, volatilidade e estilo / filosofia gerencial. O ambiente do usuário diz respeito às decisões tomadas com base na saída do sistema. O ambiente de desenvolvimento consiste em métodos e técnicas de desenvolvimento. O ambiente de operações incorpora os recursos necessários à operação do sistema. O aplicativo compreende a saída do sistema de informação, considerando seu conteúdo, forma de apresentação e periodicidade (on-line ou não).

Combinando-se o modelo proposto por Ives et al (1980) ao raciocínio dedutivo e indutivo, baseado na literatura pesquisada, formulou-se um modelo teórico para estudo dos fatores que influenciam a auditoria de informática em organizações onde

se pratica o comércio eletrônico através da Internet. Este modelo, esquematizado na Figura 2.2, é composto por 4 contextos: o ambiente externo, o ambiente organizacional, o ambiente tecnológico e o ambiente de auditoria.

Figura 2.2 - Modelo para auditoria no comércio eletrônico através da Internet



No contexto externo é considerada a evolução tecnológica e a Internet, como ferramenta que permite às organizações ampliarem sua fronteira de atuação.

No contexto organizacional considera-se a postura da instituição para atuar neste novo ambiente no que diz respeito à preocupação com segurança e controles. Esta preocupação está focada nos processos que buscam fornecer uma razoável segurança quanto à eficiência e eficácia das operações, isto é, que tais operações sejam realizadas usando os recursos adequados e atendendo às necessidades da organização.

O ambiente tecnológico envolve a plataforma tecnológica que provê controles para permitir à organização atuar na Internet de forma razoavelmente segura.

O ambiente de auditoria compreende a estrutura e o funcionamento da auditoria, com seus métodos, políticas de trabalho e formas de atuação. Envolve o posicionamento da auditoria para conduzir seus trabalhos atendendo aos anseios da organização. Uma ênfase especial é dada à auditoria especializada na verificação se os recursos de tecnologia estão sendo adequadamente utilizados para fornecer à organização as informações que esta necessita para cumprir sua finalidade.

A auditoria de informática no comércio eletrônico através da Internet envolve a atuação da auditoria na avaliação dos riscos e dos controles associados à condução

dos processos comerciais através da Internet. Esta avaliação visa verificar se os processos estão sendo conduzidos a um nível de risco conhecido e aceito pela organização.

Nas próximas seções deste capítulo estão sendo apresentados, de forma sucinta, os fatores que permitiram às organizações expandirem sua fronteira de atuação e as preocupações associadas à atuação neste novo ambiente (descritos no modelo como ambiente externo e ambiente organizacional).

Nos capítulos 3 a 5 são apresentados em maiores detalhes o ambiente tecnológico, o ambiente de auditoria e a auditoria no comércio eletrônico através da Internet.

2.2 Comércio, mercado, a corporação virtual e a economia digital

Pode-se considerar o comércio como a forma civilizada como os seres humanos procuram suprir suas necessidades básicas através da aquisição de produtos. Esta forma Kotler (1994) chama de troca: "o ato de obter um produto desejado de alguém, oferecendo-se algo em contrapartida". Segundo ele, para que ocorra troca, cinco condições devem ser atendidas:

- Há pelo menos duas partes envolvidas
- Cada parte tem algo que pode ser de valor para a outra
- Cada parte tem capacidade de comunicação e entrega
- Cada parte é livre para aceitar ou rejeitar a oferta
- Cada parte acredita estar em condições de lidar com a outra

Esta atividade e o ambiente onde é praticada (o mercado) também são objeto de estudo da microeconomia. Pindyck e Rubinfeld (1991) apontam que esta ciência estuda o comportamento das unidades econômicas individuais (isto é consumidores, trabalhadores, investidores e proprietários de recursos) e como estas unidades tomam decisões econômicas.

Pindyck e Rubinfeld (1991) dividem as unidades econômicas em dois grupos, segundo sua função, que interagem formando os mercados. Estes grupos são:

- compradores, que abrangem os consumidores (adquirentes de bens e serviços) e as empresas (adquirentes de trabalho, capital e matérias-primas que utilizam para produzir bens e serviços); e
- vendedores, isto é, as empresas (que vendem bens e serviços), os trabalhadores (que vendem seus serviços por meio do trabalho) e os proprietários de recursos, que arrendam estes ativos ou os comercializam com as empresas.

Com a evolução do conhecimento, o comércio procura se sofisticar cada vez mais, visando permitir que os compradores sejam melhor atendidos, aumentando o retorno dos vendedores e permitindo seu crescimento. Esta busca contínua da melhoria é o que Davidow e Malone (1992) chamam de produto ou serviço virtual, isto é, aquele que "é produzido instantaneamente e sob medida, em resposta à demanda do cliente". Para tornar possível esta função, os vendedores devem controlar tipos cada

vez mais sofisticados de informações e dominarem todas as novas práticas organizacionais e de produção. As instituições que desenvolverem esta habilidade (as "corporações virtuais") serão mais competitivas porque poderão produzir a um custo menor produtos mais adequados às necessidades de seus clientes.

Com a evolução tecnológica e o advento da redes, a economia passou a ser o que Tapscott (1995) chamou de a "economia digital":

> *A economia para a idade da inteligência em rede é uma economia digital. Na velha economia, o fluxo de informação era físico: dinheiro, cheques, faturas, notas de embarque, relatórios, reuniões face-a-face, [...] Na nova economia, a informação e todas as suas formas tornaram-se digitais - reduzidas a bits armazenados em computadores e correndo à velocidade da luz através das redes. Usando este código binário, informação e comunicação transformam-se em dígitos um e zero.*

A evolução tecnológica está fazendo surgir uma nova economia, segundo Tapscott (1995) e passamos a viver a "idade da areia". Através da história, revoluções nos recursos naturais têm classificado novos paradigmas em ferramentas (por exemplo, pedra, bronze, etc.), que levam a novos modos de criação de riqueza e desenvolvimento social. A situação atual pode ser chamada de idade da areia: os assuntos de comércio, transações de negócio, comunicações humanas, e descobertas científicas são todas reduzidas a mudanças em partículas de silício e transmitidas através de fibras óticas, ambas derivadas da areia.

Esta nova realidade anunciada por Tapscott pode ser sintetizada com o uso em larga escala da rede mundial, a Internet. Esta rede permitiu tornar mais próxima da realidade a corporação virtual visualizada por Davidow e Malone em 1992.

2.3 A Internet

Laudon e Laudon (1996) definem a Internet como "a rede internacional de redes conectando mais de 20 milhões de pessoas em 100 países; ela é a maior auto-estrada de informação ("information superhighway") no mundo". Por definição de seus idealizadores (o Departamento de Defesa, do Governo Americano), ela não tem um proprietário nem uma organização gerencial formal. Isto ocorre para torná-la menos vulnerável a ataques terroristas ou de inimigos na situação de uma guerra. Mesmo que um ou mais nós da rede sejam desfeitos, a informação continuará fluindo por outros caminhos. Para se filiar à Internet, uma rede necessita apenas pagar uma pequena taxa e acertar protocolo de comunicação baseado no TCP/IP (Transmission Control Protocol/Internet Protocol). As redes que se conectam à Internet se comprometem a transferir mensagens para outras redes sem cobrança de taxa adicional por esta transferência.

Além do baixo custo, o que permitiu à Internet tornar-se um meio extremamente forte de comunicação, também segundo Laudon e Laudon (1996), foi a ferramenta de fácil uso para oferecer produtos e serviços: a World Wide Web (WWW). Esta

ferramenta é um padrão para armazenamento, recuperação, formatação e apresentação das informações, que utiliza arquitetura "cliente/servidor" e interface gráfico para permitir fácil visualização. Baseia-se em uma linguagem de hipertexto chamada *Hipertext Markup Language (HTML)* que formata os documentos e incorpora ligações dinâmicas com outros documentos e quadros gravados no mesmo computador ou em outros remotos.

Garfinkel e Spafford (1997) descrevem que o modelo "cliente/servidor", que sustenta a maioria dos serviços da Internet, está baseado na solicitação de serviço de um programa para outro, sendo que os dois programas podem estar sendo processados no mesmo computador ou, como ocorre na maioria dos casos, em computadores diferentes. O programa que solicita o serviço, é chamado *cliente* e o que responde à solicitação é o chamado *servidor*. Para ser mais rigoroso, do ponto de vista técnico, o *cliente* normalmente é um computador pessoal, enquanto que o *servidor* é um equipamento de maior capacidade operando em Unix, Windows NT ou outro sistema operacional.

Ainda segundo Garfinkel e Spafford (1997), a WWW foi inventada em 1990 por Tim Bernes-Lee, quando estava na base suíça do European Laboratory for Particle Physics (CERN) para evitar que os arquivos contendo trabalhos científicos tivessem que ser transferidos e impressos através da rede. Este produto foi originalmente criado para computadores NeXT e adaptado posteriormente pelo pessoal da Universidade de Illinois que escreveu um navegador para a rede ("browser") chamado "Mosaic", para uso em sistemas operacionais Macintosh e Windows. O potencial comercial desta invenção foi visualizado por Jim Clark, um empresário do Vale do Silício que se associou ao líder do projeto que criou o "Mosaic", Mark Andreessen, e fundou a "Mozilla". Esta empresa logo mudou seu nome para "Netscape Communications" e o browser foi renomeado para "Netscape Navigator"

Além dos conceitos acima, e no âmbito deste trabalho, é importante destacar inicialmente três outros termos utilizados rotineiramente quando se fala em Internet: *"URL"*, *"Web Site"* e *"Portal"*. Fluss e Harris (1999) assim definem estes termos:

- *URL (Uniform Resource Locator)* é o conjunto de caracteres, ou endereço na rede (*Web address)*, que identifica o nome e localização exatos de um documento (ou de um *site*) na Internet
- *Web Site* é a coletânea de arquivos acessados através de um endereço da rede, cobrindo um tema ou assunto específico, e administrado por uma pessoa ou por uma organização em particular. Sua página de abertura é chamada *home page.* Um Web Site reside em servidores conectados à rede Web e seu conteúdo está disponível a qualquer usuário, em qualquer lugar do mundo, de forma contínua (24 horas por dia, 7 dias por semana). Os Web sites normalmente utilizam *Hipertext Markup Language (HTML)* para dar formato e apresentar informações e para prover facilidades de navegação que capacitem os usuários a se movimentar no site e através da rede
- *Portal* é um Web Site de grande tráfego, geralmente atraente, que contem um amplo leque de conteúdos, serviços e conexões a fornecedores (*"vendor links"*). Este site atua como um intermediário, agregando valor através da seleção de

fontes de conteúdos (em geral outros sites) e reunindo-os de maneira a facilitar a apresentação e navegação ao usuário final.

Através da "Information Superhighway" pessoas podem se comunicar de maneira interativa, pedir produtos e serviços, realizar transações de negócios com seus fornecedores e instituições financeiras, entre muitas outras possibilidades. Com ela, o comércio eletrônico rompeu qualquer limite físico e passou para um mundo virtual e sem barreiras. Afinal, este recurso permite que um fornecedor (que pode ou não ser uma empresa), possa ofertar seus produtos através da rede e esta oferta ser percebida e acatada por um consumidor (pessoa física ou jurídica) de qualquer outra parte do mundo. A liquidação financeira deste negócio poderá ser feita utilizando-se transferência de recursos entre instituições financeiras, que poderão estar ainda em outra parte do mundo diferente de onde se localizam os agentes iniciais da operação. A liquidação física da operação (obviamente se o objeto comercializado não puder trafegar pela rede), pode ser comandada para especialistas em entregas, também sem restrição física de localização.

2.4 Preocupações com a segurança associadas à atuação na Internet

Em contraposição ao fato de representar uma opção altamente interessante para realização de comércio, a presença na Internet representa também área de grande risco potencial.

A título de curiosidade, Tanenbaum (1992) cita "o verme da Internet", que naquela época era "a maior violação de segurança de todos os tempos". Esta falha foi criada em 2 de novembro de 1988 por Robert Tappan Morris, um estudante de graduação de Cornell. Ele descobriu que era possível obter acesso aos servidores Unix de toda rede Internet. Este acesso era obtido através dois programas: um que processava no servidor sob ataque "(99 linhas em linguagem de programação C)" e o outro, chamado por este primeiro, "infectava" a máquina atacada, para tentar quebrar as senhas de acesso de seus usuários.

Morris acabou sendo preso, mas os custos decorrentes de sua "brincadeira" foram significativos (Tanenbaum cita que provavelmente excederam 150.000 dólares, em uma época que a Internet estava praticamente restrita aos meios militares e acadêmicos).

Na literatura pesquisada foram identificadas diversas preocupações que afligem as organizações ao praticar comércio eletrônico através da Internet. Estes riscos, bem como as soluções sugeridas para reduzi-los, de forma geral, repetem-se entre os vários autores. Nos próximos parágrafos são destacadas, de maneira sucinta, algumas destas abordagens. No capítulo 3 as técnicas citadas para incrementar a segurança estão descritas com maior nível de detalhes.

Applegate, McFarlan e McKenney (1995) apontam 6 tipos de problemas que trazem preocupações associadas ao comércio eletrônico através da Internet. Um resumo

das preocupações trazidas por estes problemas, e das soluções que propõem, é apresentado no Quadro 2.1.

Quadro 2.1 - Preocupações associadas ao comércio eletrônico

Problema	Preocupação do negócio	Solução
Autorização	• O usuário tem permissão para acessar um computador específico ou informação?	Nome de usuários e senhas ou outro mecanismo de controle de acesso
Autenticação	• O usuário é realmente quem se diz ser?	Hardware ou software especiais para gerar números aleatórios para identificar o usuário
Integridade	• remetente da mensagem realmente a enviou? • O destinatário pode estar certo que a mensagem não foi trocada?	Assinatura digital
Privacidade	• A minha conversação (ou transação comercial) é privativa? • Existe alguém espionando?	Criptografia - processo de embaralhamento das mensagens usando chaves públicas e privadas
Fraude/Roubo	• Alguém está me roubando?	Log, auditorias, procedimentos e política de administração de sistemas
Sabotagem	• Alguém pode entrar em meu sistema e destruir ou alterar informações	Firewalls – barreiras eletrônicas criadas com hardware dedicados e sistemas de software que monitoram o tráfego da rede e validam o fluxo de informação entre redes internas e externas Firebreaks – barreiras físicas através das quais não existe conexão eletrônica entre o servidor Internet e os sistemas de informações internos da empresa.

Fonte: Applegate et al (1995)

Santos (1997) comenta que existem várias formas de pessoas não autorizadas, através da Internet, terem acesso à rede interna e aos sistemas de uma organização. Uma vez obtido este acesso, o intruso pode destruir, alterar ou roubar informações, trazendo prejuízos à organização. Para evitar esta invasão, ou diminuir seus danos, descreve diversos tipos de proteção. Além da criptografia e do firewall, já citados por Applegate et al (1995), deve-se destacar:

- **Política de segurança**

  Como não é viável garantir-se proteção absoluta, uma organização, ao invés de procurar total segurança, deve avaliar o valor da informação que tenta proteger. Conhecido este montante, deve compará-lo com a probabilidade de ocorrer uma violação de segurança e o custo de implementar medidas de proteção.

  A primeira ação neste sentido envolve o desenvolvimento (ou revisão) da política de segurança da instalação, na qual a conexão com a Internet seja abordada. Nesta política deve estar definido detalhadamente o acesso que os funcionários deverão ter a cada tipo de serviço. Através da política de segurança os funcionários devem ser alertados sobre suas responsabilidades na proteção de senhas e sobre ações que devem ser tomadas caso uma violação de segurança seja detectada.

  Uma vez implantada a política de segurança, a companhia deve iniciar a avaliação do uso de firewalls, criptografia e autenticação.

- **Autenticação**

  O termo "autenticação" descreve vários métodos que identifiquem um usuário. Senhas ("passwords") são o método mais comum de autenticação utilizado. Outro método de reconhecimento compreende o uso de dispositivos físicos de identificação, como cartões inteligentes, por exemplo.

Zboray (1998), por sua vez, aponta que os preocupações de segurança na Internet podem ser agrupados nos seguintes tópicos:

- **Autenticação e autorização**

  Para efetivar uma autenticação o usuário deve estar identificado de maneira confiável. Associada à necessidade de autenticação, existe a necessidade de controle do acesso dos usuários exclusivamente às informações a eles autorizadas.

- **Privacidade e integridade das sessões através da Internet**

  Um processo eficiente de autenticação não é suficiente para garantir proteção para transações mais sensíveis. Mesmo depois de legitimar um usuário, os dados sensíveis são passíveis de serem visualizados por público não autorizado, pois trafegam através de uma rede pública, que utiliza IP (Internet Protocol). Para se defender contra ataques neste ambiente, as comunicações devem estar protegidas por criptografia, com chaves suficientemente seguras.

- **Proteção no Servidor**

  Mesmo sendo dotada de criptografia, as informações podem ser corrompidas se os servidores de comunicações não forem seguros. Bons sistemas administrativos são importantes mas não suficientes para proteger o servidor da rede, por isto, ele deve ser configurado apenas com as ferramentas necessárias para que cumpra seu papel. Demais informações e aplicativos devem ser removidos para se evitar que possam vir a se tornar um caminho para quebra na segurança.

- **Protegendo a Intranet**

  O servidor Web precisa ganhar acesso aos dados internos dentro de uma rede confiável. Para obter este acesso, um caminho deve estar especificado no firewall. Tipicamente estes caminhos podem ser porta de entrada para um ataque. Os firewalls podem limitar a abrangência destes ataques restringindo as permissões de comunicação somente entre endereços previamente definidos.

Albertin (1999) divide as preocupações de segurança no comércio eletrônico em dois tipos:

- **Segurança em cliente-servidor**

  Consiste na verificação, através de vários métodos de autorização, se existe certeza que apenas usuários autorizados e programas válidos têm acesso às informações e somente aos recursos a eles compatíveis; exemplos de técnicas para garantir esta segurança são senhas, cartões criptografados e firewalls.

- **Segurança de dados e transmissão**

  Visa privacidade e confidencialidade das mensagens em trânsito e autenticação dos usuários remotos; busca, através de técnicas como criptografia, evitar que a mensagem seja visualizada por pessoas não autorizadas e que uma das partes assuma identidade falsa.

Mehta (2000) comenta que apesar das pessoas virem se sentindo mais confortáveis em acessar a Internet, questões envolvendo privacidade e segurança ainda estão presentes e são um grande inibidor a uma aceitação maior da rede. Estas questões envolvem:

- **Privacidade e confidencialidade**

  Os dados que trafegam através da Internet passam por diversos pontos, de onde são redirecionados, até chegar ao seu destino final. O protocolo que suporta a comunicação através da rede (IP - Internet Protocol) é essencialmente inseguro, tornando-a vulnerável à leitura por outras pessoas que não as destinatárias destes dados (assim com a mensagem de um cartão postal despachado pelo correio). Embora inseguro, o uso de tal protocolo é necessário para acomodar a comunicação entre plataformas de computação heterogêneas.

  O uso de protocolos seguros é um caminho para melhorar a proteção das informações em trânsito porque permite que as comunicações entre o servidor e o cliente sejam criptografadas.

- **Roubo e Fraude**

  Os riscos associados a roubos ou fraudes são maiores nas transações baseadas na Internet que nas transações tradicionais em decorrência da ampliação da base de acesso. Para ilustrar esta vulnerabilidade, ele cita uma pesquisa efetuada pelo FBI em conjunto com o Computer Security Institute (CSI) entre as 500 maiores empresas em faturamento (*"Fortune's 500"*) na qual identificou-se que 42% das empresas pesquisadas haviam sofrido acesso não autorizado a

seus sistemas de informação e 32% indicaram perdas ao redor de US$ 100 milhões decorrentes de falhas na segurança. Embora não necessariamente tais falhas fossem na Internet, sua presença torna o problema mais crítico, porque o roubo eletrônico pode ser feito a partir de qualquer lugar do mundo.

- **Violações na integridade dos dados**

  A perda de integridade pode ser acidental ou intencional. Entretanto, como normalmente não existe intervenção humana para avaliar se um movimento vindo através da rede é razoável ou não, o resultado de um erro de comunicação pode ser muito grande.

- **Indisponibilidade do serviço**

  A recusa de acesso (ou "denial of service") é um ataque que torna o acesso a um "site" indisponível, inviabilizando temporariamente sua operação e causando prejuízo em decorrência desta inoperância. Infelizmente, além de ser difícil a prevenção contra estes ataques, as instruções para realizá-los estão organizadas e disponíveis na rede.

- **Repúdio**

  A negativa de uma das partes do processo comercial em assumir ações pelas quais foi efetivamente responsável é uma grande ameaça, principalmente no meio comercial. Como na rede os parceiros comerciais podem não se conhecer por contato comercial anterior ou mesmo por referências, pode ser difícil confirmar-se efetivamente uma transação. Em função disso, são fundamentais controles, como certificados digitais que garantam a validade e autenticidade de uma identificação, para assegurar integridade e não repúdio das operações.

- **Vulnerabilidades na estação-cliente e no servidor Web**

  O principal risco às estações-cliente conectadas à Internet é o recebimento de códigos executáveis que se instalam nestas estações quando se efetua acesso a um site. Tais códigos (por exemplo "*Java applets*", "*ActiveX*", "*JavaScript,* e "*VBScript*") existem para tornar a navegação no servidor Web mais eficientes. Entretanto, por erro ou por má intenção, podem danificar ou buscar informações sigilosas existentes nos arquivos da estação-cliente (freqüentemente à revelia do proprietário desta estação).

