# O AUDITOR FACE AO COMÉRCIO ELETRÔNICO

*Fernando José de Araujo Silva*(*)

**RESUMO**

O comércio é uma atividade intrínseca à natureza humana. Vem evoluindo acompanhando a evolução do conhecimento humano desde o início dos tempos. Com o desenvolvimento técnico experimentado nos dias atuais, se vê o surgimento e evolução do comércio eletrônico. O potencial desta modalidade de operações é imenso, estimando-se que venha a movimentar, no ano de 2001, cerca de 2% do PIB mundial. Em oposição à oportunidade representada por este novo filão, existe a ameaça trazida pela insegurança associada à infra-estrutura que apoia o novo comércio. Neste contexto, coloca-se o auditor verificando se os controles existentes permitem que a empresa atue no comércio eletrônico com nível de segurança compatível ao grau de risco que os proprietários da empresa estão dispostos a assumir. Neste trabalho são apresentados conceitos gerais de "Comércio Eletrônico", procedimentos de segurança associados e se discute atuação do auditor neste novo ambiente.

(*) Mestrando pelo Programa de Pós-Graduação em Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo. Graduado em Ciências Contábeis e em Administração pela FEA/USP. E-mail: fernando.araujo@originet.com.br.

**Comércio, Desenvolvimento Tecnológico e Atuação do Auditor**

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-se das novas tecnologias que surgem.

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. Com isto, se vê surgir o comércio eletrônico, ou seja, a utilização de recursos da eletrônica (como computação e telecomunicações), para prática desta atividade humana.

Como este conceito é muito abrangente, pode-se restringi-lo considerando-se como *comércio eletrônico* exclusivamente as operações comerciais realizadas tendo como base a rede mundial de comunicações, isto é a Internet (*Inter*continental *net*works, segundo Albertin, 1997). Esta rede nasceu inicialmente com objetivos militares, expandiu-se para os meios acadêmicos e, finalmente, passou a ser utilizada pelo público, de maneira geral. Mesmo dentro deste conceito mais restrito, o volume financeiro que o comércio eletrônico deve movimentar é imenso. Matéria publicada na revista Byte, de março/1998, citando pesquisa da Activ-Media Inc. estima que 2% do PIB mundial, em 2001, deverá ser movimentado pela Internet. Isto significa que, no período de 1998 até 2001, serão negociados pela rede mundial cerca de US$ 1,8 trilhão. Outras estimativas são igualmente gigantescas, como a elaborada pela empresa de pesquisa Forrester Research, citada pela revista *Exame*, de 12.08.98. Ela prevê que, durante o ano de 1998 serão negociados pela rede, no mundo, 22 bilhões de dólares, volume que deverá atingir, em 2002, 349 bilhões.

Embora estes números sejam assustadores, não devem ser considerados como fantasiosos, quando se leva em consideração a velocidade de expansão da Internet. Santos e Gimenez (1998) apresentam diversos dados que dão conta da rápida evolução da rede. Como exemplo, pode-se destacar os seguintes:

> *Embora a Internet venha funcionando muito mais como um canal de mídia do que de vendas, 5% das 500 maiores empresas norte-americanas já fazem vendas através dela; ou seja, no mundo, as receitas geradas através de compra de produtos via Internet, segundo as fontes mais conservadoras, já atingem mais de US$ 500 milhões.*
> *Quanto ao número de usuários, estima-se que possam ser, atualmente, até 80 milhões de internautas e que pelo menos 15% deles façam compras pelo computador.*
> *Ressalte-se, ainda, que a Internet alcançou o ambicionado* status *de meio de comunicação de massa, em muito menos tempo que outras mídia* [Vide Tabela 1].

**Tabela 1**
**Mídias e Tempo Gasto para se Alcançar 50 Milhões de Habitantes**

| MÍDIA | ANO $ |
|---|---|
| Rádio | 38 |
| TV | 14 |
| TV a Cabo | 10 |
| Internet | 5 |

Fonte: Morgan Stanley Technology Research.