  No caso do servidor Web, a preocupação que inicialmente se destaca é a confidencialidade das informações nele armazenadas já que, se não estiverem adequadamente protegidas, podem ser vistas, manipuladas, ou destruídas. Visando evitar esta abertura, é fundamental que dados sensíveis não estejam neste ambiente. Outro destaque importante é que a maioria das fraquezas no servidor decorrem de sua configuração. Usualmente a característica padrão ("default") quando da instalação de um sistema (tanto um firewall quanto um sistema operacional) privilegia a operacionalidade. Isto faz com que vários serviços de rede ou protocolos estejam inicialmente disponíveis de maneira automática. O risco associado a esta opção de instalação é que quanto mais serviços disponíveis, mais caminhos um intruso terá para penetrar em uma rede privada.

- **Vulnerabilidades no correio eletrônico**

  O correio eletrônico também é uma ferramenta utilizada na prática do comércio através da Internet e, como tal, também é um foco de preocupações do ponto de vista da segurança. Esta ameaça pode decorrer tanto de uma sobrecarga de mensagens inúteis ("spamm") que levem à indisponibilização do serviço, quanto a contaminação por vírus.

  Para atenuar este risco são necessários controles como políticas e procedimentos padrões e formalizados (provenientes da alta administração dando respaldo às regras de segurança), empregados competentes e satisfeitos e acompanhamento contínuo da conformidade a estes padrões.

  Mehta comenta que a segurança no correio eletrônico normalmente é baseada em dois pilares: o técnico e o não-técnico. Os controles técnicos incluem:

  - uso de programas anti-vírus nas estações e no servidor
  - atualização regular dos programas anti-vírus
  - quando possível, o firewall deve estar configurado para verificação automática se as mensagens eletrônicas recebidas não contêm vírus
  - uso de mecanismos de criptografia para garantir a confidencialidade

  Os aspectos não-técnicos exercem papel fundamental para evitar as vulnerabilidades neste meio. Entre estes aspectos destacam-se as políticas e procedimentos formais de correio eletrônico, que devem prever:

  - entendimento que os sistemas de correio eletrônico da empresa serão utilizados somente com assuntos da empresa; mensagens inúteis recebidas podem resultar em risco adicional além de implicarem em perda de produtividade e gasto desnecessário de espaço
  - não abertura de mensagens recebidas de fontes desconhecidas (especialmente aquelas com arquivos anexados)
  - pesquisar se arquivos anexados não têm vírus (caso o processo não seja automático)
  - procedimentos de notificação quando vírus forem descobertos
  - procedimentos para tratamento e recuperação em caso de incidentes

  Os procedimentos detalhados acima enfocam os aspectos de segurança. Uma política de segurança para correio eletrônico eficaz deve também cobrir aspectos como produtividade, eficiência e questões legais. Por exemplo, retenção e monitoração dos conteúdos das mensagens e evitar-se o uso do sistema de correio eletrônico como sistema de arquivamento.

2.5 Síntese dos aspectos externos e organizacionais associados à segurança para a prática do comércio eletrônico através da Internet

Com base na literatura pesquisada pode-se deduzir que existem alguns aspectos do ambiente externo e do organizacional que são relevantes quando se considera a segurança na prática do comércio eletrônico através da Internet. Estes aspectos

estão resumidos a seguir e, no capítulo 3, discute-se técnicas que podem proporcionar a segurança que se procura:

- **Política de segurança**

  O comprometimento da alta administração na definição da política de segurança de informações válida para toda a organização é de importância fundamental porque, a partir desta estrutura básica, é que os tratamentos associados à segurança das informações poderão ser definidos.

  A política de segurança deve contemplar, no mínimo, os seguintes aspectos:

  - Critérios para classificação das informações, isto é, parâmetros para que se possa identificar os diferentes graus de importância que cada informação tem para a organização. O conhecimento do valor de cada informação é fundamental para se avaliar de maneira objetiva a adequação ou não do nível de controles necessários para protegê-la. Conhecido este valor, diminui-se o risco de se desenvolver mecanismos excessivamente onerosos para proteger informações que não sejam de grande relevância para a organização
  - Proprietários das informações, ou seja, quem são os responsáveis por julgar a relevância de cada tipo de informação e disciplinar o acesso a ela. Esta definição contempla também regras para acesso à rede, utilização de correio eletrônico, etc.
  - Alerta a todos usuários da importância dos riscos associados à atuação na rede. Isto significa que a política deve ser divulgada a todos usuários para gerar neles uma consciência de segurança de informações
  - Regras claras para atuação em caso de se detectar possíveis violações, visando abreviar o tempo para sua resolução e diminuir as perdas dela decorrentes

- **Acesso ao ambiente interno**

  Ao se colocar na rede os participantes do processo comercial (independente de serem fornecedores ou consumidores) podem tornar seu ambiente interno de tratamento de informações mais vulnerável a acessos não autorizados. Visando diminuir estes riscos é necessário que se implante mecanismos de proteção compatíveis ao grau de relevância das informações que se quer proteger.

- **Acesso indevido às informações que transitam na rede**

  As informações ao transitarem na rede podem ser interceptadas e utilizadas de maneira indevida. Para protegê-las neste ambiente existem diferentes tipos de criptografia.

- **Não reconhecimento dos parceiros**

  Como o contato entre as partes passou a ser feito através da rede, existe o risco de falsa autenticação das partes envolvidas e de repúdio indevido. Para se resguardar contra esta ocorrência existem ferramentas como assinaturas e certificações digitais. A escolha do mecanismo de proteção também deve ser compatível à sensibilidade do bem protegido.

CAPÍTULO 3

AMBIENTE TECNOLÓGICO

Como o ambiente Internet não foi inicialmente projetado para privilegiar a segurança, é necessário que se utilize diversas técnicas para obtenção desta garantia. Neste capítulo são apresentados alguns exemplos destas ferramentas. O objetivo desta apresentação não é citar exaustivamente todos mecanismos e estratégias existentes, mas fornecer uma visão destes produtos e o que se procura com sua utilização. Deve-se destacar também que a ordem com que as ferramentas são apresentadas foi estabelecida arbitrariamente, procurando deixar mais próximas as técnicas com finalidades complementares ou semelhantes.

3.1 Criptografia

Esta ferramenta é fundamental e sobre ela se apoia a maioria das outras técnicas que procuram garantir integridade e confidencialidade das informações. É uma técnica milenar utilizada para evitar que mensagens sejam visualizadas por agentes não autorizados. Generais gregos e romanos já a utilizavam antes da era cristã para se comunicar com seus comandados no campo de batalha.

Lynch e Lundquist (1996) sustentam que qualquer sistema de criptografia realmente seguro deve atender simultaneamente os seguintes princípios:

- **identificação**

  Processo de verificar se o remetente de uma mensagem realmente é quem diz ser
- **autenticação**

  Processo de verificar o verdadeiro remetente de um texto criptografado, além de comprovar que o texto não foi alterado
- **verificação**

  Capacidade de identificar e autenticar com segurança uma comunicação específica
- **impedimento de rejeição**

  É o mecanismo para evitar que qualquer pessoa negue autoria de uma ação sobre a qual seja de fato responsável
- **privacidade**

  A capacidade do sistema de ocultar efetivamente as comunicações dos olhares curiosos

Garfinkel e Spafford (1997) consideram que a força do processo criptográfico depende dos seguintes fatores:

- a confidencialidade da chave
- a dificuldade de adivinhar a chave ao tentar todas possíveis combinações (através de tentativa exaustiva)
- a dificuldade de deduzir o algoritmo de criptografia sem conhecer a chave (quebra do algoritmo)
- a existência (ou ausência) de "porta dos fundos", isto é, caminhos alternativos que permitem que um arquivo codificado seja decifrado sem conhecimento da chave
- a capacidade de decodificar uma mensagem quando se conhece o caminho que a decifra
- as características do texto original e conhecimento destas por quem esteja tentando decifrar (por exemplo, o sistema criptográfico pode ser vulnerável se todas mensagens codificadas comecem ou terminem de maneira uniforme; este método foi usado pelos aliados durante a II Guerra Mundial para decifrar o código usado pela Alemanha)

Existem duas técnicas básicas para efetuar a criptografia:

- **Substituição**

  Consiste na troca de cada caracter da mensagem que se quer codificar por outro, seguindo algum princípio lógico; por exemplo, no código de Cesar, a letra *d* substituí a letra *a*, *e* substituí *b*, e assim por diante

- **Transposição**

  Envolve embaralhamento dos caracteres da mensagem; para facilitar o raciocínio, pode-se imaginar uma mensagem e colocá-la em uma tabela linha a linha e transmitindo-a coluna a coluna; uma dupla transposição compreende um novo embaralhamento do resultado obtido no passo anterior

No início do Século XX foram desenvolvidos na Europa e Estados Unidos dispositivos eletrônicos com o propósito de codificar mensagens enviadas por rádio e telefone. Estes sistemas, por dificuldade no armazenamento de uma mensagem completa usando técnica de transposição, normalmente baseavam-se em substituição. Na atualidade, com o uso da computação, é possível usar combinação das duas técnicas, assim como de outras funções matemáticas.

Garfinkel e Spafford (1997) descrevem os seguintes tipos de algoritmos de criptografia:

- **algoritmos de chave simétrica**

  A mesma chave é usada para codificar e para decodificar a mensagem

- **algoritmos de chave pública**

  Com estes algoritmos uma chave é usada para codificar a mensagem e outra para decodificá-la; a chave de codificação é chamada chave pública, porque pode ser disponibilizada sem o compromisso de manter-se sua

confidencialidade. A chave de decodificação é a chave privada ou secreta. Este sistema também é chamado de algoritmo de chave assimétricas

- **sistemas híbridos**

  Utilizam, de maneira combinada algoritmos de chave simétrica e de chave pública

- **funções de resumo de mensagens**

  Uma função que gera um único conjunto de bits para uma dada entrada

Os algoritmos de chave simétrica são valorizados nos modernos sistemas de criptografia por serem de mais fácil implementação e, geralmente, processados mais rapidamente. O ponto negativo deste algoritmo é que, antes de ser utilizado com segurança, necessita que as partes envolvidas troquem entre si a chave de criptografia.

No caso das chaves públicas, esta dificuldade da troca prévia deixa de existir, conforme pode ser observado no exemplo a seguir:

- uma entidade, seja esta uma pessoa jurídica ou física (que pode ser chamada de Empresa A, para facilitar o entendimento), cria uma chave pública, podendo, por exemplo, deixar esta chave disponível em seu *site* na Internet
- outra entidade, digamos Cliente C, que deseja se comunicar com a Empresa A, usando esta chave pública, envia uma mensagem
- apenas a Empresa A pode decodificar a mensagem recebida do Cliente C, porque apenas ela tem a chave secreta que permite esta operação

A grande restrição da chave pública é que seu processamento é muito lento (entre 10 e 100 vezes mais lento que processamento usando chave simétrica). Uma alternativa para contornar tal limitação é a utilização de ***chaves híbridas***: para estabelecer a chave comum, se utiliza o algoritmo de chave pública e, a partir daí, passa-se a utilizar o algoritmo de chave simétrica.

A função resumo transforma as informações contidas em arquivo em um número único com tamanho variado (normalmente entre 128 e 256 bits). Deve combinar as seguintes propriedades matemáticas:

- cada bit da função resumo é influenciada por cada bit da entrada
- se qualquer bit da entrada é trocado, cada bit da saída tem 50% de chance de ser trocado
- dado um arquivo de entrada e sua função resumo correspondente, não deve existir outra entrada que gere a mesma função resumo

Uma característica de fundamental importância no algoritmo de criptografia é o tamanho da chave utilizada. Para facilitar a visualização, pode-se ilustrar indicando que uma chave de 40 bits permite 2^{40} combinações possíveis, ou, aproximadamente, $1 * 10^{11}$ (cerca de 1 trilhão de chaves), enquanto que uma de 128 bits proporciona 2^{128} combinações (cerca de $3,4 * 10^{38}$).

No Apêndice I são destacados alguns exemplos citados por Garfinkel e Spafford (1997) de algoritmos de criptografia, com as características técnicas de cada um.

3.1.1 Criptografia e Segurança na Web

Com base no exposto na seção 3.1, pode-se afirmar que a criptografia desempenha as seguintes funções de fundamental importância nas operações através da Internet:

- **Confidencialidade**

  A criptografia é usada para embaralhar informações visando protegê-la contra olhares indiscretos quando enviadas através da rede ou quando armazenadas nos arquivos internos da organização

- **Autenticação e não repúdio**

  Assinaturas digitais são usadas para identificar o autor da mensagem; podem ser usadas em conjunto com passwords ou como alternativa a este controle. Os protocolos ("recibos") criptográficos criados não permitem que alguém alegue não ser responsável por uma ação que na verdade executou

- **Integridade**

  Para assegurar que a mensagem não foi modificada quando em trânsito; esta função normalmente é desempenhada pela função de resumo de mensagens

Garfinkel e Spafford (1997) dividem os sistemas que trabalham com criptografia em duas categorias. No primeiro grupo estão programas e protocolos usados exclusivamente para criptografia, isto é, para codificar e decodificar textos. Tais textos codificados podem tanto ser enviados através da rede quanto arquivados. Como exemplo de produtos com este propósito destacam o PGP (Pretty Good Privacy) e o S/MIME (Multipurpose Internet Mail Extensions). Na segunda categoria dos sistemas de criptografia estão os protocolos de rede, que fornecem confidencialidade, autenticação, integridade e não-repúdio no ambiente de rede. Para exercerem este papel tais sistemas exigem conversação em tempo-real entre o cliente o servidor para funcionarem adequadamente. Como exemplo destes sistemas destacam-se os seguintes:

- SSL (Secure Socket Layer)
- PCT (Private Communicatios Technology)
- S-HTTP (Secure HyperText Transfer Protocol)
- SET (Secure Electronic Transaction) e Cybercash
- DNSSEC (Domain Name System Security)
- IPsec e IPv6
- Kerberos
- SSH (Secure Shell)

Uma descrição sucinta dos sistemas de criptografia apontados por Garfinkel e Spafford é apresentada no Apêndice 2. Os programas citados eram os utilizados em 1997, quando o livro foi escrito. Nos dias atuais já sofreram atualizações (por exemplo, o SET, que naquela época ainda estava sendo desenvolvido, já vem sendo utilizado em sua plenitude atualmente). Entretanto, são úteis para ilustrar as diferentes categorias dos produtos voltados para criptografia. No Quadro 3.1 é apresentado um resumo dos diferentes sistemas citados por Garfinkel e Spafford com a finalidade de cada um.

Os sistemas SSL e SET, por serem os mais citados na bibliografia tratando segurança para a prática de comércio através da Internet estão descritos com maior nível de detalhes nas seções 3.1.2 e 3.1.3.

Quadro 3.1 - Exemplo de sistemas de criptografia

Sistema	O que é?	Algoritmo que usa	Proporciona
PGP	Programa aplicativo para codificação de correio eletrônico	IDEA, RSA, MD5	Confidencialidade, autenticação, integridade e não-repúdio
S/MIME	Codificação de correio eletrônico	Especificado pelo usuário	Confidencialidade, autenticação, integridade e não-repúdio
SSL	Protocolo para criptografia de transmissões TCP/IP	RSA, RCZ, RC4, MD5 e outros	Confidencialidade, autenticação, integridade e não-repúdio
PCT	Protocolo para criptografia de transmissões TCP/IP	RSA, RCZ, RC4, MD5 e outros	Confidencialidade, autenticação, integridade e não-repúdio
S-HTTP	Protocolo para codificar solicitações e respostas HTTP	RSA, DES e outros	Confidencialidade, autenticação, integridade e não repúdio (entretanto é obsoleto, segundo os autores)
SET e Cybercash	Protocolo para envio de instruções de pagamento seguras através da Internet	RSA, MD5, RC2	Confidencialidade do número do cartão de crédito, integridade da mensagem, autenticidade do comprador e vendedor e não-repúdio da transação
DNSSEC	Sistema de segurança do nome do domínio	RSA, MD5	Autenticação e integridade
IPsec e Ipv6	Protocolo de baixo nível para codificar pacotes IP	Diffie-Hellman e outros	Confidencialidade (opcional), autenticação e integridade
Kerberos	Serviço de Segurança de rede para proteger aplicativos de maior nível	DES	Confidencialidade e autenticação
SSH	Codificar terminais remotos	RSA, Diffie-Helman, DES, Triple-DES, Blowfish e outros	Confidencialidade, autenticação

Fonte: GARFINKEL, Simson e SPAFFORD, Gene (1997)

Mehta (2000) destaca que existem protocolos genéricos, para incrementar a segurança das comunicações através da Internet, e protocolos específicos para tratar transações financeiras. Dentre os protocolos genéricos, destaca o SSL e o S-HTTP. Para tratar transações financeiras cita, além do *SET (Secure Electronic Transaction)* e do *CyberCash,* já comentados por Garfinkel e Spafford, outro protocolo chamado *First Virtual,* mas não fornece maiores detalhes sobre este protocolo. Mehta, baseando-se em Ghosh (1998), também fornece uma visão dos papeis desempenhados pelos protocolos de comunicação e de segurança para garantir a integridade de dados financeiros em trânsito através da rede. Esta visão, formada por camadas, é apresentada na Figura 3.1.

Figura 3.1 - Camadas da estrutura de comunicação financeira através da rede

<table>
<tr><td colspan="4">Protocolos de Pagamento (SET, Cybercash)</td></tr>
<tr><td>S-HTTP</td><td>HTTP</td><td>S/MIME</td><td>Telnet, Correio, DNS, NNTP, etc.</td></tr>
<tr><td colspan="4">Secure Socket Layer (SSL), para fornecer segurança na conexão</td></tr>
<tr><td colspan="4">Transport Control Protocol (TCP), para permitir entrega confiável das mensagens</td></tr>
<tr><td colspan="4">Internet Protocol (IP), para encaminhamento das mensagens ("routing")</td></tr>
<tr><td colspan="4">Camada de conexão aos dados</td></tr>
</table>

Fonte: MEHTA (2000), citando GHOSH, Anup. E-Commerce Security - Weak Links, Best Defenses, United States (1998)

3.1.2 - SSL

Garfinkel e Spafford (1997) descrevem o Secure Socket Layer como sendo um protocolo criptográfico para proteger comunicações bidirecionais. Os sites que utilizam SSL para propiciar conexões seguras são normalmente identificadas por um prefixo (por exemplo, ***https***, para conexões HTTP) e por um símbolo específico (por exemplo, um cadeado se o browser utilizado for o Internet Explorer, da Microsoft, ou uma chave, se o browser for o Netscape Navigator).

O SSL é uma camada existente entre o protocolo TCP/IP puro e a camada da aplicação. Enquanto uma mensagem normal utilizando TCP/IP envia somente uma seqüência de bits entre dois computadores (ou dois processadores no mesmo computador), o SSL possui três camadas: uma de mensagem (com dados do usuário, dados do protocolo de criptografia, mensagens de identificação e mensagens de erro), outra de dados (em blocos de até 16.823 bytes) e outra de transporte dos dados (usualmente TCP/IP).

Com o uso deste produto é possível obter-se:

- autenticação e não-repúdio do servidor e do cliente, usando assinaturas digitais
- confidencialidade dos dados, através do uso da criptografia

- integridade de dados, através do uso de código de autenticação de mensagens

O protocolo de criptografia somente funciona quando os parceiros que estão comunicando utilizam o mesmo padrão. Quando um programa usando SSL inicia contato com outro, automaticamente os dois se analisam para determinar qual o protocolo mais forte que ambos têm em comum. Após estabelecido este acordo inicial, a comunicação continua naquele protocolo.

Como características importantes do SSL pode-se destacar as seguintes:

- **separação de papéis**

  São utilizados algoritmos distintos para criptografia, autenticação e integridade de dados; esta propriedade lhe permite ser útil mesmo quando uma de suas funcionalidades não é usada integralmente, como quando a integridade e a autenticação são requeridas, mas a criptografia não puder ser usada (por restrições legais, por exemplo)

- **eficiência**

  A codificação e decodificação consomem tempo; para a comunicação ser mais eficiente, aplicativos SSL armazenam uma "chave mestra", que é preservada durante a conexão, o que permite que a comunicação flua de maneira segura sem necessidade de novos tratamentos

- **autenticação baseada em certificação**

  O SSL fornece autenticação tanto a clientes quanto a servidores através do uso de certificados digitais e assinaturas digitais

O SSL usa chave secreta de 128 bits, mas sua exportação, ainda de acordo com Garfinkel e Spafford (1997), somente pode ser feita com 40 bits e até 512 bits de chave pública. O próprio browser apresenta a segurança do protocolo utilizado: se o desenho da chave (usada no Netscape) tiver dois segredos, a chave usada é de 128 bits; se tiver apenas um segredo, é de apenas 40 bits e se estiver quebrada não existe criptografia. Caso o browser seja o Explorer, se existir um pequeno cadeado na barra inferior da tela, a comunicação está protegida e, se tal cadeado não existir, não existe criptografia. Ao "clicar-se" sobre o desenho do cadeado é possível obter detalhes da proteção fornecida.

3.1.3 SET

De acordo com informações obtidas no site da Visa (www.visa.com), o projeto para desenvolvimento do sistema de criptografia Secure Electronic Transaction foi divulgado em 1 de fevereiro de 1996 com o objetivo de conferir autenticidade das partes envolvidas em pagamentos de compras efetuadas em qualquer tipo de rede on-line, inclusive a Internet, utilizando-se de cartão. As empresas inicialmente envolvidas neste projeto eram a Visa e a Mastercard, com o apoio de outras empresas líderes de tecnologia, como Microsoft, IBM, Netscape, SAIC, GTE, RSA e Terisa Systems. O padrão foi usado em testes pilotos em 1997 e passou a ser

utilizado em 1998. As informações são criptografadas com chaves públicas e privadas, usando algorítimo RSA de 1024 bits.

O objetivo do SET é garantir que cada parte envolvida no processo comercial tenha acesso exclusivamente às informações que necessita para realizar o papel que lhe cabe na operação (por exemplo, o vendedor não precisa conhecer o número do cartão de crédito do cliente que compra seus produtos mas apenas ter certeza que receberá o valor correspondente à venda). O requisito para implementar o padrão é que todas partes envolvidas na transação eletrônica sejam autenticadas por uma entidade certificadora, que fornecerá um certificado digital para cada uma delas.

Fajardo (1998) assim descreve as partes envolvidas no SET:

- **entidade certificadora**

  Emite autenticação digital a bancos, administradoras e portadores de cartão de crédito (ou de débito) e a lojas virtuais; funciona como um cartório do mundo real, responsabilizando-se pela identificação e validação das partes envolvidas em uma transação eletrônica; esta entidade, após confirmar autenticidade das informações emite um documento digital (o "certificado")

- **carteira eletrônica**

  É onde o usuário guarda o seu "dinheiro digital", isto é, os meios com que pagará as operações que realizar; esta "carteira" contém os dados do cartão de débito e/ou de crédito do comprador e seus certificados digitais; ao realizar uma operação, esta "carteira" é acionada e o cliente seleciona o meio com que deseja liquidar a operação

- **servidor de comércio**

  Centraliza e divulga os catálogos eletrônicos das lojas virtuais, executando a interação entre a "carteira eletrônica" (descrita acima) e o "gateway de pagamentos" (descrito a seguir); cada loja virtual tem seu certificado digital que a garante perante o comprador; o servidor de comércio evita que a loja tenha acesso às informações dos meios de pagamento do comprador e que a instituição financeira identifique quais bens ou serviços o comprador adquiriu

- **gateway de pagamentos**

  Recebe mensagens dos servidores de comércio e as envia à instituição financeira responsável pela liquidação da operação

- **instituição financeira**

  Processa a operação, pagando a loja virtual e cobrando do cliente

- **cliente**

  Para efeitos desta descrição, é a entidade que realiza compras na rede; tem os dados dos meios de pagamentos que utilizará (cartão de débito ou de crédito, por exemplo), em uma carteira digital, que é usada sempre que fizer uma compra dentro do padrão SET

- **loja virtual**

  Para efeitos desta descrição, é a entidade que realiza vendas de bens e serviços através da rede usando o padrão SET

O processo comercial efetuado utilizando o padrão SET é o seguinte:

a) o cliente (possuidor da carteira eletrônica) acessa um servidor de comércio (loja eletrônica ou shopping virtual) através do browser, seleciona os produtos ou serviços que deseja e define como os pagará; o pedido de compra e a indicação do método de pagamento escolhido são enviados para o servidor de comércio

b) o servidor de comércio repassa para o "gateway de pagamentos" as informações relativas à carteira eletrônica, solicitando autorização para dar encaminhamento ao processo

c) o gateway de pagamentos encaminha os dados da carteira eletrônica para a instituição financeira informada pelo cliente (um banco, se for cartão de débito, ou uma administradora de cartão de crédito, caso este seja o meio de pagamento utilizado), para confirmar que o cliente possui crédito para efetuar a compra

d) após receber confirmação da instituição financeira, o gateway de pagamentos confirma a operação para o servidor de comércio

e) o servidor de comércio confirma a compra para o cliente, fornecendo as informações sobre prazo de entrega e número do pedido

3.2 Certificados Digitais

O objetivo dos certificados digitais é assegurar aos participantes da transação comercial que eles podem ter confiança mútua entre si. São usados para aprovar um documento eletrônico de forma que possa mais tarde ser validada sua autenticidade e fornece ajuda para evitar o repúdio indevido.

Mehta (2000) comenta que antes de entender o certificado digital é fundamental que se conheça a assinatura digital: um conjunto de dados (sumário de mensagem criptografado que é criado a partir da mensagem original) o qual é enviado juntamente com a mensagem codificada para identificar o gerador da mensagem e para verificar se ela não foi alterada desde que foi enviada. A assinatura digital ultrapassa outras técnicas como mecanismos de verificar a integridade da mensagem, porque garante também que não haja seu repúdio.

Os certificados digitais são um conjunto de informações ao qual uma assinatura digital é anexada por uma CA (*"Certificate Authority"*), instituição alheia ao processo, que desfrute da confiança da comunidade de usuários de certificados. Normalmente o certificado digital contém o nome de proprietário, o nome da CA que está garantindo a autenticidade, um número de série, o período de validade do certificado e a chave digital. Tanto o nome do proprietário quanto o número de série devem ser únicos.

As CAs prestam um serviço de garantia independente de autenticação da identidade de uma pessoa ou de um site da rede. Para capacitar-se a obter este serviço, as empresas precisam registrar-se nesta entidade certificadora. A CA usará sua chave privada (ou chave simétrica de criptografia) para colocar sua assinatura digital no certificado. Quando alguém utilizar uma sessão SSL o certificado é baixado para o browser do cliente que o decodifica usando a chave pública da CA. Se a informação decodificada coincidir com a existente no browser o site é autêntico.

O certificado funciona como uma "carteira de identidade digital". A assinatura digital é equivalente à "impressão digital" e a CA pode ser comparada a um "cartório digital".

Mehta (2000) lembra que a CA apenas autentica a identificação, mas não garante que o site é confiável no que diz respeito às mercadorias e informações que comercializa.

3.3 PKI

A Public Key Infraestructure é um sistema para verificar a identidade das pessoas que tenham chaves de criptografia e gerenciar de maneira eficaz os certificados digitais. Esta função pode ser executada internamente ou confiada a um terceiro com conhecimento especializado no assunto.

Segundo Mehta (2000), embora várias empresas estejam implementando as PKIs, seu uso está praticamente no início. Além da falta de padrões, a própria infra-estrutura deficiente também afeta as PKI. Nesta deficiência de infra-estrutura estão incluídos, por exemplo, fatores como guarda dos certificados e mecanismos de revogação de chaves, chaves de back up e recuperação e gerenciamento de expiração e renovação de chaves.

3.4 Configuração do servidor Web

Mehta (2000) comenta que um caminho que pode ser utilizado para a entrada não autorizada ao ambiente interno é através dos *"CGI (Common Gateway Interface) scrits"*. Este mecanismo consiste de roteiros que permitem busca de informações e realização de pesquisas on-line em outros ambientes computacionais, fora do servidor Web (por exemplo, nos arquivos internos da organização, onde processam seus aplicativos).

A maioria das fraquezas no servidor decorrem de sua configuração. Usualmente a característica padrão ("default") quando da instalação de um sistema (tanto um firewall quanto um sistema operacional) privilegia a operacionalidade. Isto faz com que vários serviços de rede ou protocolos estejam inicialmente disponíveis de maneira automática. O risco associado a esta opção de instalação é que quanto mais serviços disponíveis, mais caminhos um intruso terá para penetrar em uma rede privada.

As proteções sugeridas por Mehta para permitir maior segurança no servidor Web envolvem:

- remover os roteiros CGI padrão não necessários
- o servidor Web deve utilizar privilégios mínimos para executar os roteiros CGI (por exemplo, em um sistema UNIX, o servidor não deve executar como "root")
- desligar a opção de listagem automática do diretório; se esta estiver disponível, o programa fonte pode ser baixado para se analisar eventuais vulnerabilidades
- Desabilitar aceitação de *"SSI (Server-Side Includes)"*. SSI são códigos inseridos em documentos HTML que, se carregados no servidor, executarão com autoridade de servidor Web
- Restringir os diretórios onde os roteiros CGI podem ser executados a partir do servidor. Se estes forem executados nos diretórios dos usuários, podem ser ameaças à segurança
- Verificar a adequada configuração da distribuição de *"cookies"*[1]. *"Cookies"* transitam entre o servidor Web e a estação-cliente podendo incluir informações de autenticação. Se estiverem mal configurados, um servidor não autorizado pode ser capaz de recuperar aquele "cookie", e tentar ganhar acesso não autorizado ao servidor Web original
- Assegurar-se que todas opções padrão do sistema operacional e do aplicativo específico que podem trazer danos ("deadly defaults") foram tratadas. A identificação destas opções, de acordo com Mehta, pode ser obtida consultando-se os fornecedores destes produtos, ou pesquisando em sites como o do CERT[2] (www.cert.org) e o www.ntsecurity.net, para ambientes Windows NT
- Bloquear serviços de rede não necessários. Por exemplo, em um servidor exclusivo para correio eletrônico, serviços como navegação e transferência de arquivo não são necessários
- Manter o sistema operacional atualizado. As últimas atualizações normalmente corrigem falhas e aberturas descobertas no sistema operacional.

3.5 Firewalls

Firewalls são dispositivos (normalmente um computador processando um sistema especialmente desenvolvido ou um sistema operacional adaptado) que atuam como barreiras entre duas redes: a interna e a externa. Seu papel é confrontar os pacotes de informações que entram e saem da organização contra um conjunto de parâmetros definidos pelo administrador, para permitir (ou negar) o tráfego. Visa evitar intrusos e contaminação por vírus vindos do ambiente externo.

---

[1] "Cookie", de acordo com Garfinkel e Spafford (1997) é um texto (um bloco de caracteres em ASCII) que o servidor Web pode passar através do navegador da rede (browser). O browser armazena o cookie em um arquivo texto chamado cookie.txt, e o envia de volta ao servidor, a cada vez que solicita uma página do servidor.

[2] CERT - Computer Emergency Response Team é um grupo da Carnegie Mellon University que coleta relatórios sobre crimes em computadores, fornece informações aos vendedores e distribuí informações dos vendedores alertando vulnerabilidades de seus sistemas.

Segundo Santos (1997) existem dois tipos de configurações de proteção por firewall. Um atua com filtros ("packet filters") nos quais se estabelece endereços IP (Internet Protocol address) com os quais a organização aceita estabelecer conexão. Esta modalidade de proteção é prática e de baixo custo, já que não é perceptível ao usuário e praticamente não traz degradação na performance da rede. Entretanto, tem baixa confiabilidade pois, usando uma técnica chamada "IP spoofing", o invasor altera seu endereço original para outro que seja aceitável para organização, burlando assim o controle. Outro tipo de proteção por firewall é o chamado "application gateway" (literalmente, aplicativo de passagem ou portão). "Application gateways", são programas escritos para Internet que processam em um servidor com duas conexões de rede, agindo como um servidor para o aplicativo cliente e como um cliente para o servidor de aplicação. Têm maior confiabilidade que os "packet filters" na validação das conexões, mas trazem prejuízos ao desempenho da rede em decorrência do duplo processamento.

Guttman e Bagwill (1997) comentam que os firewalls proporcionam os seguintes tipos de proteção:

- podem bloquear tráfego indesejável
- podem direcionar o fluxo vindo da rede para sistemas internos mais confiáveis
- escondem sistemas vulneráveis que não podem ser vistos a partir da Internet
- podem registrar (manter "log") do tráfego vindo para a rede interna e dela proveniente
- podem ocultar informações como nome de sistemas, topologia da rede, tipos de dispositivos da rede e identificação de usuários internos
- podem fornecer autenticação mais eficiente que as aplicações padrão são capazes de fornecer

Ainda Guttman e Bagwill (1997) comentam que na configuração "application gateways" os firewalls utilizam programas do servidor (chamados "proxies"). Cada programa tem uma finalidade específica, isto é, existe uma proxy para transferência de arquivos ("FTP"), outra para navegação na rede ("HTTP"), etc. São considerados configurações mais seguras de firewall porque podem permitir, por exemplo:

- controles que assegurem que todas as conexões da rede interna para a externa e no sentido contrário somente sejam feitas através do firewall
- usando-se "proxies" para diferentes serviços evita-se acesso direto à rede interna, protegendo-se a organização contra acessos inseguros
- implantação de mecanismos mais eficientes de autenticação

Mehta (2000) comenta que considerações de segurança do firewall incluem:

- evitar a administração remota do firewall, principalmente através da Internet
- questões associadas ao servidor Web (descritas na seção 3.4, como, por exemplo, configurações padrão inseguras), também são válidas para o firewall

- o software do firewall deve ser atualizado regularmente porque assim como nos produtos anti-vírus, sua eficiência é melhorada à medida que novas vulnerabilidades são identificadas e corrigidas
- revisão periódica dos firewalls; para execução desta atividade sugere produtos existentes no mercado como o ISS (Internet Security Scanner - www.iss.net)

Um fato importante a destacar é que a existência de firewalls não garante a integridade das informações na rede interna da organização. Esta limitação ocorre porque, por exemplo, podem haver violações por parte dos próprios usuários internos.

3.6 Síntese dos aspectos técnicos associados à segurança para a prática do comércio eletrônico através da Internet

Resumindo o que foi apresentado neste capítulo vale destacar que embora a Internet seja um processo pouco seguro de realizar operações comerciais, a tecnologia fornece recursos para melhorar esta segurança. Estes recursos envolvem:

- **proteção das informações**

  Os recursos de criptografia fornecem proteção contra visualização e alteração não autorizada das informações em trânsito através da rede ou armazenadas nos arquivos internos da organização.

  Por outro lado, mecanismos como o firewall permitem razoável proteção contra ameaças vindas através da rede ao interior da organização.

- **reconhecimento dos parceiros**

  Também existem recursos, como certificado digital, por exemplo, que permitem à organização assegurar-se que os seus parceiros de negócio através da rede são efetivamente quem dizem ser.

- **preservação de informações restritas**

  Existem recursos, como SET, por exemplo, que viabilizam fornecer a cada parte envolvida no processo comercial, somente as informações necessárias e suficientes para que ela desempenhe seu papel na negociação.

Compete à administração da organização, com base no valor das informações que deseja proteger e no custo do mecanismo de proteção, definir qual estratégia de segurança vai utilizar para praticar comércio eletrônico através da Internet.

Capítulo 4

AMBIENTE DE AUDITORIA

Boynton e Kell (1996) comentam que o termo *auditoria* pode ser usado para descrever uma grande variedade de atividades. Segundo eles, na definição mais abrangente, constante do Relatório do Comitê de Conceitos Básicos de Auditoria da Associação Americana de Contabilidade, auditoria compreende:

> *o processo sistemático de, objetivamente, obter e avaliar evidências enfocando afirmações sobre ações e eventos econômicos para avaliar o grau de correspondência entre estas afirmações e os critérios estabelecidos, para comunicação dos resultados aos usuários interessados*

Nesta definição os seguintes termos merecem destaque:

- **processo sistemático**

  Envolve uma série de passos e procedimentos organizados de maneira lógica e estruturada.

- **obtenção e avaliação objetiva das evidências**

  Significa examinar as bases das afirmações e avaliá-las de maneira justa sem viés ou preconceito.

- **afirmações sobre ações e eventos econômicos**

  São as declarações ou informações fornecidas pelo indivíduo ou entidade correspondentes aos assuntos sujeitos à auditoria. Afirmações incluem informações contidas nas demonstrações financeiras, relatórios de operações internas, ações executadas, etc.

- **grau de correspondência**

  Refere-se à afinidade com que as afirmações podem ser associadas com os critérios estabelecidos.

- **critérios estabelecidos**

  São os padrões contra os quais as afirmações ou representações são julgadas. Podem ser determinados internamente (normas da administração, por exemplo) ou partir de fontes externas (como leis e regulamentos, por exemplo).

  No contexto deste trabalho, pode-se considerar como critérios estabelecidos os padrões de segurança para atuação da organização na Internet.

- **comunicação dos resultados**

  Obtêm-se através de um relatório formal que indique o grau de correspondência entre as afirmações e os critérios definidos. A comunicação de resultados tanto pode fortalecer como enfraquecer a credibilidade das representações feitas por terceiros.

- **usuários interessados**

  São indivíduos que usam (ou confiam) nas constatações dos auditores. Incluem-se alta administração, acionistas, credores, órgãos governamentais e o público em geral.

Ainda Boynton e Kell (1996) definem que existem três tipos de auditoria:

- **auditoria das demonstrações financeiras**

  Envolve a obtenção e avaliação das evidências sobre as demonstrações financeiras de uma entidade, com o propósito de opinar se tais demonstrações foram elaboradas obedecendo um critério estabelecido (normalmente os princípios de contabilidade geralmente aceitos). Este tipo de auditoria é conduzido por auditores externos nomeados pela organização cujas demonstrações financeiras estejam sendo auditadas. O resultado da auditoria nas demonstrações financeiras é destinado a um leque amplo de usuários, como acionistas, credores, órgãos reguladores e o público em geral.

- **auditoria de conformidade (*"compliance"*)**

  A auditoria de *compliance* compreende a obtenção e avaliação de evidências para determinar se certas atividades financeiras ou operacionais de uma entidade estão em conformidade com as condições, regras e regulamentos específicos. O critério estabelecido neste tipo de auditoria pode ser derivado de várias fontes. Como exemplos destas fontes, e de critérios estabelecidos por cada uma, pode-se destacar:

  - a administração, definindo políticas de segurança das informações e de operação de correio eletrônico
  - os credores (ou um tipo especial de credor) definindo que as operações da empresa sigam determinados padrões para que conceda crédito a taxas subsidiadas
  - o governo ou órgãos de tutela (Banco Central, por exemplo), definindo os tipos de operação autorizadas para a organização

  Os relatórios da auditoria de compliance são geralmente direcionados para a autoridade que estabeleceu os critérios e podem incluir um sumário das constatações (*"findings"*) e um parecer que assegure o grau de aderência aos critérios estabelecidos.

- **auditoria operacional**

  Uma auditoria operacional envolve a obtenção e avaliação de evidências sobre a eficiência e a eficácia das atividades operacionais de uma entidade em relação a objetivos específicos. Este tipo de auditoria normalmente é chamado de auditoria de desempenho ou auditoria administrativa.

  Os relatórios destas auditorias geralmente incluem não somente avaliação da eficiência e eficácia das operações, mas também recomendações para tornar tais operações mais eficientes e eficazes.

Os profissionais que executam as atividades associadas à auditoria estão classificados em três grupos:

- **auditores independentes**

  São profissionais que, isoladamente ou como membros de uma empresa de auditoria, prestam serviços de auditoria contábil, de compliance ou operacional a clientes aos quais não estão ligados funcionalmente. A remuneração pela prestação destes serviços é feita através de honorários.

- **auditores internos**

  São funcionários da empresa em que efetuam auditoria. Efetuam uma atividade de avaliação independente, chamada *auditoria interna*, dentro da organização e para ela. O objetivo da auditoria interna é auxiliar a administração da organização no exercício de suas responsabilidades.

  A abrangência da função auditoria interna estende-se a todas as fases das atividades organizacionais. Envolve principalmente auditoria operacional e de compliance, mas pode também auxiliar os auditores independentes na auditoria das demonstrações financeiras.

- **auditores governamentais**

  São funcionários de órgãos municipais, estaduais e federais que executam auditorias de demonstrações financeiras, de compliance e operacionais, prestando contas de seu trabalho aos órgãos que os empregam e ao público.

Como o objetivo deste trabalho é tratar a auditoria de informática no comércio eletrônico através da Internet, o foco principal está sendo dirigido para a auditoria operacional executada tanto por auditores independentes quanto por auditores internos. Este foco, em algumas situações, abre-se um pouco, abordando também a auditoria de compliance, quando, por exemplo, trata da avaliação da existência e cumprimento da política de segurança. Não é objetivo deste trabalho tratar auditoria das demonstrações financeiras e trabalhos efetuados por auditores governamentais mesmo que estas atividades estejam ligadas à realização do comércio eletrônico através da Internet.

4.1 A auditoria e o controle interno

Qualquer atividade humana, para cumprir sua finalidade, necessita ser conduzida dentro de determinados padrões. A importância destes padrões é ampliada quando várias pessoas se unem para conduzir em comum determinado empreendimento, seja ele uma organização comercial, uma associação recreativa, um condomínio, etc. Este conjunto de padrões que rege a vida de uma organização no sentido dela atingir seus objetivos pode ser chamado de controle interno.

A importância do controle interno e sua relevância para o trabalho dos auditores é reconhecida há longo tempo. Ilustrando tal reconhecimento, Boynton e Kell (1996) citam que uma publicação de 1947 do AICPA (American Institute of Certified Public

Accountants) chamada *Internal Control* indicava que os seguintes fatores contribuíam para a expansão do reconhecimento da importância do controle interno:

> ▪*O âmbito e o tamanho das entidades comerciais se tornou tão complexo e comum que a administração tem que confiar em numerosos relatórios e análises para controlar as operações de maneira eficaz*
>
> ▪*A verificação e revisão inerente a um bom sistema de controle interno garante proteção contra fraquezas humanas e reduz a possibilidade que erros ou irregularidades ocorram*
>
> ▪*É impraticável para os auditores auditar a maioria das empresas obedecendo limitações econômicas dos honorários sem confiar no sistema de controle interno do cliente*

A preocupação com controle interno ao longo do tempo ultrapassou as fronteiras de auditoria e contabilidade. Em Outubro de 1987, ainda segundo Boynton e Kell (1996), o relatório final da *National Commission on Fraudulent Financial Reporting (Treadway Commission)*, formada pelo Congresso dos Estados Unidas, incluía o seguinte na página 11:

> ▪*A importância fundamental na prevenção de relatórios financeiros fraudulentos é definida pela alta administração que influencia o ambiente organizacional dentro do qual os relatórios financeiros ocorrem*
>
> ▪*Todas empresas públicas devem manter controles internos que forneçam razoável segurança que relatórios financeiros fraudulentos sejam prevenidos ou detectados*
>
> ▪*As organizações patrocinadoras da Comissão, inclusive o Conselho de Padrões de Auditoria (Auditing Standards Board - ASB), devem cooperar para o desenvolvimento de instruções adicionais de um sistema de controles internos*

Em 1992, seguindo a última recomendação da Treadway Commission, o Comitê de Organizações Patrocinadoras (*COSO - Committee of Sponsoring Organizations*) divulgou um relatório chamado *Internal Control - Integrated Framework*. Este Comitê (COSO) congregava representantes do AICPA, da American Accounting Association, do Institute of Internal Auditors, do Institute of Management Accountants e do Financial Executives Institute. O propósito do trabalho era:

- estabelecer uma definição comum de controle interno atendendo as necessidades de diferentes parceiros, e
- fornecer um padrão contra o qual as empresas e outras entidades poderiam avaliar seu sistema de controle e determinar como incrementá-lo.

O relatório do COSO define controle interno como sendo:

> *O processo, executado pelo conselho de administração da organização, pela gerência e por todos os funcionários, projetado*

para fornecer razoável segurança que os objetivos da organização sejam atingidos, nas seguintes categorias:

- *confiabilidade dos relatórios financeiros*
- *conformidade às leis e regulamentos aplicáveis*
- *eficácia e eficiência das operações*

A existência de controle interno na organização pressupõe a existência de uma estrutura de controle. Segundo o relatório do COSO (1992[3]) esta estrutura está baseada em cinco componentes interrelacionados:

- **ambiente de controle**

  O ambiente de controle é a base sobre a qual se apoiam todos os outros componentes, porque rege a organização, influenciando a consciência de controle de seus integrantes. Compreende integridade, valores éticos e competência das pessoas da organização, filosofia gerencial e estilo operacional, o modo como a administração delega autoridade e responsabilidade, organiza e desenvolve as pessoas e a atenção e direção fornecida pelo conselho de administração.

- **avaliação de riscos**

  Todas instituições enfrentam uma variedade de riscos provenientes de fontes externas e internas que têm que ser avaliados. Um pré-requisito para avaliação de riscos é o estabelecimento de objetivos interligados e consistentes. A avaliação de riscos envolve a identificação e análise das ameaças que possam comprometer o alcance dos objetivos, formando uma base para determinar como o risco deve ser administrado. Como as condições mudam, são necessários mecanismos para tratar estas mudanças.

- **atividades de controle**

  São políticas e procedimentos que ajudam a assegurar que as decisões gerenciais estão sendo seguidas. Também ajudam a assegurar que ações necessárias são tomadas para enfocar e mitigar riscos para que a organização alcance seus objetivos. Podem ocorrer através da organização em todos os níveis hierárquicos e inclui atividades como aprovações, autorizações, revisões de desempenho operacional e segregação de tarefas.

- **informação e comunicação**

  A informação adequada precisa ser identificada, obtida e comunicada no formato e tempo oportuno de maneira que permita às pessoas executarem suas responsabilidades. As informações compreendem não apenas os dados gerados internamente, mas também dados e eventos externos. A comunicação para ser eficaz deve fluir por toda a organização e todo pessoal deve ter claramente definido seu papel no sistema de controle interno e como sua atividade se relaciona com o trabalho dos outros. Também deve fluir com os parceiros externos, clientes, fornecedores, órgãos de tutela e acionistas.

---

[3] A versão pesquisada neste trabalho foi editada em Julho/1994, tendo como base o relatório de 1992.

- **monitoração**

  O sistema de controle interno deve ter sua qualidade avaliada ao longo do tempo. Esta avaliação pode tanto ser permanente (o acompanhamento ser feito durante o curso normal das operações), como em avaliações separadas do processo normal ou ainda uma combinação dos dois critérios.

Ainda de acordo com o relatório COSO, existe uma sinergia entre os componentes formando um sistema integrado que reage dinamicamente às mudanças. Este sistema de controle interno está entrelaçado com as operações da organização e se torna mais efetivo quando está construído sobre a infra-estrutura organizacional e faz parte da filosofia da empresa.

As Normas Internacionais de Auditoria (1997)[4], na Norma 400 - Avaliações de Risco e Controle Interno, estabelecem que o auditor deve obter um entendimento de controle interno suficiente para planejar a auditoria e executá-la de maneira eficaz. Para isso, deve avaliar o risco de auditoria e definir procedimentos para garantir que esse risco foi reduzido a um nível aceitável. "Risco de auditoria", de acordo com esta norma, significa o risco de que o auditor expresse uma opinião incorreta ou dê um parecer errado, no caso das demonstrações contábeis possuírem distorções significativas. Para a geração do risco de auditoria cooperam três tipos de riscos:

- *"risco inerente" - é a suscetibilidade do saldo de uma conta ou classe de transações a uma distorção que poderia ser relevante, individualmente ou quando considerada em conjunto com distorções em outros saldos ou classes, desde que não houvessem controles internos correlatos*
- *"risco de controle" - é o risco de que os sistemas contábeis e de controle interno deixem de prevenir ou detectar, e corrigir em tempo hábil, uma distorção no saldo de uma conta ou classe de transações, que poderia ser relevante, individualmente ou quando agregada em outros saldos ou classes*
- *"risco de detecção" - é o risco de que os procedimentos de comprovação de um auditor não detectem uma distorção existente no saldo de uma conta ou classe de transações que possa ser relevante, individualmente ou quando considerada em conjunto com distorções em outros saldos ou classes*

O conceito de risco de auditoria expresso nas Normas Internacionais de Auditoria (NIA) é específico para auditoria de demonstrações financeiras. Todavia o conceito de risco pode ser estendido, sem prejuízo do sentido original, para auditoria de outras informações ou de serviços correlatos.

---

[4] A Federação Internacional de Contadores (IFAC - International Federation of Accountants) divulga periodicamente normas aplicáveis à auditoria de demonstrações contábeis, que devem também ser aplicadas (com as necessárias adaptações) a auditorias de outras informações e a serviços correlatos: as Normas Internacionais de Auditoria. Também divulga os Pronunciamentos Internacionais de Auditoria, que visam orientar os auditores na implantação das normas. Em 1998 o IBRACON - Instituto Brasileiro de Contadores, com a permissão da IFAC traduziu e publicou em português as normas e pronunciamentos emitidos até 1° de julho de 1997.

Ao executar a avaliação do controle interno procura-se verificar se objetivos de controle estão sendo atendidos, isto é, se a finalidade para a qual um procedimento de controle existe está sendo atingida. Como existem vários fatores que influenciam o atendimento destes objetivos de controle, procura-se garantir, com razoável segurança, tal atendimento. Este parâmetro "razoável segurança" deve sempre ser levado em consideração, pois a segurança integral dificilmente pode ser atingida porque:

- é impossível obter-se total segurança do atendimento, ou
- o volume de controles para garantir segurança integral torna este processo muito dispendioso, não compensando o benefício dele decorrente; ou
- a implementação de todos os controles necessários em um processo podem torná-lo inviável operacionalmente.

4.2 A auditoria em um ambiente computadorizado

A avaliação da estrutura de controle interno existe independentemente da ferramenta utilizada para tratamento e divulgação das informações. Obviamente quando estas são tratadas através de processamento eletrônico, os mecanismos para avaliar o ambiente de controle são diferentes. Não necessariamente existe uma trilha visível de todos os tratamentos que um dado recebeu para se transformar em uma informação relevante para o processo organizacional.

Boynton e Kell (1996) traçam as seguintes diferenças que afetam o controle interno ao comparar o processamento manual e o computadorizado:

- o sistema computadorizado pode produzir uma trilha da transação que esteja disponível para auditoria apenas por um curto espaço de tempo
- freqüentemente existe menos evidência dos procedimentos de controle nos sistemas computadorizados do que nos manuais
- as informações nos sistemas manuais são visíveis, ao contrário dos arquivos e registros nos sistemas computadorizados, que não podem ser lidos sem a ajuda de um computador
- a diminuição do envolvimento humano nos sistemas computadorizados pode ocultar erros que poderiam ser identificados em sistemas manuais
- as informações em sistemas computadorizados pode ser mais vulnerável a desastres físicos, manipulação não autorizada e defeitos mecânicos que as informações em sistemas manuais
- várias funções podem ser concentradas nos sistemas computadorizados, reduzindo assim a segregação de funções seguida nos sistemas manuais
- as mudanças nos sistemas computadorizados são mais difíceis de implementar e controlar que nos sistemas manuais
- os sistemas computadorizados podem fornecer um nível de consistência mais confiável que os manuais porque sujeita todas as transações aos mesmos controles

- relatórios que subsidiem a administração podem ser fornecidos de maneira mais oportuna por sistemas computadorizados que por sistemas manuais

Embora as duas últimas diferenças favoreçam o ambiente computadorizado, as outras sete representam problemas ou riscos maiores, que devem ser tratados na estrutura de controles internos.

Comparando os riscos no sistema computadorizado e controles para mitigar tais riscos, apontados por Boynton e Kell (1996), com a abordagem recomendada pelas Normas Internacionais de Auditoria (1997), identifica-se diversas semelhanças. Visando evitar a redundância de informações, é apresentada a seguir a visão de Boynton e Kell, de maneira sucinta. No Apêndice 3, com um nível maior de detalhamento, apresenta-se a abordagem existente nas Normas Internacionais de Auditoria.

O tratamento dos riscos trazidos pelo sistema de informação computadorizado, de acordo com Boynton e Kell (1996), pode ser feito por controles gerais e controles de aplicação.

Os controles gerais compreendem:

- **Controles organizacionais e operacionais**

  Estão associados à filosofia gerencial, estilo operacional e estrutura organizacional. Estes controles estão associados à segregação de tarefas dentro da área de processamento de dados e entre a área de processamento e os departamentos usuários.

- **Controles de documentação e de desenvolvimento de sistemas**

  Os controles no desenvolvimento de sistemas compreendem revisão, teste e aprovação de novos sistemas, controles de alteração de programas e procedimentos documentados.

  Os controles de desenvolvimento estão relacionados à documentação e registros mantidos pela organização para descrever as atividades de processamento computacionais.

- **Controles de equipamentos e de sistemas operacionais**

  São os controles para detectar eventuais falhas nos equipamentos ("hardware") ou sistemas operacionais ("system software") onde o processamento é efetuado.

- **Controles de acesso**

  Estes controles devem prevenir uso não autorizado dos equipamentos de processamento, arquivos de dados e programas. Incluem salvaguardas físicas (acesso restrito à área de processamento, chaves especiais, etc.) e procedimentos de revisão, como avaliação da utilização dos computadores

- **Controles de dados e processamentos**

  Fornecem uma estrutura para controlar diariamente as operações dos computadores, diminuindo a probabilidade de ocorrência de erros e

assegurando a continuidade das operações no caso de um desastre físico ou falha dos equipamentos.

Os controles de aplicações compreendem:

- **Controles de entrada**

  Estão projetados para fornecer razoável segurança que os dados recebidos para processamento estão adequadamente autorizados e que os dados inicialmente incorretos tenham sido rejeitados, corrigidos e incluídos novamente.

- **Controles de processamentos**

  Estes controles são projetados para fornecer razoável segurança que o processamento foi executado como planejado sem perder, adicionar, duplicar ou alterar dados indevidamente.

- **Controles de saídas**

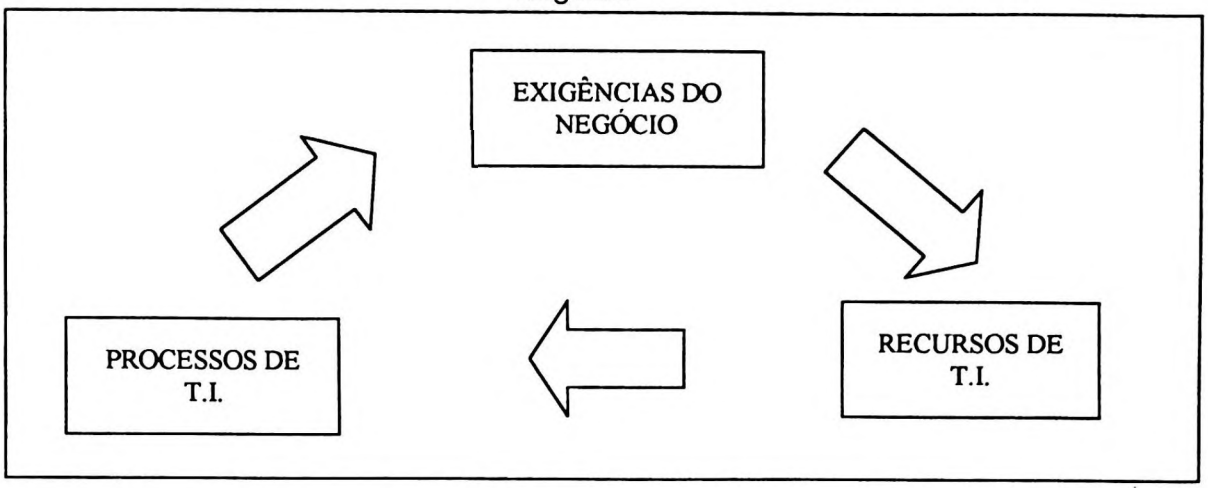
  São projetados para assegurar que o resultado do processamento (relatórios ou arquivos magnéticos) seja correto e que somente o pessoal autorizado tenha acesso a ele.

Uma associação de auditores de informática (ISACA - Information Systems Audit and Control Association, associação mundial que congrega auditores de informática de mais de 100 países), com o apoio de instituições como Unisys e Coopers & Lybrand, desenvolveu, em 1996 (com revisão em abril/98) uma estrutura para facilitar a condução de auditoria em ambientes computadorizados. Tal estrutura, baseando-se nos componentes de controle definidos no relatório COSO, procura avaliar se as exigências do negócio estão sendo atendidas pela tecnologia de informação (T.I.). Esta ferramenta chama-se COBIT - Control Objectives for Information and Related Technology.

A estrutura COBIT define que deve existir um entrelaçamento entre as exigências do negócio, os recursos de tecnologia de informações e os processos de gerenciamento destes recursos, conforme esquematizado na Figura 4.1.

O gerenciamento dos recursos de tecnologia de informações é feito através de processos de T.I., que consolidam as diversas atividades relacionadas à tecnologia da informação, para atender as exigências do negócio. A execução destas atividades deve ser feita de forma que se atinjam objetivos de controle. Alcançando-se estes objetivos, existe uma razoável segurança que as exigências do negócio estejam sendo atendidas. A função da auditoria é avaliar a execução destas atividades e se os objetivos de controle correspondentes a elas estão sendo atingidos.

Figura 4.1 - Entrelaçamento da Tecnologia de Informações com as exigências do negócio



Fonte: Estrutura COBIT (1998)

A estrutura COBIT (1998) define controle como sendo

> *as políticas, procedimentos, práticas e estruturas organizacionais projetadas para fornecer razoável segurança que os objetivos do negócio serão atingidos e que eventos não desejados serão prevenidos, detectados e corrigidos.*

Objetivo de controle em tecnologia de informações é definido na estrutura COBIT como

> *uma declaração do resultado desejado ou propósito a ser atingido com a implementação de procedimentos de controle em uma atividade específica de tecnologia de informações.*

Segundo a estrutura COBIT as informações para serem úteis ao processo comercial devem satisfazer às seguintes exigências do negócio:

- **eficácia**

  A informação deve ser relevante e pertinente ao processo comercial, ser disponível oportunamente, de maneira correta, consistente e utilizável.

- **eficiência**

  A informação deve ser obtida utilizando os recursos da maneira mais produtiva e econômica.

- **confidencialidade**

  Deve haver proteção às informações sensíveis contra divulgação não autorizada.

- **integridade**

  A informação deve ser correta e válida em relação às expectativas e valores do negócio.

- **disponibilidade**

  A informação deve estar disponível quando exigida pelo processo do negócio tanto no momento atual quanto no futuro.

- **conformidade**

  Diz respeito ao atendimento às exigências externas ao negócio, na obediência às leis, regulamentos e acordos aos quais ele está sujeito.

- **confiabilidade**

  A informação deve ser fornecida de forma apropriada para o gerenciamento financeiro e operacional da entidade.

A abordagem COBIT define que a geração das informações para o negócio é feita utilizando os seguintes recursos de tecnologia de informações:

- **dados**

  Objetos em seu sentido mais amplo (tanto internos, quanto externos), estruturados ou não.

- **sistemas aplicativos**

  O conjunto de procedimentos manuais e mecanizados que tratam os dados, transformando-os em informações.

- **tecnologia**

  Compreende hardware, sistemas operacionais, sistemas de gerenciamento de banco de dados, redes, etc.

- **instalações**

  Todos os recursos para hospedar e apoiar os sistemas de informações.

- **pessoas**

  Pessoal que efetua o planejamento, organização, aquisição, implantação, manutenção e monitoração dos sistemas de informações e serviços.

Visando verificar se as atividades ligadas à tecnologia de informação estão atendendo seus objetivos de controle, as atividades de natureza semelhante foram agrupadas em 34 *processos*, os quais também foram agrupados, obedecendo semelhanças entre eles, em quatro *domínios*:

- Planejamento e Organização
- Aquisição e Implementação
- Produção e Suporte
- Monitoração

Uma visão resumida dos domínios, processos e objetivos de controle definidos pela estrutura COBIT (1998) é apresentada no Apêndice 4.

4.3 Síntese do ambiente de auditoria

A auditoria significa a realização de uma atividade sistemática, logicamente ordenada, para avaliação de um processo. Esta avaliação envolve comparar o processo sob exame com outro já conhecido ou com alguma diretriz estabelecida, procurando identificar eventuais desvios e propor, se for o caso, medidas que melhorem o processo analisado.

O ambiente de auditoria compreende avaliação dos controles que permitam à administração a gestão adequada das operações da organização. Quando estes controles estão suportados em uma plataforma computadorizada, a avaliação executada pela auditoria deve envolver também o ambiente de tecnologia de informações.

No contexto deste trabalho, a influência do ambiente de auditoria é exercida através do estabelecimento de padrões de atuação para avaliação dos controles associados à atuação na rede. Esta avaliação visa fornecer à administração subsídios para julgar se os controles existentes são adequados e se o risco de operar na Internet é conhecido e aceito.

No capítulo 5 a atuação da auditoria de informática na avaliação do comércio eletrônico através da Internet é estudada com um nível de detalhamento maior.

Capítulo 5

AUDITORIA NO COMERCIO ELETRÔNICO ATRAVÉS DA INTERNET

A abertura das empresas para a Internet é recente. A auditoria ainda está em busca de caminhos próprios para desenvolver suas atividades neste novo ambiente e assegurar-se que a empresa está operando com um nível de risco conhecido e aceito por seus proprietários.

Embora não tenha sido identificada definição formal de entidades ligadas à auditoria divulgando normas de atuação no novo ambiente, documentos disponíveis na rede fornecem indicações dos caminhos que devem ser seguidos. Como exemplo destes documentos pode-se destacar o elaborado por Guttman e Bagwill (1997) disponível, ainda no formato de "draft", no site do National Institute of Standards and Technology (http://csrc.nist.gov). Este documento, chamado *Internet Security Policy: A Technical Guide,* tece comentários gerais sobre Internet, riscos associados a este ambiente e fornece recomendações de políticas e proteções que podem ser adotadas, dependendo da sensibilidade das informações que precisam ser protegidas. Um resumo destas recomendações é apresentado na seção 5.1.

Além do subsídio oferecido por documentos disponíveis na rede, conforme o exemplificado acima, a condução da auditoria no ambiente Internet deve basear-se também em estruturas existentes de auditoria, efetuado-se adaptação destas às características próprias do ambiente de rede. Como exemplo destas metodologias, pode-se destacar a COBIT (1998), no que se refere aos processos para garantir a segurança das informações e monitoração dos processos de tecnologia de informações. Estas estruturas estão apresentadas na seção 5.2.

Na seção 5.3 é apresentada uma síntese dos aspectos relevantes para a condução de auditoria no comércio eletrônico através da Internet. Esta síntese está baseada nos fatores técnicos e conceitos de auditoria, detalhados nos capítulos 3 e 4, e nos comentários apresentados nas seções 5.1 e 5.2. Pretende-se com esta síntese fornecer uma contribuição para execução de novas pesquisas envolvendo o assunto.

5.1 Política de segurança na Internet

O primeiro passo para o estabelecimento de uma política de segurança é conhecer o grau de sensibilidade das informações que se quer proteger. Conhecida a importância de cada informação, pode-se projetar os mecanismos de proteção, atribuindo-se os controles mais sofisticados (e dispendiosos) proporcionalmente à importância das informações por eles protegidas.

O tratamento das informações é efetuado através de processos e é nestes que os controles devem ser incorporados. As políticas de segurança devem destacar cada processo e descrever os controles que devem revestir as informações, indicando-se os que deverão ser usados para cada nível de sensibilidade.

Guttman e Bagwill (1997) descrevem sete processos associados ao tratamento de informações. Os controles usualmente aplicáveis dependem da sensibilidade da informação que o processo está tratando. Um resumo desta visão é apresentado a seguir:

- **Identificação e autenticação**

  É o processo de reconhecimento e validação do usuário, usado para determinar quais recursos ou sistemas ele está autorizado a acessar. Este processo está desdobrado em:

  - políticas gerais de identificação e autorização para a Internet, onde define os controles associados aos recursos de importância baixa, média e alta
  - políticas de gerenciamento de passwords, descrevendo as características das senhas, prazos de validade, etc.
  - políticas de autenticação, tratando da segurança obtida com processos de autenticação e do custo da sua utilização
  - Certificados e assinaturas digitais

- **Controle da aquisição de software**

  É o processo de verificação dos programas que estão sendo recebidos ou adquiridos. Envolve:

  - Prevenção, detecção e remoção de vírus
  - Controle de softwares interativos, como Java e ActiveX (por exemplo), baixados pelo servidor para serem executados no computador do usuários
  - Licença de utilização de softwares

- **Criptografia**

  É o processo de codificação das informações armazenadas internamente ou em trânsito através da rede. Está desdobrado em:

  - Política geral de criptografia
  - Regras de codificação para acessos remotos efetuados através da Internet ou não

- **Arquitetura de sistemas**

  A conexão à Internet envolve decisões associadas a estrutura dos sistemas que têm impacto direto na segurança de todas as informações da organização. Os aspectos abordados compreendem:

  - Uso da Internet para suportar a rede interna da empresa (VPN - Virtual Private Network)

- Possibilidade de acessos a sistemas externos a partir da rede interna sem utilização de mecanismos previamente configurados para isso (por exemplo, micros ligados à rede interna usando modem para se conectar ao ambiente externo, desviando-se assim dos mecanismos de segurança previstos para a conexão à Internet
- Acesso a banco de dados internos; este acesso pode ser fundamental caso, por exemplo, a organização esteja fazendo uso de uma VPN
- Uso de múltiplos firewalls, organizados em linha para proporcionar aumento de segurança (para acessar dados de maior sensibilidade deve-se atravessar bloqueios com grau crescente de dificuldades) ou em paralelo, para proporcionar melhor desempenho (quando o negócio exigir agilidade na resposta)

- **Tratamento de incidentes**

  Incidentes são eventos que podem trazer conseqüências adversas reais ou potenciais, resultando em fraude, perda, ou comprometimento das informações. Neste tópico as políticas devem prever:

  - Detecção da invasão, isto é, instrumentos que permitam detectar eventuais "portas abertas" ou "portas violadas"
  - Reação a invasões, ou seja, procedimentos para tratar possíveis violações, visando manter a tranqüilidade e contornar o problema

- **Infra-estrutura administrativa**

  A política de segurança na Internet deve estar fortemente ligada à utilização e gerenciamento deste ambiente no dia a dia. Este processo compreende:

  - Definição da estrutura funcional responsável pela viabilização dos mecanismos de segurança e conferindo ao administrador da rede poder para configurá-la no formato mais adequado à organização
  - Definição do uso apropriado dos recursos da Internet às exigências da organização
  - Privacidade, definindo-se como as informações que trafegarem pela rede poderão ser monitoradas

- **Consciência e educação**

  Envolve a divulgação dos riscos associados à utilização da rede e formação de todos os usuários para identificarem prontamente eventuais ocorrências que fragilizem a segurança. Este processo envolve a divulgação ampla a todos usuários da organização das políticas de segurança que regem a utilização da Internet naquela organização.

5.2 Estrutura para avaliação de segurança

São apresentadas a seguir atividades relacionadas à segurança de sistemas e os objetivos de controle que devem ser atingidos com a execução destas atividades.

Estas atividades e objetivos de controle foram extraídos da estrutura COBIT (1998), procurando-se focar aquelas com relacionamento mais estreito com a prática do comércio eletrônico através da Internet.

- **Identificação, autenticação e acesso**

  O objetivo de controle neste caso é que o acesso lógico e uso dos recursos de computação sejam delimitados pela implementação de adequados mecanismos de autenticação e identificação de usuários e de recursos associados a estas regras de acesso. Tais mecanismos devem impedir acesso de pessoal não autorizado e conexões a partir de modems ("dial-up") dos equipamentos internos

- **Segurança no acesso "on-line" aos dados**

  Devem ser implementados procedimentos coerentes com a política de segurança que forneça controle de segurança de acesso baseado na necessidade de cada usuário para visualizar, incluir, alterar ou excluir dados.

- **Vigilância**

  Os serviços de informações da administração de segurança devem assegurar que atividades de segurança são registradas e que qualquer indicação de uma iminente violação de segurança seja notificada imediatamente para o administrador da rede e que medidas de proteção sejam acionadas automaticamente

- **Classificação dos dados**

  A administração deve implementar procedimentos para assegurar que todos os dados sejam classificados formalmente, segundo sua sensibilidade, pelo proprietário destes dados baseando-se em um esquema previamente definido. Até mesmo os dados que não necessitam de proteção devem passar por esta avaliação formal.

- **Centralização na identificação e gerenciamento de direitos de acesso**

  Devem existir controles para assegurar que o gerenciamento na concessão de direitos de acesso esteja centralizado, visando obter-se consistência e eficiência do controle de acesso global.

- **Relatórios sobre violações e atividades da segurança**

  A administração de segurança deve assegurar que violações e atividades da segurança sejam registradas, relatadas, revisadas e identificadas regularmente, para detectar e solucionar incidentes relacionados a atividades não autorizadas.

- **Tratamento de incidentes**

  A administração deve estabelecer uma capacidade de tratamento de incidentes fornecendo uma plataforma centralizada com suficiente familiaridade do ambiente e equipamentos com dispositivos rápidos e seguros de comunicação. A responsabilidade pelo gerenciamento de incidentes deve ser estabelecida para assegurar uma apropriada, efetiva e oportuna resposta aos incidentes de segurança

- **Revalidações**

  A administração deve assegurar que revalidações de segurança são executadas periodicamente para manter atualizado o nível de segurança aprovado e o risco residual aceito. Este risco residual corresponde àquele que os mecanismos de controle não permitem eliminar

- **Reciprocidade de confiança**

  A política organizacional deve assegurar que práticas de controle sejam implementadas para verificar a autenticidade de parceiros fornecendo instruções ou executando transações eletrônicas. Este controle pode ser implementado com a troca segura de senhas, chaves de criptografia ou dispositivos físicos de identificação.

- **Autorização de transações**

  A política organizacional deve assegurar, onde aplicável, a implementação de controles, como técnicas de criptografia para assinatura e verificação de transações, visando assegurar sua autenticidade.

- **Não repúdio**

  A política organizacional deve assegurar que, onde aplicável, transações não possam ser negadas pelo parceiro, e que provem o recebimento e processamento das transações. Tal controle pode ser obtido através da implementação de assinaturas digitais por exemplo.

- **Caminho confiável**

  Devem existir controles que assegurem que dados de transações sensíveis somente sejam trocados através de um caminho confiável. Informações sensíveis incluem aquelas relacionadas ao gerenciamento da segurança, dados confidenciais, senhas e chaves criptográficas. Para atingir este objetivo, pode ser necessário criar-se canais confiáveis que envolvam também utilização de criptografia entre usuários, entre usuários e sistemas e entre sistemas.

- **Proteção das funções de segurança**

  Toda segurança associada aos equipamentos e sistemas deve ser permanentemente protegida contra tentativas de comprometer sua integridade e contra divulgação de suas chaves secretas. Paralelamente, as organizações devem manter reservas sobre seu plano de segurança, mas não confiando sua segurança exclusivamente na manutenção da confidencialidade deste plano

- **Gerenciamento de chaves criptográficas**

  A administração deve definir e implementar procedimentos e protocolos a serem usados para geração, distribuição, certificação, armazenamento, entrada, uso e arquivamento de chaves criptográficas assegurando-se que estão protegidas contra modificações ou exposição não autorizada. Se uma chave for comprometida, a administração deve assegurar-se que o fato seja propagado

através do uso de "Listas de Revogação de Certificados" ou mecanismos similares

- **Prevenção, detecção e correção de programas danosos**

  A administração deve definir mecanismos para prevenir, detectar e corrigir programas ofensivos à organização (como vírus e cavalos de Tróia, por exemplo)

- **Arquiteturas de firewall e conexões com a rede pública**

  Firewalls adequados devem operar para proteger contra todas tentativas de acesso não autorizado aos recursos internos. Os controles devem existir tanto no sentido da rede para a organização quanto no sentido inverso

- **Proteção de valores eletrônicos**

  A administração deve proteger a integridade permanente de todos os cartões ou outros dispositivos físicos utilizados para autenticar ou armazenar informações financeiras ou sensíveis, levando em consideração os dispositivos e métodos de validação utilizados.

5.3 Síntese dos aspectos a considerar na auditoria do ambiente para prática do comércio eletrônico através da Internet

A prática do comércio eletrônico através da Internet requer que esta atividade esteja suportada em uma estrutura que garanta integridade, disponibilidade, e confidencialidade. Além disso, é fundamental que as organizações, ao se colocarem na rede, tenham seu ambiente interno razoavelmente protegido contra acessos não autorizados.

Resumindo os aspectos identificados na pesquisa bibliográfica pode-se concluir que para avaliar se estes objetivos estão sendo atendidos, o foco de uma auditoria no ambiente de prática de comércio eletrônico através da Internet envolve, além das verificações já destacadas na seção 4.2, os seguintes cuidados especiais:

- **Política de segurança**
  - Avaliar a existência e adequação de uma política ampla que defina postura da organização para tratamento de suas informações, com critérios objetivos para classificação da sensibilidade destas informações e de atribuição de responsabilidades aos seus proprietários.

- **Acesso ao interior da organização**
  - Identificar e avaliar os dispositivos que controlam o acesso ao interior da organização, verificando onde estão instalados, sua configuração e se são compatíveis às informações que devem proteger.
  - Controles para assegurar que usuários externos somente terão acesso aos aplicativos e informações reservados para eles e que estes caminhos não sejam passíveis de alterações efetuadas remotamente.

- Identificar e avaliar mecanismos de detecção de invasões e procedimentos caso estas ocorram.
- Controles sobre informações íntegras (arquivos de "back up") que permitam reativação das operações caso ocorra algum sinistro decorrente da rede (contaminação por vírus, por exemplo ou danos nas informações existentes).
- Controles para evitar que a organização seja usada como intermediária de ataque a outro "site", quer este ataque seja proveniente de usuários internos da empresa, quer seja através de usuário externo que se passa por usuário interno.
- Mecanismos para identificar e, se possível, reprimir ataques que indisponibilizem acesso ao site (por exemplo, através da inundação de mensagens sem sentido).
- Controle sobre informações que transitem internamente na empresa para evitar que sejam visualizadas e/ou manipuladas por usuários não autorizados.

- **Acesso às informações que transitam na rede**
  - Identificar e avaliar os controles sobre as informações que trafeguem pela rede para resguardá-la contra visualizações e/ou modificações indevidas.
  - Controles sobre chaves secretas da organização (quem são os responsáveis por sua custódia, procedimentos de alterações e procedimentos de contingência para o caso de serem perdidas).

- **Autenticação das partes envolvidas em negócios através da rede**
  - Identificar e avaliar os mecanismos utilizados para reconhecimento dos parceiros da organização, atentando para controles que resguardem contra repúdio indevido.
  - Controles para aceitação e inclusão de novos parceiros e para exclusão daqueles com os quais não são mantidas mais operações.

- **Manutenção atualizada das versões de programas de segurança**
  - Avaliar mecanismos que garantam a permanente atualização dos mecanismos que forneçam segurança como programas anti-vírus, firewalls, etc.

Estas avaliações procuram verificar se a estrutura tecnológica e organizacional fornece mecanismos que permitam à instituição operar com um nível de segurança conhecido e aceito por sua administração. Caso se identifique novas vulnerabilidades, as mesmas devem ser informadas formalmente à administração, a qual deve analisar o custo e o benefício das modificações, ordenar as mudanças aplicáveis e estar consciente do novo nível de risco assumido.

Capítulo 6

METODOLOGIA

A condução de um projeto de pesquisa, segundo Yin (1989), envolve:

- obtenção de uma estrutura teórica, que apoiará o trabalho,
- a definição da estratégia para a condução do estudo,
- a realização da pesquisa propriamente dita, atentando para o estabelecimento de parâmetros que garantam sua qualidade, e
- a formulação de conclusões, baseadas na fundamentação teórica e nas observações efetuadas na pesquisa.

A estrutura teórica que orientou a realização deste trabalho, está explicitada nos Capítulos 2 a 5.

A estratégia de pesquisa utilizada foi um estudo de caso abordando a atuação da auditoria de informática em uma instituição financeira que pratica o comércio eletrônico através da Internet. As justificativas para escolha desta abordagem e cuidados adotados na sua aplicação estão apresentados neste Capítulo 6.

A aplicação da pesquisa está descrita no Capítulo 7 e, no Capítulo 8, são apresentadas as conclusões obtidas.

6.1 Estudo de Caso

Yin (1989) relacionou estratégias de pesquisa com as situações relevantes para sua escolha. Nesta análise, resumida no Quadro 6.1, aponta-se que a escolha da estratégia depende de três condições:

- o tipo da questão básica da pesquisa
- o controle que o pesquisador tem sobre os eventos comportamentais reais
- o grau de foco em eventos contemporâneos em oposição a eventos históricos

No Quadro 6.1 pode-se observar que o estudo de caso além de responder às questões "Como?" e "Por que?", foca em eventos contemporâneos e não requer controles sobre eventos comportamentais.

Quadro 6.1 - Situações relevantes para diferentes estratégias de pesquisa

Estratégia	Forma da questão de pesquisa	Requer controles sobre eventos comportamentais	Foca em eventos contemporâneos?
Experimentação	Como, Por que	Sim	Sim
Pesquisa de campo	Quem, O que*, Onde, Quanto	Não	Sim
Análise de arquivos	Quem, O que*, Onde, Quanto	Não	Sim ou Não
Histórico	Como, Por que	Não	Não
Estudo de Caso	Como, Por que	Não	Sim

Observação: (*) O que, quando perguntado como parte de um estudo exploratório, pertence a todas as cinco estratégias

Fonte: Yin (1989)

O estudo de casos, de acordo com Yin (1989), é um questionamento empírico que:

- investiga um fenômeno contemporâneo dentro de um contexto de vida real, cujas
- fronteiras entre o contexto e o fenômeno não estejam claramente definidas e no qual
- múltiplas fontes de evidência sejam utilizadas.

Martins (1994) aponta o estudo de casos como um dos tipos de abordagens utilizado nas pesquisas sociais (educação, administração, contabilidade, economia, etc.). Segundo ele, este método "dedica-se a estudos intensivos do passado, presente e de interações ambientais de uma (ou algumas) unidade social: indivíduo, grupo, instituição, comunidade... São validados pelo rigor do protocolo estabelecido."

Yin (1989) comenta que a utilização de estudo de casos, embora bastante utilizada em campos orientados pela prática, tem sido criticada. Tais críticas decorrem principalmente de preconceitos envolvendo a perda de rigor nas pesquisas com estudo de caso, a dificuldade em se efetuar uma generalização científica e ao fato de estudos de casos normalmente envolverem extenso período de tempo, gerando, consequentemente, relatórios maçantes e de difícil leitura.

Contrapondo a estas críticas, Yin comenta que a falta de rigor também pode ocorrer quando se usa outras estratégias de pesquisa. Para evitá-la é necessário que o pesquisador desenvolva grande esforço. Quanto à generalização, Yin sustenta que, a partir de estudo de casos, é possível efetuar-se generalizações para proposições teóricas e não para populações ou universos. Para tornar possível esta proposição teórica é fundamental que se construa uma base teórica relacionada aos tópicos em estudo, pois esta facilitará a coleta de informações e proporcionará o contexto no qual a generalização do estudo de caso vai ocorrer. Quanto à extensão do levantamento e dificuldade de sua leitura, Yin argumenta que a crítica não procede, pois pode-se realizar um projeto de estudo de caso que não seja longo e com relatório adequadamente redigido.

A proposta para este trabalho enquadra-se às características que Yin aponta como recomendando o estudo de caso. O tipo das questões pesquisadas, conforme detalhado mais adiante, enquadra-se nas características "como?" e "por que?". Não existe controle sobre os eventos em estudo nem sobre o comportamento dos agentes estudados, uma vez que o pesquisador, embora atuando na organização sob estudo, não participava diretamente da área da auditoria responsável por avaliar os processos ligados à prática do comércio eletrônico através da Internet. Finalmente, o foco se dá sobre um fato que iniciou em passado recente (três anos) e que ainda está ocorrendo.

Uma vez escolhido o estudo de casos como sendo a estratégia de pesquisa a ser utilizada, é necessário optar-se entre o estudo de um caso individual ou de múltiplos casos. Ainda segundo Yin (1989), o estudo de um caso único pode ser feito quando ocorre uma das seguintes situações:

- **caso crítico**

  Quando o caso pode ser usado para sustentar uma teoria bem formulada. Neste caso a teoria tem um conjunto claro de proposições e circunstâncias dentro das quais se acredita que as proposições sejam verdadeiras.

- **caso único ou extremo**

  Quando o caso corresponde a uma situação rara, que não seja passível de nova observação.

- **caso revelador (*"revelatory case"*)**

  Esta situação ocorre quando o pesquisador tem oportunidade de observar e analisar um fenômeno previamente inacessível à investigação científica, muito embora eventos semelhantes ao observado possam estar acontecendo em outros lugares.

A escolha do estudo de caso único neste trabalho foi feita baseada na terceira razão apontada por Yin. O pesquisador acompanhou desde o início, a implantação da equipe da auditoria interna voltada à avaliação da atuação da organização na prática do comércio eletrônico através da Internet. Com isso tinha oportunidade de conduzir uma pesquisa mais profunda da instituição, o que não seria possível se não vivesse seu cotidiano.

A definição sobre o tipo de organização pesquisada (uma instituição financeira) foi decorrente do alto nível de sensibilidade deste tipo de organização a um relacionamento mais aberto entre seus ambientes interno e externo. O patrimônio de uma instituição financeira é bastante volátil (os recursos financeiros não têm "carimbo" de procedência) e, de maneira geral, o ambiente interno de tecnologia de informações é que provê controles sobre este patrimônio. Como a atuação na prática do comércio eletrônico através da Internet envolve abertura do ambiente interno para o mundo exterior, o risco associado às operações transforma-se, levando também à alteração na atuação da auditoria.

6.2 Componentes do estudo de caso

Quando a pesquisa envolver um estudo de caso, Yin (1989) aponta que cinco componentes são particularmente importantes:

- as questões do estudo;
- suas proposições, se existentes;
- sua(s) unidade(s) de análise;
- a ligação lógica entre os dados e as proposições e
- os critérios para interpretar os achados.

O tipo de questões que se pretende responder com a pesquisa é um dos fatores chaves que orientam a escolha de estratégia de pesquisa mais adequada. Neste trabalho as questões foram formuladas buscando-se identificar "como" é a atuação da auditoria interna de uma instituição financeira em particular que pratica o comércio eletrônico através da Internet e "por que" este critério de atuação foi adotado. As questões objeto de estudo foram as seguintes:

1. Por que foi implantada a auditoria de informática no ambiente de comércio eletrônico através da Internet na organização?
2. Como a organização adquiriu habilidade para executar auditoria no ambiente de comércio eletrônico através da Internet? Por que foi feito desta forma?
3. Foi utilizado algum projeto piloto para implantação da área na organização?
4. O que a organização considera como competências necessárias para que um auditor atue no ambiente Internet?
5. A implantação da auditoria no comércio eletrônico através da Internet trouxe alguma modificação no processo de desenvolvimento de sistemas da organização?
6. Os aspectos relevantes identificados na pesquisa bibliográfica envolvendo política de segurança, acesso ao ambiente interno e às informações em trânsito, são objeto de exames de auditoria? Como são aplicadas estas verificações?
7. Como a auditoria se assegura que a técnica utilizada para proteção é válida e é compatível com o valor da informação protegida?
8. Existe algum processo de medição para assegurar a eficiência da área?
9. Como a auditoria no ambiente de Internet se assegura que está conduzindo seus trabalhos de maneira a auxiliar a administração no conhecimento e avaliação dos riscos aos quais a organização está exposta?
10. Quais os aspectos positivos e negativos para a organização decorrentes da implantação da auditoria de informática na prática do comércio eletrônico através da Internet?

No segundo componente do estudo de caso apontado por Yin, cada proposição dirige a atenção para algo que deve ser examinado dentro da abrangência do estudo. Yin comenta que nem todos estudos têm uma proposição, ou uma hipótese, a ser testada. Situações que dispensam a formulação de uma proposição correspondem a estudos exploratórios. Entretanto, mesmo para tais estudos, é

necessário estabelecer-se um objetivo que se pretende atingir. O propósito do estudo foco deste trabalho foi identificar fatores que direcionam a atuação da auditoria no comércio eletrônico através da Internet e descrever a forma como esta função foi implementada em uma organização.

O terceiro componente, unidade de análise, está relacionado com a definição exata do caso a ser estudado e serve para delimitar a coleta e análise dos dados. Sem este componente haveria a possibilidade de dispersar a pesquisa, levando-se a levantar todos os tipos de dados existentes. No caso estudado, uma instituição financeira nacional de grande porte, a unidade de pesquisa é a área da auditoria interna voltada à avaliação dos controles que suportam as operações de comércio eletrônico praticadas através da Internet.

Segundo Yin (1989), o quarto e o quinto componentes do projeto de pesquisa têm sido os menos desenvolvidos nos estudos de caso, e para os quais não existe um receituário pré-definido. Estes componentes, ligação entre os dados e proposições e conclusões, envolvem a análise dos dados e apoiam-se principalmente na percepção do pesquisador. No caso estudado, busca-se cobrir estes requisitos na coleta e análise de dados, e na apresentação das conclusões.

6.3 Qualidade do projeto de pesquisa

Conforme mencionado por Yin (1989), em razão do projeto de pesquisa envolver um conjunto de enunciados, deve estar suportado por algum critério que lhe dê sustentação lógica. Em estudos de caso quatro são os testes para validar a qualidade do projeto:

- validade de construção
- validade interna
- validade externa
- confiabilidade

A validade de construção envolve o estabelecimento de medidas operacionais para os conceitos que estão sendo estudados, procurando-se diminuir a influência de fatores subjetivos. Como técnicas recomendáveis para estabelecer esta validade destaca-se o uso de múltiplas fontes de evidência, estabelecimento de uma cadeia de evidências e uso de informantes críticos, para reverem o relatório preliminar do estudo de caso. As múltiplas fontes de evidência utilizadas no trabalho foram:

- entrevista pessoal com os profissionais que atuam na área da auditoria que avalia o ambiente da organização para a prática do comércio eletrônico através da Internet
- observação pessoal das atividades da auditoria neste ambiente
- exames de parte dos programas de trabalho utilizados e dos relatórios sobre trabalhos efetuados (com as recomendações para possíveis melhorias de controles identificadas)

As observações efetuadas a partir destas diferentes fontes foram condensadas, estabelecendo-se um relacionamento lógico entre elas, baseado no referencial teórico e discutidas com o pessoal envolvido diretamente na realização de auditoria do ambiente de comércio eletrônico através da Internet.

Outro requisito para garantir a qualidade do projeto de pesquisa é o estabelecimento da validade interna, isto é, o relacionamento de causa e efeito entre eventos distintos. Este teste normalmente é mais aplicável a estudos explicativos ou causais. Para estudos de caso a questão de validade interna pode ser associada ao problema mais amplo que é o de se estabelecer inferências, que ocorrem todas as vezes em que um evento não pode ser diretamente observado. No trabalho buscou-se garantir esta validade através da utilização de múltiplas fontes de evidência e comparando-se os componentes identificados na fundamentação teórica com os obtidos no estudo de caso. Os componentes analisados estavam relacionados ao Ambiente Externo, ao Ambiente Organizacional, ao Ambiente Tecnológico, e ao Ambiente de Auditoria.

A validade externa tem sido um dos maiores empecilhos à realização de estudo de casos, em razão das críticas às possibilidades de generalização das conclusões. Yin (1989) contesta tais críticas com o argumento que o estudo de caso não utiliza generalização estatística (onde o resultado com uma amostra adequadamente selecionada pode ser generalizado para o universo). No estudo de caso, a generalização é analítica, a partir da teoria elaborada.

A outra condição para garantir a qualidade do projeto de pesquisa diz respeito à sua confiabilidade. Para garantir este quesito Yin (1989) recomenda que os procedimentos seguidos sejam documentados, visando permitir, na medida do possível, sua repetição posteriormente.

Em função das características específicas deste trabalho, onde a pesquisa envolveu o acompanhamento da implantação da auditoria em uma organização que pratica comércio eletrônico através da Internet, os testes de validade externa e possibilidade de reaplicar a pesquisa ficam comprometidos. Entretanto, apesar desta limitação, não consideramos que a mesma prejudique o resultado final do projeto.

Um último aspecto que Yin (1989) destaca como preocupação que deve ser coberta em um projeto de pesquisa é o desenvolvimento de um protocolo do estudo. O protocolo contem os instrumentos da pesquisa e as regras de sua utilização. Por incrementar a confiabilidade da pesquisa, seu uso é recomendável em estudos de caso, de forma geral, e fundamental, quando se utilizam múltiplos casos. Compõem o protocolo as seguintes seções:

- visão geral do projeto de estudo
- procedimentos de campo a serem utilizados
- questões de estudo
- guia para o relatório apresentando o estudo

A existência deste protocolo é importante por lembrar ao pesquisador a finalidade do estudo e força-o a antecipar diversos problemas, inclusive como o relatório deve ser completado.

Como este trabalho envolve um estudo de caso único, não foi desenvolvido um protocolo de pesquisa específico, mas seu conteúdo está disperso nas diversas seções que compõem o trabalho.

Capítulo 7

A PESQUISA

7.1 Caracterização do ambiente onde a pesquisa foi realizada

A organização pesquisada é uma instituição financeira nacional privada de grande porte, que atua fortemente no mercado de varejo. Visando preservar a imagem da instituição, bem como manter o sigilo de estratégias e de negócios, o nome da organização, bem como das pessoas entrevistadas, será omitido. Esta omissão não compromete o estudo, visto que as informações apresentadas são verdadeiras, não sofrendo qualquer alteração além da omissão de sua procedência. Para facilitar a referência à instituição, para efeito deste trabalho, ela será chamada de Banco "A".

Embora utilize intensivamente recursos de tecnologia de informações, o Banco "A" não costuma ser pioneiro no uso de novas ferramentas tecnológicas ou canais de comercialização. Esta atitude aconteceu também no que diz respeito à atuação através da rede mundial. Enquanto outras instituições, inclusive algumas de menor porte, tomaram a dianteira ao atuar na Internet realizando operações que sensibilizavam seus sistemas internos, o Banco "A" operava apenas com finalidade institucional. Seu "site" na rede fornecia informações genéricas sobre a instituição mas não permitia qualquer operação.

A postura conservadora se, por um lado, tira a vantagem do pioneirismo, por outro, evita que se cometam erros decorrentes da inexperiência. Como o pioneirismo tecnológico não é uma vantagem competitiva significativa no mercado financeiro, a atuação mais lenta do Banco "A" para iniciar a comercialização de produtos através da Internet não pode ser classificada como negativa.

Atualmente a instituição já opera na Internet. Entretanto esta atuação é exclusivamente no segmento B2C ("business to consumer") comercializando somente produtos ligados ao mercado financeiro. Os principais produtos comercializados hoje estão ligados às movimentações de contas correntes (como a conta corrente, propriamente dita, fundos de investimento, poupança, etc.) Estão sendo conduzidos estudos visando estender esta atuação também para o segmento B2B ("business to business"), e expandir o leque de operações, como compra e venda de ações ("home broker"), fechamento de operações de câmbio, etc.

A execução rotineira de trabalhos específicos para validação dos controles voltados para a prática de comércio eletrônico através da Internet é parte das funções de uma equipe pertencente ao Departamento de Auditoria de Informática da organização. Esta equipe, além de atuar neste ambiente, também conduz verificações nos processamentos realizados externamente ao processador central ("mainframe"), isto é, em ambientes que utilizam redes e servidores locais.

7.2 Respostas às questões formuladas

A pesquisa foi conduzida baseando-se no roteiro apresentado no Capítulo 6. Envolveu, conforme comentado naquele capítulo, questionamentos diretos aos profissionais da organização, conduzidas observações pessoais e efetuado exame da documentação dos trabalhos. Os questionamentos foram realizados através de entrevistas informais com o pessoal da auditoria.

As respostas obtidas com a pesquisa foram as seguintes:

1. **Por que foi implantada a auditoria de informática no ambiente de comércio eletrônico através da Internet na organização?**

   A administração do Banco "A" entendeu que a atuação de instituições financeiras na Internet era um fato irreversível e incentivou a área de tecnologia de informações a desenvolver ferramentas que permitissem esta atuação. Simultaneamente a esta fase de desenvolvimento e implantação de tecnologia, passou a solicitar que a área de auditoria opinasse sobre os riscos e controles existentes neste novo ambiente e auxiliasse no aprimoramento destes controles.

   Ao procurar atender a demanda da administração, o pessoal da auditoria percebeu que o ambiente de processamento de informações ao qual estava acostumado estava se modificando radicalmente. Surgiram riscos novos, desconhecidos no ambiente anterior, onde o processamento era centralizado e uma boa segurança física já garantia relativa tranqüilidade. Os conhecimentos que o pessoal de auditoria de informática detinha não eram suficientes para fornecer uma avaliação eficiente à administração do novo ambiente. Esta constatação despertou a auditoria para a necessidade de obtenção de novos conhecimentos que lhe possibilitassem continuar fornecendo à administração informações confiáveis e de maneira independente para que esta pudesse gerir a organização tendo um nível de riscos conhecido e aceito.

   Uma vez que existia a demanda da administração da organização por uma informação independente sobre riscos e controles no ambiente Internet e que para se atender esta demanda era necessário um nível específico de conhecimentos, decidiu-se pelo desenvolvimento de uma equipe voltada para atuação neste ambiente. A equipe deveria ser composta por pessoal especializado em avaliação de riscos e controles, mas que também detivesse um razoável conhecimento no ambiente Internet, de maneira a poder atuar sem depender em demasia do pessoal que dominava a tecnologia.

   Partindo-se das premissas apresentadas acima, foi criado no Departamento de Auditoria de Informática um grupo para atuar na validação dos controles que envolvessem utilização da Internet. Esta equipe foi criada em meados de 1997 e chamava-se "Auditoria de Canais Eletrônicos".

2. Como a organização adquiriu habilidade para executar auditoria no ambiente de comércio eletrônico através da Internet? Por que foi feito desta forma?

A equipe de "Auditoria de Canais Eletrônicos" possuía inicialmente dois auditores vindos do próprio Departamento de Auditoria de Informática. Os cargos destes profissionais eram "Auditor de Sistemas Sênior", ao qual coube a liderança da equipe e "Auditor de Sistemas Pleno". Posteriormente (final de 1997 e início de 1998) foram contratados mais dois profissionais. Um deles vinha de outro departamento do Banco, que detinha conhecimentos de tecnologia de informações, mas não especificamente do ambiente Internet. O outro era recém-formado e pertencia a um programa conduzido pela instituição de contratação de formandos em escolas de primeira linha (no caso o profissional estava concluindo o curso de Engenharia Elétrica, pela Escola Politécnica, da USP), visando tê-los, no futuro, em seu corpo gerencial.

Como nenhum dos membros da equipe possuía conhecimentos suficientes para atuar na validação do ambiente Internet, esta habilidade deveria ser desenvolvida. Entretanto, já possuíam conhecimento da organização (três dos componentes da equipe) e de auditoria (dois dos componentes). O conceito que orientou a formação da equipe é que seria mais produtivo formar pessoal que já vivesse o ambiente organizacional, conhecendo portanto sua estrutura, e que fosse especializado em controles antes de ser especialista em tecnologia.

A fase inicial da aquisição de cultura sobre o ambiente Internet foi feita com auto-estudo, buscando-se em publicações e em "sites" da rede, conhecimento sobre o assunto. Como exemplo dos "sites" visitados nesta fase pode-se destacar os pertencentes a instituições oficiais de auditoria de informática e de pesquisa tecnológica, assim como os ligados a órgãos do Governo Americano. Esta fase de familiarização com o assunto envolvia principalmente o líder da equipe.

Após o estágio inicial, que durou aproximadamente seis meses, passou-se a uma nova etapa, envolvendo todos os profissionais do grupo na realização de cursos formais e atuação em parceria com empresas de consultoria e de auditoria independente especializadas em testar ambientes de rede. Nestas atuações em parceria buscava-se, como resultado paralelo à avaliação do ambiente interno, adquirir conhecimento da rede e das ferramentas utilizadas para validação do ambiente.

O maior volume do treinamento formal realizado pela equipe de Auditoria de Canais Eletrônico foi conduzido junto à Escola Politécnica da Universidade de São Paulo (Laboratório de Sistemas Integráveis). A escolha desta escola foi feita a partir de indicações e baseada na própria imagem que a mesma desfruta junto à comunidade empresarial.

3. Foi utilizado algum projeto piloto para implantação da auditoria no comércio eletrônico através da Internet?

Conforme comentado na questão 2 acima, parte do treinamento dos auditores de canais eletrônicos foi feito através de atuações em parceria com empresas especializadas neste tipo de atividade. Estas atuações envolveram principalmente "testes de intrusão", onde um consultor, sem ter conhecimento prévio do ambiente interno, tentava ganhar acesso a este ambiente a partir da rede, e "testes de segurança", onde, os consultores, com o uso de ferramentas apropriadas, verificavam a segurança da rede interna e dos mecanismos de proteção existentes.

Como estas atuações em parceria não ocorreram exatamente no início da implantação da área, não se pode considerá-las como sendo "projetos piloto" do ponto de vista cronológico. Entretanto a atuação assessorada por pessoal mais especializado contribuiu para melhorar os procedimentos que estavam sendo seguidos. Visto por este ângulo, pode-se considerar que a instituição utilizou-se também de projetos piloto para implantar auditoria no ambiente de prática de comércio eletrônico através da Internet.

4. O que a organização considera como competências necessárias para que um auditor atue no ambiente Internet?

Existem três características necessárias para que um profissional atue na auditoria do comércio eletrônico praticado pela organização através da Internet:

- conhecimento do ambiente organizacional
- conhecimento de auditoria
- conhecimento da plataforma tecnológica

O conhecimento do ambiente organizacional envolve não apenas a familiaridade com a instituição propriamente dita, conhecendo sua estrutura administrativa, sua forma de atuação, sua filosofia empresarial, como também o conhecimento do mercado onde atua a instituição, isto é, os produtos financeiros, os cuidados que devem cercar o tratamento destes produtos, as restrições legais, a proteção ao sigilo bancário, etc.

O conhecimento de auditoria compreende familiaridade na avaliação de riscos e de controles que possam mitigar estes riscos, facilidade para transmitir o resultado destas avaliações à alta administração, facilidade para documentar os trabalhos efetuados, de maneira a manter as avaliações do ambiente perfeitamente evidenciadas e possibilitar que outros profissionais possam chegar às mesmas conclusões se efetuarem os mesmos exames.

O conhecimento da plataforma tecnológica está associado à familiaridade com os mecanismos que permitem a uma instituição atuar na rede de forma razoavelmente segura. Esta familiaridade não significa necessariamente conhecê-los em profundidade, mas saber como utilizá-los e como avaliá-los.

Como estas competências não são permanentes, isto é, precisam ser sempre aprimoradas, existe um programa contínuo de treinamento e atualização. Este programa contempla não apenas os aspectos associados ao conhecimento da plataforma tecnológica, que é mais volátil por sua própria natureza, como também aspectos relacionados ao ambiente organizacional e de auditoria.

5. A implantação da auditoria no comércio eletrônico através da Internet trouxe alguma modificação no processo de desenvolvimento de sistemas da organização?

O processo de desenvolvimento de sistemas do Banco "A" não segue uma metodologia, com fases perfeitamente definidas e documentadas, e que requeiram a participação da auditoria (ou de um órgão independente do desenvolvimento) para validar estas fases. Em função disso, não é possível afirmar que a implantação da Auditoria de Canais Eletrônicos tenha causado mudança no processo de desenvolvimento. Entretanto, apesar de não existir uma determinação formal, a Auditoria tem sido chamada a opinar sempre que se desenvolve ou se disponibilize uma funcionalidade que envolva utilização da Internet. Esta solicitação tem partido tanto dos gestores dos produtos quanto da área de tecnologia, que se sentem mais confortáveis em ouvir uma opinião independente sobre a segurança do processo em que estão envolvidos.

Normalmente os questionamentos compreendem tanto aspectos técnicos ligados à colocação de um produto específico na rede, como validação de critérios para reconhecimento de parceiros.

6. Os aspectos relevantes identificados na pesquisa bibliográfica envolvendo política de segurança, acesso ao ambiente interno e a informações em trânsito, são objeto de exames de auditoria? Como são aplicadas estas verificações?

A auditoria do ambiente Internet sempre que aplicável, avalia todos os mecanismos existentes para permitir razoável segurança na operação deste ambiente. Esta avaliação é efetuada em função do objetivo do exame que está sendo conduzido. Assim, por exemplo, quando está se conduzindo exame das operações de contas correntes, avalia-se a segurança do protocolo de comunicações, os caminhos que a informação trilha internamente na organização até sensibilizar os arquivos do aplicativo que trata o produto, os processos para reconhecimento da contra-parte e os critérios para criptografia das informações mantidas em arquivos internos.

Um problema identificado que contraria um aspecto bastante destacado na pesquisa bibliográfica, é que a instituição ainda não tem uma política de segurança global, válida para todas as informações da organização. A deficiência vem sendo parcialmente suprida com políticas setoriais (por exemplo, Utilização de Serviços de Internet, Segurança na Utilização da Microinformática, etc.).

O fato de existir divergência entre o modelo obtido na pesquisa bibliográfica e o identificado na prática ressalta a importância do modelo teórico: observou-se grande reincidência de problemas apontados pela auditoria decorrentes da ausência de um modelo global definindo parâmetros para classificar as informações. Com esta ausência muitas vezes utiliza-se o mesmo padrão de proteção tanto para informações sensíveis como para aquelas de pouca relevância. Tal uniformidade de tratamento para dados diferentes gera vulnerabilidade das informações sensíveis, decorrente de baixo nível de proteção, e desperdício de recursos protegendo dados pouco relevantes.

Outro fato que reforça a validade do modelo teórico quanto à necessidade de uma política global de segurança de informações, é que a instituição está desenvolvendo esta política. Existe um grupo de trabalho, formado por representantes da área de tecnologia, da auditoria, de segurança e por consultores externos. Sua divulgação está prevista para ocorrer no 2º semestre/2000. Após desta divulgação todos usuários de informações serão envolvidos visando classificar as informações que utilizam segundo os critérios estabelecidos na política.

7. Como a auditoria se assegura que a técnica utilizada para proteção é válida e é compatível com o valor da informação protegida?

Como não existe critério único para classificar informações, a análise que a Auditoria tem efetuado da adequação das técnicas de proteção utiliza-se de critérios subjetivos. Como exemplo destes critérios pode-se destacar:

- informação envolve cifras financeiras?
- existe risco à imagem da instituição?
- a informação trafega para ambiente externo à organização?
- existe algum tipo de risco legal associado à informação?

Algumas vezes a auditoria usou como critério para avaliar a proteção das informações, e tentar fugir à subjetividade do julgamento, comparações com as proteções oferecidas ao mesmo tipo de informações por instituições concorrentes.

Como tanto o uso de critérios subjetivos como o artifício de comparação com concorrentes têm sido fortemente questionados, principalmente pela área de tecnologia, este ainda é um ponto de constantes atritos e de desgastes do trabalho. A implementação do processo de classificação de informações pelos usuários, após a divulgação da política global de segurança, comentadas na questão anterior, devem diminuir este problema.

8. **Existe algum processo de medição para assegurar a eficiência do grupo da auditoria que atua no ambiente da prática de comércio eletrônico através da Internet?**

   Não existe um processo formal de avaliação de desempenho das áreas de administração e suporte do Banco "A". Todavia, o próprio retorno obtido através de convites à participação da Auditoria na validação da segurança de produtos que serão lançados através da rede, comentado na questão 5, pode ser um indicador que a área está cumprindo seus objetivos.

   Deve-se destacar que o chamado à participação da Auditoria é feito espontaneamente pelas áreas e não para cumprir normas formais da administração da organização.

9. **Como a auditoria no ambiente de Internet se assegura que está conduzindo seus trabalhos de maneira a auxiliar a administração no conhecimento e avaliação dos riscos aos quais a organização está exposta?**

   As técnicas descritas a seguir valem para toda a Auditoria e não apenas para o grupo que valida o ambiente Internet. A resposta a esta questão envolveu dois enfoques: a aderência às expectativas da administração quanto à atuação da auditoria e a atualização no uso das ferramentas existentes.

   Para atender às expectativas da administração existe uma estrutura estabelecida de acompanhamento dos trabalhos. Esta estrutura compreende um plano de trabalho semestral elaborado pela Auditoria e aprovado pela administração da organização. A cada três meses se reúne um grupo de alto nível, composto pelo Presidente da Instituição, os Vice-Presidentes e o Diretor de Auditoria para discutir os resultados dos trabalhos efetuados no período anterior. Este grupo, chamado Comissão de Auditoria, também eventualmente propõe mudanças de enfoque nos trabalhos em andamento ou nas próximas atividades.

   Além do planejamento semestral, os executivos de maior nível da organização (Vice-Presidentes e Diretores Executivos) têm autonomia para solicitar atuação da auditoria em alguma situação específica ou para validação de algum produto que esteja sendo lançado.

   Um outro cuidado para assegurar que os trabalhos da Auditoria estão atendendo expectativas da administração, é que os relatórios prestando contas destes trabalhos são submetidos à Diretoria responsável pela área que sofreu o exame. Estes relatórios indicam as deficiências e recomendações de melhoria formuladas pela Auditoria e os comentários dos responsáveis pelos processos examinados. Caso haja algum desacordo entre proposições dos auditores e posição do pessoal que sofreu a auditoria, o assunto é discutido em nível de diretoria. Se mesmo assim persistir a pendência, o tema é submetido à apreciação da Comissão de Auditoria.

Quanto ao aspecto atualização da auditoria, existe um programa contínuo de treinamento e reciclagem do pessoal. No caso específico da Auditoria na Internet, além deste programa comum a todos auditores, existe a preocupação permanente de atualização no uso de ferramentas. Para atender esta preocupação, são feitos cursos específicos na área e acompanhamento contínuo da rede, em busca de novidades. Este monitoramento foca principalmente "sites" especializados em segurança. Como exemplo desses "sites" pode-se destacar os já citados no corpo deste trabalho (ISACA, CERT, "sites" de fabricantes, etc.). Além deste trabalho de pesquisa, esporadicamente continuam sendo desenvolvidos trabalhos em parceria com instituições especializadas em segurança no ambiente Internet. Uma outra forma de atualização que merece ser destacada é o trabalho de acompanhamento e discussão com integrantes de outras organizações financeiras, feito através da participação em fóruns específicos sobre o assunto, existentes na Febraban.

10. Quais os aspectos positivos e negativos para a organização decorrentes da implantação da auditoria de informática na prática do comércio eletrônico através da rede?

O principal aspecto positivo que a implantação da auditoria no ambiente para prática comércio eletrônico através da Internet trouxe à organização foi trazer à sua Administração uma informação independente acerca dos riscos e dos controles existentes para atuação neste ambiente.

Um outro benefício que se pode destacar com a participação da auditoria no ambiente Internet foi que esta atividade talvez tenha feito ver à Administração a importância de uma política global de segurança de informações, precipitando assim seu desenvolvimento e implantação.

Um aspecto negativo que pode ser ressaltado é que a implantação da área foi relativamente morosa, em função da alternativa usada para sua criação: formação e desenvolvimento de pessoal interno. Quando se opta por desenvolver capacitação interna, paralelamente ao benefício do pessoal já conhecer a cultura da empresa, se paga o preço associado à lentidão na apresentação dos primeiros resultados. Deve-se salientar que o tempo para geração de resultados no Banco "A" não foi muito grande (foi inferior a um ano), o que atenua o aspecto negativo apontado.

Considerando-se os aspectos positivos e negativos associados à implantação da auditoria no ambiente para prática do comércio eletrônico através da Internet pode-se avaliar o resultado como plenamente satisfatório.

Capítulo 8

CONCLUSÃO

8.1 Critérios que suscitaram e orientaram a pesquisa

Uma pesquisa normalmente nasce da inquietação do pesquisador com relação a algum assunto específico. No caso particular deste trabalho a situação não foi diferente. O advento da Internet, com os benefícios e riscos a ela associados, ao mesmo tempo que desafia as organizações a operar utilizando os novos recursos disponíveis, as constrange. Este constrangimento decorre de novas ameaças que surgiram e da transformação de riscos que existiam antes mas que assumiram um potencial destrutivo maior em razão da mudança de escala das operações. Neste contexto, cabe à auditoria fornecer à administração da organização, de maneira isenta e fundamentada, subsídios que lhe permitam operar na rede mundial correndo um nível de risco conhecido e aceito.

A atuação na Internet gera simultaneamente desafio e sensação de insegurança em qualquer tipo de atividade econômica. Esta sensação é particularmente verdadeira em uma instituição financeira, onde parte substancial dos ativos é intangível, controlado apenas por processamento eletrônico. No momento que passa a atuar na Internet, a fronteira entre o ambiente de processamento interno e externo da organização torna-se mais tênue, aumentando o risco de ocorrerem violações que podem inclusive ameaçar sua sobrevivência.

A partir das inquietações descritas acima formulou-se a proposta inicial deste trabalho, que foi buscar resposta às questões:

1. O que é a Internet?
2. Quais os riscos que a organização se expõe ao atuar na Internet e quais os mecanismos que podem mitigar estes riscos?
3. O que é auditoria e como ela contribui para a administração de uma organização?
4. Como é a atuação da auditoria de informática em uma organização onde se pratica o comércio eletrônico através da Internet?
5. Como uma organização desenvolve habilidade para efetuar auditoria em ambiente onde se pratica o comércio eletrônico através da Internet?
6. Quais são as competências exigidas do auditor para atuar neste novo ambiente?

Definidas estas questões iniciais, o trabalho do pesquisador orientou-se na busca de suas respostas. Um fator limitador nesta busca foi a baixa disponibilidade de material para consulta tratando especificamente auditoria em ambiente Internet. Para contornar esta limitação, procurou-se obter uma visão geral sobre o ambiente externo e interno das organizações e sobre aspectos técnicos ligados à segurança na Internet e à auditoria, para posteriormente unir estes conceitos tratando auditoria em ambiente Internet. O resultado desta busca é apresentado nos Capítulo 2 a 5.

Esta forma de apresentação foi escolhida porque, baseando-se na literatura pesquisada, concluiu-se que a auditoria no comércio eletrônico praticado através da Internet é influenciada por fatores ligados ao ambiente externo, ao ambiente organizacional, ao ambiente tecnológico e ao ambiente de auditoria.

Uma vez estabelecida a fundamentação teórica, procurou-se confrontá-la com um caso prático, observado pelo pesquisador, mas no qual este não participou diretamente. Este caso, descrito no Capítulo 7, envolveu a implantação de um grupo de auditoria especializado em validar controles sobre operações comerciais praticadas através da Internet em uma Instituição Financeira.

8.2 Considerações sobre o resultado da pesquisa

Com a pesquisa foi possível obter-se respostas às questões inicialmente formuladas. No Quadro 8.1 está indicado onde pode-se buscar resposta a cada uma destas questões.

Quadro 8.1 - Relacionamento entre questões da pesquisa e respostas obtidas

Questão	Local da Resposta
1. O que é a Internet?	Seção 2.3
2. Quais os riscos que a organização se expõe ao atuar na Internet e quais os mecanismos que podem mitigar estes riscos?	Seção 2.4 e Capítulo 3
3. O que é auditoria e como ela contribui para a administração de uma organização?	Capítulo 4
4. Como é a atuação da auditoria de informática em uma organização onde se pratica o comércio eletrônico através da Internet?	Capítulos 5 e 7
5. Como uma organização desenvolve habilidade para efetuar auditoria em ambiente onde se pratica o comércio eletrônico através da Internet?	Capítulo 7
6. Quais são as competências exigidas do auditor para atuar neste novo ambiente?	Capítulo 7

Com base nas respostas obtidas na pesquisa, foi possível chegar às seguintes conclusões:

- a prática do comércio eletrônico através da Internet, apesar de trazer riscos, é perfeitamente viável. Embora este ambiente seja, por princípio, inseguro, existem mecanismos que permitem modificar esta característica básica e fornecer uma razoável segurança para as operações. Cabe à administração das organizações, com base no valor das informações que deseja proteger, definir qual configuração de segurança mais se enquadra às suas necessidades

- a auditoria de informática pode assessorar a administração fornecendo informes isentos e fundamentados sobre riscos e controles, que subsidiem o julgamento da adequação da proteção das informações
- para que auditoria de informática assessore eficientemente a administração, ao atuar em uma organização que pratique o comércio eletrônico através da Internet, os trabalhos da auditoria devem também contemplar avaliação da sensibilidade das informações que trafegarão (ou que estarão disponíveis) neste ambiente, bem como dos riscos que as ameaçam e dos controles para mitigar estes riscos
- a habilidade para execução de avaliação do ambiente Internet pode ser desenvolvida pela organização fornecendo-se formação teórica e prática nas técnicas utilizadas neste meio a profissionais que já detenham conhecimento do ambiente organizacional e de auditoria
- a atuação na Internet requer que o auditor conheça o ambiente organizacional, domine práticas de auditoria e tenha familiaridade com os recursos técnicos que dão sustentação à operação através da rede
- os fatores identificados na fundamentação teórica como influenciando a atuação da auditoria na Internet exercem de fato esta influência. No caso prático estudado, a condução da auditoria no ambiente onde se pratica o comércio eletrônico através da Internet é afetada, em ordem de influência, pelo ambiente de auditoria, pelo ambiente técnico, pelo ambiente organizacional, e pelo ambiente externo
- os aspectos apontados na fundamentação teórica como necessários a uma adequada avaliação do ambiente Internet têm de fato esta importância quando confrontados com o caso estudado. Dentre estes aspectos merece destaque especial a necessidade de uma política global de segurança para a organização

8.3 Limitações do trabalho

As limitações desse trabalho podem ter sido muitas, visto que o território é muito complexo e pouco explorado. Uma limitação que merece destaque especial é o fato de ter sido conduzido um estudo de caso único, no qual as entrevistas efetuadas envolveram apenas os profissionais da auditoria. Para atenuar o viés de concentração das entrevistas apenas com o pessoal diretamente envolvido no processo estudado, utilizou-se também como fonte de evidências a observação pessoal e o exame de relatórios de auditoria e de suas respostas. O uso do caso único inviabiliza uma generalização estatística das conclusões.

Apesar das limitações, acredita-se que o objetivo inicial do trabalho, que era fornecer um panorama associando comércio eletrônico através da Internet e atuação da auditoria de informática, foi atendido.

8.4 Recomendações para futuros estudos sobre o assunto

No sentido de dar continuidade ao trabalho que iniciamos, nossas recomendações são:

- Elaboração de novos estudos, abordando com maior profundidade o assunto e expandindo as entrevistas para o pessoal externo à auditoria;
- Desenvolvimento de estudos de casos enfocando atuação da auditoria no comércio eletrônico através da Internet em diferentes ramos de atividade;
- Realização de estudos visando criar cursos acadêmicos multi-disciplinares de formação em informática e em auditoria, para preparar profissionais que exerçam estas funções nas organizações.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, Alberto Luiz. Comércio Eletrônico : modelo, aspectos e contribuições de sua aplicação. São Paulo : Editora Atlas, 1999

ALBERTIN, Alberto Luiz. Comércio Eletrônico : um estudo no setor bancário. Tese de doutorado, Faculdade de Economia, Administração e Contabilidade da USP : Departamento de Administração, São Paulo, 1997

APPLEGATE, Lynda M. McFARLAN, F. Warren e McKENNEY, James L. Corporate information systems management : text and cases. 4rd Edition : Irwin, 1995

ATTIE, William. Auditoria : conceitos e aplicações. São Paulo : Editora Atlas, 1983

BASTOS, Lília da Rocha, PAIXÃO, Lyra, FERNANDES, Lucia Monteiro, DELUIZ, Neise. Manual para a elaboração de projetos e relatórios de pesquisa, teses, dissertações e Monografias. 4ª ed. Rio de Janeiro: LTC Livros Técnicos e Científicos Editora S.A., 1995

BOYNTON, William C., KELL, Walter G. Modern Auditing. 6th edition: John Wiley & Sons, Inc., 1996

COBIT - Governance, Control and Audit for Information and Related Technology - Framework : Information Systems Audit and Control Foundation, April 1998 - 2nd Edition

COSO - Committee of Sponsoring Organizations of the Treadway Commission - Internal Control - Integrated Framework, July 1994 Edition

DAVIDOW, William H., MALONE, Michael S., A corporação virtual : estruturação e revitalização da corporação para o século 21. São Paulo: Livraria Pioneira Editora, 1993 ; tradução de Nivaldo Montingelli Jr. do original The virtual corporation : structuring and revitalizing the corporation for the 21st century, publicado pela Harper Collins Publishers, Inc., 1992

FAJARDO, Karine. "Como funciona o padrão SET". Internet World, nº 35, pp 40-43, Jul 98

FLUSS, D., HARRIS, K. E-Business Glossary for Customer Service: Version 1.0, November 23, 1999 - Gartner Advisory : Commentary

GARFINKEL, Simson, SPAFFORD, Gene - Web security & commerce : risks, technologies, and strategies. First Edition : O'REILLY, June 1997

GIL, Antonio de Loureiro. Auditoria de Computadores. 4. ed. - São Paulo : Atlas, 1999

GUTTMAN, Barbara, BAGWILL, Robert. Internet Security Policy: A Technical Guide. July 31, 1997. Disponível no site do National Institute of Standards and Technology (http://csrc.nist.gov/isptg/html).

HALLAWELL, A. – Information security strategies (ISS) Research Note : Tutorials Gartner Group : February 9, 1998

IVES, B. et al., "A Framework for Research in Computer_Based Management Information Systems", Management Science, September 1980, pp. 910-934

KOTLER, Philip, Administração de marketing : análise, planejamento, e controle; tradução Ailton Bonfim Brandão, 4th ed. São Paulo : Atlas, 1994

LAUDON, Kenneth C., LAUDON, Jane Price, Management Information Systems : organization and technology, 4th ed. New Jersey : Prentice-Hall Inc., 1996

LOPES, Mikhail. "Sucesso.com". Exame, ano 33, nº 15, pp 64-78, 28/julho, 1999

LOPES, Mikhail. Quer ser a mosca ou a aranha? Exame, ano 32, nº 17, pp 90-94, agosto, 1998

LYNCH, Daniel C., LUNDQUIST, Leslie . Dinheiro Digital: o comércio na Internet. Rio de Janeiro: Campus, 1996; Tradução de: Digital money

MARTINS, Gilberto de Andrade. Manual para elaboração de monografias e dissertações. São Paulo: Atlas, 1994, 2ª Edição

MEHTA, Raj. Secure E-Business. Information Systems Control Journal, Volume I, 2000

MONTEIRO, Gilson. Guia para a elaboração de projetos, trabalhos de conclusão de cursos (TCCs), dissertações e teses. São Paulo : EDICON, 1998

Normas Internacionais de Auditoria, 1997 - São Paulo: IBRACON, 1998. Tradução: Vera Maria Conti Nogueira e Danilo A. Nogueira

PAULA, Maria Goreth Miranda Almeida. Auditoria interna : embasamento conceitual e suporte tecnológico. São Paulo : Atlas, 1999

PINDYCK , Robert S., RUBINFELD, Daniel, L., Microeconomia. São Paulo : Makron Books, 1994 ; tradução Pedro Catunda de original Microeconomia, Second Edition ; revisão técnica Roberto Luis Troster

Procedimentos de Auditoria Informática, 1993 - São Paulo : Instituto dos Auditores Internos do Brasil

SANTOS, Ana Maria Medeiros M., GIMENEZ, Luiz Carlos Perez (1998). O comércio eletrônico através da Internet. (Disponível no site do BNDES - www.bndes.gov.br - Gerência Setorial da Indústria Automobilistica, Comércio e Serviços)

SANTOS, Richard A. Internet Security. Information Systems Audit & Control Journal, Volume I, 1999 - reprinted from PC Magazine, February 4, 1997

TANENBAUM, Andrew S., Modern Operating Systems. New Jersey : Prentice-Hall, Inc., 1992

TAPSCOTT, Don, CASTON, Art. *Paradigm shift : the new promise of information technology.* Baskerville: McGraw-Hill, 1993

TAPSCOTT, Don. *The digital economy : promise and peril in the age of networked intelligence.* New York: McGraw-Hill, 1995

VIDAL, Antonio Geraldo da Rocha. A influência de fatores ambientais no desenvolvimento de aplicações pelo usuário. Tese de doutorado, Faculdade de Economia, Administração e Contabilidade da USP : Departamento de Administração : USP, São Paulo, 1996

YIN, Robert K. Case Study Research Design and Methods. California : Sage Publications, Inc., 1989

ZBORAY, M. Secure commerce over the Web, April 08, 1998 - InSide Gartner Group (IGG): Research Products

BIBLIOGRAFIA COMPLEMENTAR

- ANONYMOUS - Maximum security : a hacker's guide to protecting your internet site and network. First Edition : Suns.net, 1997

APÊNDICE 1

EXEMPLOS DE ALGORITMOS DE CRIPTOGRAFIA

1. *Algorítmos de chaves simétricas*

- **DES** - o Data Encryption Standard foi adotado como padrão pelo governo americano em 1997; usa um bloco com tamanho de 56 bits e tem vários modos de operação dependendo do propósito que é empregado
- **DESX** - é um algorítmo derivado do DES, com modificações que incrementam sua segurança
- **Triple-DES** - utiliza três vezes codificação DES com três chaves diferentes, também para aumentar sua segurança
- **Blowfish** - chave inventada por Bruce Schneier, mas de domínio público, permite chaves de tamanho variável de até 448 bits
- **IDEA** - o International Data Encryption Algorithm foi desenvolvido por James L. Massey e Xuejia Lai e divulgado em 1990; usa uma chave de 128 bits e é usado pelo programa PGP (Pretty Good Privacy) para codificar mensagens do correio eletrônico
- **RC2** - desenvolvido por Ronald Rivest e mantido secreto pela RSA Data Security até 1996 quando foi divulgado de maneira anônima; utiliza chaves de 1 a 2048 bits
- **RC4** - desenvolvido por Ronald Rivest e mantido secreto pela RSA Data Security até 1994 quando foi também divulgado de maneira anônima; assim como o RC2, também utiliza chaves de 1 a 2048 bits
- **RC5** - desenvolvido por Ronald Rives e divulgado em 1994; permite que o usuário defina o tamanho da chave, tamanho do bloco e número de embaralhamentos

2. *Algorítmos de chaves públicas*

- **RSA** - sistema desenvolvido por três professores do MIT - Massachusetts Institute of Technology (Ronald Rivest, Adi Shamir e Leonard Adleman) usado tanto para codificar informações como base de um sistema de assinatura eletrônica (a assinatura eletrônica pode ser usada para comprovar a autoria e autenticidade de uma informação digital); a chave pode ser de qualquer tamanho, dependendo da implementação usada
- **DSS** - o Digital Signature Standard foi desenvolvido pela National Security Agency (NSS) e adotado como um Federal Information Processing Standard (FIPS) pelo National Institute for Standards and Technology (NIST). Baseia-se no algorítmo de assinatura digital (DSA - Digital Signature Algorithm); usa chaves entre 512 e 1024 bits

- **Diffie-Hellman** - é um sistema para troca de chaves criptográfica entre pares, não sendo propriamente um método de codificação e decodificação. Consiste em um esquema de desenvolvimento e troca de chaves privadas realizado através de um canal público de comunicação. Nele os pares entram em acordo sobre valores numéricos comuns e cada par cria uma chave. Transformações matemáticas da chaves são trocadas e cada par então calcula uma terceira chave que não possa ser facilmente deduzida por um terceiro que conheça apenas os valores trocados

3. ***Funções de resumo de mensagens***

- **HMAC** - o Hashed Message Authentication Code é uma técnica que usa uma chave secreta e uma função resumo para criar um código secreto
- **MD2** - Message Digest nº 2, desenvolvido por Ronald Rivest; é a mais segura das que ele criou, mas tem processamento muito lento; produz um código de 128 bits.
- **MD4** - foi desenvolvido por Ronald Rivest para ser uma alternativa menos custosa que o MD2, mas tem como fato negativo também ser menos segura; também gera códigos de 128 bits
- **MD5** - também criado por Ronald Rivest e gerando código de 128 bits; é melhor que o MD4, mas não tem demonstrado confiabilidade, razão pela qual não vem sendo muito utilizado
- **SHA** - o Secure Hash Algorithm foi desenvolvido pelo NSA para ser usado como padrão de assinatura digital pelo Instituto Nacional de Padrões e Tecnologia (NIST's DSS); produz um código de 160 bits, mas, de acordo com o NIST precisa de um pequeno ajuste para poder funcionar
- **SHA-1** - é o Secure Hash Algorithm revisado; produz código com 160 bits.

Fonte: Garfinkel e Spafford (1997)

APÊNDICE 2

EXEMPLOS DE PROGRAMAS DE CRIPTOGRAFIA

1. PGP

O "Pretty Good Privacy" é um programa desenvolvido por Phil Zimmermann e divulgado em 1991 para permitir criptografia de arquivos e de mensagens de correio eletrônico. Compreende também um conjunto de padrões que descrevem formatos para mensagens codificadas, chaves e assinaturas digitais. Utiliza a chave pública RSA para codificar o gerenciamento da chave e o padrão simétrico IDEA para codificar os dados da mensagem.

2. S/MIME

O Secure/Multipurpose Internet Mail Extension é um padrão para envio de arquivos com textos binários anexados, que tornam o conjunto codificado. Foi desenvolvido pela RSA Data Security e pode ser adicionado ao sistema originalmente existente para envio de mensagens.

3. SSL

O Secure Socket Layer é um protocolo genérico utilizado para propiciar segurança na comunicação entre dois pontos. Embora normalmente utilizado com os browsers Internet Explorer (da Microsoft) e Netscape Navigator, pode ser usado em qualquer serviço baseado no protocolo TCP/IP, como:

- FTP (File Transfer Protocol), para transferência de arquivos
- NNTP (Network News Transfer Protocol), para busca de notícias armazenadas em um banco de dados centralizado
- Telnet, para conexão e execução de comandos em um computador, a partir de um terminal remoto

Os benefícios oferecidos pelo SSL compreendem confidencialidade (através do uso de algoritmos de criptografia especificados pelos usuários), integridade (através do uso de funções de embaralhamento de mensagens, também definidas pelos usuários), autenticação (através do uso de certificados de chaves públicas) e não-repúdio (com o uso de mensagens assinadas de maneira criptográfica).

4. PCT

O Private Communications Technology é uma camada de segurança existente no protocolo de transporte de mensagem semelhante ao SSL. Foi desenvolvido pela Microsoft para corrigir falhas que existiam na versão 2.0 do SSL (que foram corrigidas na versão 3.0). Segundo Garfinkel e Spafford (1997) é utilizado por grandes clientes da Microsoft em redes corporativas ("Intranet").

5. S-HTTP

O Secure HyperText Transfer Protocol é um sistema para assinar e criptografar informações enviadas usando o protocolo HTTP da Web. Foi desenvolvido antes do SSL ser divulgado. É flexível quanto ao tipo de protocolo utilizado, aceitando isoladamente ou em conjunto algoritmos com chaves públicas e privadas ou resumo de mensagens. O protocolo a utilizar é definido na negociação entre o cliente e o servidor, baseado na configuração de cada um. Por exemplo, o servidor pode exigir do browser do cliente a função resumo de mensagem para garantir a integridade da transação alimentada. A menos que o browser do cliente esteja configurado para recusar tal exigência, a conexão será estabelecida.

6. SET

O Secure Electronic Transfer é um protocolo projetado para envio do número de cartão de crédito codificado através da Internet. Na seção 3.4.3 está descrito em maiores detalhes.

7. CyberCash

Este sistema, assim como o SET, também é um protocolo de pagamento eletrônico. Está baseado em tecnologia de chave pública que permite o uso de cartões de crédito convencionais através da rede. Antes de usar o produto o cliente deve baixar um aplicativo do site da CyberCash (www.cybercash.com) para criação de uma "carteira eletrônica" onde os registros de seu número de cartão de crédito (ou de outros meios de pagamento) serão mantidos.

8. DNSSEC

O padrão Domain Name System Security é um sistema projetado para trazer segurança ao nome do identificador do site na Internet, isto é, o DNS (Domain Name System). Este sistema cria uma infraestrutura de chave pública sobre o sistema DNS. Para cada domínio DNS é assinalada uma chave pública, tornando confiável a obtenção desta chave. Este sistema também permite atualização segura das informações armazenadas no servidor DNS, possibilitando sua administração de maneira remota.

9. IPsec e Ipv6

Estes sistemas foram desenvolvidos para permitir confidencialidade de ponta a ponta para os pacotes de informações em trânsito através da Internet. São utilizados em conjunto com outros protocolos para permitir a criação de redes privadas particulares através da Internet (VPN - Virtual Private Network).

10. Kerberos

Este é um sistema de segurança na rede desenvolvido pelo MIT que se baseia em chaves simétricas e secretas compartilhadas entre o servidor Kerberos e cada usuário individual. Cada usuário tem sua própria senha e o servidor usa esta senha para codificar a mensagem enviada para aquele usuário de forma que apenas ele possa lê-la.

11. SSH

O Secure Shell fornece proteção criptográfica a terminais virtuais (Telnet) e a operações de transferência de arquivos. Foi desenvolvido pela RSA Data Security e pode ser adicionado ao sistema originalmente existente para envio de mensagens.

Fonte: Garfinkel e Spafford (1997)

APÊNDICE 3

RECOMENDAÇÕES DAS NORMAS INTERNACIONAIS DE AUDITORIA PARA ATUAÇÃO EM AMBIENTES COMPUTADORIZADOS

As Normas Internacionais de Auditoria (1997) recomendam que o auditor independente, ao atuar em empresas onde existam Sistemas de Informação Computadorizados ("SIC"), considere detalhadamente esta situação na definição da extensão e no tipo dos exames que serão conduzidos. A norma que trata deste assunto (Norma 401 - Auditoria em um ambiente de sistemas de informação computadorizados) especifica que o objetivo e o alcance de uma auditoria não mudam em um ambiente de SIC. Todavia, como o controle interno pode ser afetado pelo uso do computador, o uso de SIC pode implicar em:

- alteração nos procedimentos do auditor para obtenção do entendimento sobre o sistema de controle interno
- tratamento diferenciado na consideração dos riscos inerentes e de controle, para avaliar o risco de auditoria
- realização, por parte do auditor, de testes específicos para atingir o objetivo de auditoria.

A Norma 401 estabelece ainda que, ao conduzir trabalhos em um ambiente de SIC, o auditor deve considerar a colaboração de pessoal especializado (que componha a equipe do trabalho ou que preste serviço eventual a esta equipe) para:

- obter entendimento suficiente dos sistemas contábeis e de controle interno afetados pelo ambiente de SIC
- determinar o efeito do ambiente de SIC sobre a avaliação de risco global e de risco em nível de saldo de uma conta ou classe de transações
- projetar e executar testes apropriados de procedimentos de comprovação e de controle.

O Pronunciamento Internacional de Auditoria nº 1008 - Avaliações de Risco e Controle Interno - Características e Considerações do Sistema de Informações Computadorizados, anexo às Normas Internacionais de Auditoria (1997) descreve os aspectos que devem ser considerados em ambientes que utilizam tecnologia de informações. Esta descrição aborda os principais riscos inerentes a este ambiente e os controles que devem existir.

A avaliação dos riscos envolve:

- **Avaliação da estrutura organizacional**

  A avaliação da estrutura compreende os seguintes aspectos:

- **Concentração de funções e conhecimento** - geralmente o número de pessoas envolvidas no processamento de informações é reduzido, podendo comprometer a segregação de funções e podendo fazer com que o conhecimento esteja concentrado em poucas pessoas-chave, gerando dependência destas pessoas
- **Concentração de programas e dados** - os programas e arquivos de dados podem estar concentrados em um único local, o que os expõe, na ausência de controles apropriados, a maior probabilidade de sofrerem acessos não autorizados

- **Avaliação da natureza do processamento**

  A utilização de computadores pode implicar em evidências menos visíveis e aumentar o número de pessoas que podem ter acesso às informações. Os aspectos de controle associados a este tópico envolvem:

  - **Ausência de documentos de entrada** - os dados podem ser incluídos diretamente nos sistemas, sem documentação suporte; em outros casos a evidência da aprovação pode estar baseada unicamente em autorizações eletrônicas
  - **Ausência de trilha visível de transação** - em sistemas computadorizados perde-se o vínculo com o documentos físicos (como o que originou a transação, livros contábeis, etc.), porque tais informações são mantidas em arquivos magnéticos. Além disso, a retenção destes arquivos (prazo que as informações podem ser recuperadas a partir do arquivo magnético) é limitada, podendo inviabilizar seu rastreamento
  - **Ausência de saída visível** - os resultados do processamento podem estar exclusivamente em meio magnético, dificultando, ou até mesmo inviabilizando, sua recuperação
  - **Facilidade de acesso a dados e programas de computador** - o acesso a estes dados pode ser feito a partir de terminais fora do ambiente físico da organização. Portanto, caso não existam controles adequados, o risco potencial de acesso não autorizado por pessoas internas ou externas à organização sofre aumento

- **Avaliação de procedimentos e projetos**

  O desenvolvimento de sistemas computadorizados normalmente difere dos projetos de sistemas manuais. Os aspectos a destacar neste tópico envolvem:

  - **Consistência de desempenho** - os SIC executam exatamente aquilo para o que foram preparados. Isto significa que, se por um lado são de maior confiabilidade que os sistemas manuais (por executarem exatamente as mesmas verificações, sem se deixarem influenciar por nenhum viés que não tenha sido estabelecido inicialmente), por outro lado têm um potencial de estrago maior (pois os erros eventualmente existentes se estenderão a todos os dados que passem pelo mesmo tratamento)
  - **Procedimentos de controle programados** - os dados são passíveis de validações inseridas nos programas, como geração de relatórios de exceção

e testes de razoabilidade, que destaquem dados que fujam a uma variação considerada aceitável

- **Atualização única de arquivos** - uma entrada única em um sistema pode gerar atualização em outros arquivos de outros sistemas nos quais aquela informação incluída seja relevante. Por exemplo, uma venda gera um valor a receber, uma baixa no estoque e, eventualmente, um pedido ao fornecedor. Da mesma forma que na consistência de desempenho, paralelamente ao benefício de se manter todas informações coerentes, tem-se o risco de eventuais erros trazerem desdobramentos para toda a empresa
- **Transações geradas por sistemas** - certas transações podem ser geradas automaticamente pelo sistema quando ocorrer um determinado evento (como a geração do pedido, dada como exemplo no tópico anterior). A exemplo dos aspectos citados anteriormente esta característica pode ser positiva ou negativa para a empresa
- **Vulnerabilidade dos meios de armazenamento de dados e programas** - os meios de armazenamento das informações (discos, cartuchos, CDs, etc.) são vulneráveis a roubo, perda ou destruição acidentalmente ou não.

Os controles que o Pronunciamento Internacional de Auditoria nº 1008 descreve para mitigar os riscos apresentados acima combinam procedimentos manuais e computadorizados. Envolvem controles gerais de SIC e controles específicos sobre aplicativos que geram informações contábeis, conforme descrito a seguir:

- **Controles Gerais de SIC**

  Têm por objetivo permitir um nível razoável de segurança que os controles gerais estão atuando para proporcionar um controle interno eficiente. Podem incluir:

  - **Controles organizacionais e administrativos** - definidos para estabelecer uma estrutura organizacional para as atividades de SIC. Compreendem políticas e procedimentos relacionados com funções de controle e segregação apropriada de funções incompatíveis (por exemplo, preparação e inclusão de dados em ambiente de produção realizadas pelo pessoal ligado ao desenvolvimento ou à operação do sistema)
  - **Controles de manutenção e desenvolvimento de sistemas aplicativos** - definidos para permitir uma razoável segurança que os sistemas são desenvolvidos e mantidos de maneira autorizada e eficiente. Normalmente também são definidos para estabelecer controles sobre:
    - teste, conversão, implantação e documentação de sistemas novos ou revisados
    - alterações nos sistemas aplicativos
    - acesso a documentação de sistemas
    - aquisição de sistemas aplicativos de terceiros
  - **Controles de operação de computadores** - buscam controlar a operação visando trazer razoável segurança que:
    - os sistemas foram usados somente para fins autorizados
    - o acesso à operação é restrito ao pessoal autorizado

- somente são usados programas autorizados
- erros de processamento são detectados e corrigidos

- **Controles de sistemas** - definidos para permitir segurança razoável que os sistemas foram desenvolvidos ou adquiridos de forma autorizada e eficiente, incluindo:
  - autorização, aprovação, teste, implantação e documentação de novos sistemas ou manutenções nos existentes
  - acesso à documentação e ao sistema restrito ao pessoal autorizado
- **Controles de programas e entrada de dados** - buscam fornecer razoável segurança que:
  - existe uma estrutura de autorização de acesso às transações
  - o acesso a dados e programas é restrito ao pessoal autorizado
- **Salvaguardas para permitir a continuidade do processamento** - incluem:
  - back up de dados e programas em ambiente externo ao local do processamento principal
  - procedimentos de recuperação para uso em caso de roubo, perda ou destruição acidental intencional
  - procedimentos para processamento em local alternativo, no caso de sinistro

- **Controles de aplicativos de SIC**

  Compreendem procedimentos de controle específicos sobre os aplicativos contábeis visando fornecer razoável segurança que todas transações foram autorizadas e registradas e que seu processamento ocorreu de maneira completa, precisa e oportuna. Incluem:

  - **Controles sobre entrada** - buscam garantir razoável segurança que:
    - as transações foram apropriadamente autorizadas antes de serem processadas
    - as transações foram convertidas com exatidão para a linguagem utilizada pelo computador e registradas em seus arquivos
    - as transações não foram perdidas, adicionadas, duplicadas ou indevidamente alteradas
    - as transações incorretas foram rejeitadas, corrigidas e, se aplicável, reincluídas oportunamente
  - **Controles sobre arquivos de dados e processamento** - visam garantir razoável segurança que:
    - as transações (inclusive as geradas pelo sistema) foram adequadamente processadas
    - as transações não foram perdidas, duplicadas ou alteradas indevidamente
    - os erros de processamento foram identificados e corrigidos oportunamente
  - **Controles de saída** - buscam trazer razoável segurança de que:
    - os resultados de processamento são precisos

- o acesso aos dados fornecidos é restrito ao pessoal autorizado
- a saída é fornecida ao pessoal autorizado em tempo oportuno

Fonte: Normas Internacionais de Auditoria (1997)

APÊNDICE 4

DETALHAMENTO DOS PROCESSOS DE TECNOLOGIA DE INFORMAÇÕES E OBJETIVOS DE CONTROLE QUE SE BUSCA ATINGIR

A estrutura COBIT (1998) considera que processos de tecnologia de informações são um conjunto de atividades relacionadas. Na execução destas atividades se busca atingir objetivos de controle para assim assegurar-se que os objetivos do negócio também estejam sendo atingidos.

Os processos de T.I. e objetivos de controle correspondentes para cada conjunto de atividades de natureza semelhante são os seguintes:

PLANEJAMENTO E ORGANIZAÇÃO

- **definição do plano estratégico de tecnologia de informações (T.I.)**

  Para permitir balanceamento entre as soluções de T.I. e as exigências do negócio. Compreende o processo de planejamento estratégico, realizado regularmente, que forneça os planos de longo prazo, e traduza estes planos de longo prazo em planos operacionais, com metas claras e concretas de curto prazo

- **definição da arquitetura de informações**

  Que melhor organize os sistemas de informações. Envolve a criação e manutenção de um modelo de informações do negócio e sistemas apropriados para otimizar o uso desta informação

- **determinação da direção tecnológica**

  Para se aproveitar das tecnologias emergentes disponíveis, através da criação e manutenção de um plano traçando a infraestrutura tecnológica

- **definição do relacionamento e organização de T.I**

  Para tornar disponíveis os seus serviços. É obtido através da organização apropriada onde os papeis e responsabilidades sejam definidos e divulgados

- **gerenciamento dos investimentos de T.I.**

  Para assegurar e controlar a distribuição dos recursos financeiros. Compreende um orçamento operacional e de investimentos estabelecidos e aprovados pelo negócio

- **comunicação dos alvos e instruções da administração**

  Assegurando-se que estas sejam conhecidas e entendidas. Obtêm-se através de políticas estabelecidas e divulgadas aos usuários; além disso, os padrões

necessitam ser estabelecidos para traduzir as opções estratégicas em regras práticas e utilizáveis

- **gerenciamento dos recursos humanos**

  Para ampliar ao máximo a contribuição das pessoas ao processo de T.I. É obtido através de processos sólidos de gerenciamento de pessoal.

- **assegurar conformidade a exigências externas**

  Para atender obrigações legais, e contratuais. Seu atendimento é feito identificando-se e analisando-se o impacto das exigências externas em T.I. e adotando-se medidas apropriadas para se conformar a tais exigências

- **avaliação de riscos**

  Para assegurar-se que os objetivos de T.I. estão sendo alcançados e reagir contra ameaças ao fornecimento destes serviços. Para atingir este objetivo a organização deve engajar-se em um processo de identificação dos riscos de T.I., análise dos impactos trazidos por eles e tomando providência para mitigar estes riscos. Na adoção destas providências, não se deve perder o foco da avaliação se o custo do controle compensa o benefício que ele proporciona

- **gerenciamento dos projetos**

  Para definir prioridades e entregar estes projetos no prazo estimado. Este objetivo é atendido através da identificação e atribuição de prioridades dos projetos organizacionais de maneira compatível ao plano operacional. Além disso, a entidade deve adotar e aplicar sólidas técnicas de gerenciamento de projeto para cada projeto sob avaliação

- **gerenciamento da qualidade**

  Para atender as exigências dos clientes de T.I. O atendimento a este objetivo se faz através do planejamento, implementação e manutenção pela organização de padrões e sistemas de gerenciamento de qualidade.

AQUISIÇÃO E IMPLEMENTAÇÃO

- **identificação das soluções**

  Que assegurem a melhor estratégia para atender as exigências do negócio. É obtida através de análise objetiva das diferentes oportunidades confrontadas com as exigências dos usuários

- **aquisição e manutenção do software aplicativo**

  Para fornecer funções automatizadas que atendam efetivamente o processo comercial. Este objetivo é alcançado através da definição de exigências funcionais e operacionais e implementação por etapas com validações claras efetuadas em cada etapa

- **aquisição e manutenção da estrutura tecnológica**

  Que forneça plataformas apropriadas às aplicações do negócio. Para atingir este objetivo é necessário que se avalie o desempenho do hardware e do software, o fornecimento de manutenção preventiva e a instalação, segurança e controle do sistema

- **desenvolvimento de procedimentos de T.I.**

  Para assegurar o uso apropriado das aplicações e soluções tecnológicas adotadas. Avalia-se o atendimento deste objetivo verificando-se o enfoque dado ao desenvolvimento de manuais de procedimentos operacionais, de usuários, e de materiais de treinamento

- **instalação e validação de sistemas**

  Para verificar e confirmar que as soluções estão adequadas aos propósitos pretendidos

- **gerenciamento de mudanças**

  Para diminuir a possibilidade de interrupções, alterações não autorizadas ou erros. É atendido com um sistema de gerenciamento que forneça informações para análise, implementação e acompanhamento de todas mudanças solicitadas e executadas na infraestrutura de T.I.

PRODUÇÃO E SUPORTE

- **definição do nível de serviços**

  Para estabelecer claro entendimento do nível de serviço requerido. É obtido com estabelecimento de acordos de nível de serviço que especifiquem o critério de desempenho para aferição da quantidade e qualidade do serviço

- **gerenciamento dos serviços de terceiros**

  Para assegurar que os papeis e responsabilidades de terceiros são claramente definidos e estão sendo atendidos. Este controle é executado através de revisões e acompanhamento dos contratos existentes, avaliando efetiva aderência às políticas organizacionais

- **gerenciamento da performance e capacidade**

  Para assegurar que a capacidade adequada está disponível e que o desempenho atende às exigências. Os controles para verificar este objetivo envolvem mecanismos de gerenciamento de capacidade e desempenho, que acumulem dados e relatem sobrecargas e sub-utilização do aplicativo e dos recursos de processamento

- **assegurar continuidade do serviço**

  Para tornar os serviços de T.I. disponíveis conforme as exigências e assegurar o menor impacto aos negócios no caso de interrupção. É obtido com a existência de um plano de continuidade de T.I. que seja testado e esteja compatível com o plano de continuidade dos negócios e as exigências comerciais associadas

- **assegurar segurança dos sistemas**

  Para salvaguardar as informações contra uso não autorizado, divulgação, modificação, dano ou perda. Consegue-se com controles de acesso lógico, que assegurem que o acesso ao sistema, dados e programas está restrito aos usuários autorizados

- **identificação e atribuição dos custos**

  Para assegurar uma adequada consciência dos custos atribuíveis aos serviços de T.I.. Alcança-se este objetivo com um sistema de contabilização do custo de T.I. que assegure que estes sejam registrados, calculados e alocados ao nível de detalhe exigido

- **formação e treinamento de usuários**

  Para assegurar que os usuários estão usando efetivamente a tecnologia e estão conscientes dos riscos e responsabilidades envolvidos. É obtido com um plano de treinamento e desenvolvimento abrangente

- **assistência e atendimento a clientes de T.I.**

  Para assegurar que qualquer problema vivido pelo usuário seja apropriadamente solucionado. A instalação de um "help-desk" para fornecimento de auxílio imediato aos usuários permite que este objetivo de controle seja atendido

- **gerenciamento de configurações**

  Para considerar todos componentes de T.I., evitar alterações não autorizadas, verificar existência física e fornecer uma base sólida para gerenciamento de mudanças. É conseguida através de controles que identifiquem e registrem todos os ativos de T.I. e sua localização física e um programa de verificação que confirme esta existência

- **gerenciamento de problemas e incidentes**

  Para assegurar que os problemas e incidentes sejam resolvidos e sua causa investigada para prevenir nova ocorrência. Este objetivo é atendido com um sistema de gerenciamento de problemas que registre e acompanhe todos incidentes

- **gerenciamento de dados**

  Para assegurar que os dados permanecem completos, íntegros e válidos durante sua entrada, tratamento e armazenamento. Uma combinação efetiva de

controles gerais e controles sobre a aplicação sobre as operações de T.I. permite atendimento deste objetivo

- **gerenciamento de instalações**

  Para fornecer uma proteção conveniente para os equipamentos e pessoal de T.I. contra perigos decorrentes de ações humanas ou da natureza. Consegue-se através da instalação de um ambiente adequado e controles físicos que sejam regularmente revisados

- **gerenciamento de operações**

  Para assegurar que funções importantes de apoio de T.I. estão sendo executadas regularmente e de forma metódica. É verificada através de um roteiro de atividades de apoio no qual esteja registrada a execução destas atividades.

MONITORAÇÃO

- **acompanhamento do processo**

  Para assegurar que os objetivos definidos para os processos de T.I. estejam sendo alcançados. Alcança-se com a definição de indicadores que sejam relevantes para a administração e implementação de sistemas para divulgação destes indicadores de forma regular

- **avaliação interna da adequação do controle**

  Para assegurar que os objetivos de controle interno para o processo de T.I. estão sendo atingidos. É obtido com o engajamento da administração no monitoramento do controle interno, avaliação de sua eficácia e divulgação desta avaliação em uma base regular

- **obtenção de garantia independente**

  Que aumente a confiança entre a organização, clientes e fornecedores. Este objetivo é atingindo com revisões independentes executadas a intervalos regulares.

- **submeter-se à auditoria independente**

  Para elevar o nível de confiança e beneficiar-se de recomendações para melhoria dos controles. Consegue-se com auditorias independentes executadas em intervalos regulares.

Fonte: COBIT (1998)