> *Além das empresas de todos os portes, o universo dos usuários é de pessoas predominantemente de elevado poder aquisitivo, com forte perfil de consumo, geralmente das classes A e B, com pelo menos um cartão de crédito*

Apesar de todo potencial representado por este universo que se abre frente às empresas com o comércio eletrônico, ele ainda padece de desconfiança tanto do ponto de vista da empresa quanto dos clientes. Esta desconfiança existe em dois 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 desta confraria, 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 indevido às informações que transitam na rede** – as informações ao transitarem na rede podem ser interceptadas e utilizadas de maneira indevida. Esta ameaça paira tanto sobre as empresas (de maneira geral, fornecedoras) como sobre os clientes, que podem ter, por exemplo, seu número de cartão de crédito detectado e utilizado de maneira indevida.

Zboray (1998) informa 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 operacionalização do serviço (arquivos e aplicativos internos).

Esta inquietação, que afeta os executivos da empresa de maneira geral, pode afligir em especial os auditores. Tais profissionais 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" (ATTIE, 1983, p. 53). Para cumprir esta missão, o auditor precisa assegurar-se que os controles existentes permitem que a empresa atue no comércio eletrônico com nível de segurança compatível ao grau de risco que o proprietário da empresa está disposto a assumir.

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 ocorrem aumenta a cada dia. Dentro deste contexto, o auditor precisa se capacitar para poder continuar cumprindo sua missão.

## A "Corporação Virtual"

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" (p. 27). Para que ocorra troca, ainda Kotler (1994, p. 27) define que 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 estudados pela microeconomia. Pindyck & Rubinfeld (1991) descrevem:

> *Microeconomia trata do comportamento das unidades econômicas individuais. Tais unidades incluem consumidores, trabalhadores, investidores, proprietários de terra, empresas - na realidade, quaisquer indivíduos ou entidades que desempenhem um papel no funcionamento de nossa economia. A microeconomia explica como e por que estas unidades tomam decisões econômicas. (p. 3).*
> *Podemos dividir as unidades econômicas individuais em dois grande grupos conforme sua função - compradores e vendedores. Os compradores 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). Entre os vendedores estão as empresas, que vendem bens e serviços; os trabalhadores, que vendem seus serviços por meio do trabalho; e os proprietários de recursos, que arrendam terras ou comercializam recursos minerais para as empresas. [...] Em conjunto, compradores e vendedores interagem, originando os mercados. Um mercado é um grupo de compradores e vendedores que interagem entre si, resultando na possibilidade de trocas. [...] Os mercados estão no centro da atividade econômica, e muitas das questões e temas mais interessantes na economia são relacionados com o modo de funcionamento dos mercados. Por exemplo, [...] por que será que os preços em alguns mercados têm subido ou caído rapidamente, enquanto, em outros os preços dificilmente sofrem alguma alteração? E quais serão os mercados que oferecem as melhores oportunidades para um empreendedor que esteja pensando em entrar no mundo dos negócios? (p.13)*

Com a evolução do conhecimento, o comércio procura se sofisticar cada vez mais, visando permitir que os consumidores sejam melhor atendidos, aumentando o retorno da empresa fornecedora e permitindo seu crescimento. Esta busca contínua da melhoria é o que Davidow & Malone (1992) chamam de serviço virtual:

> *O produto ou serviço virtual ideal é aquele que é produzido instantaneamente e sob medida, em resposta à demanda do cliente. Os produtos virtuais não só terão grande valor para os clientes mas também a capacidade para fazê-los irá determinar quais serão as corporações de sucesso no século 21. [...]... O desenvolvimento de um produto virtual exigirá que uma empresa revise a si mesma totalmente, controle tipos cada vez mais sofisticados de informações e domine todas as novas práticas organizacionais e de produção. Isso irá mudar de forma tão completa a maioria das empresas contemporâneas, que aquilo que emergir do processo, uma corporação virtual, terá pouco em comum com aquilo que existia antes [...] a vantagem ficará com as empresas que melhor perseguirem esta meta [...] Quanto mais perto uma corporação chegar da produção instantânea e eficaz em relação ao custo de bens e serviços de massa sob medida, mais competitiva e bem-sucedida ela será (p. 3).*
> *A resposta rápida da fabricação na corporação virtual elimina muitos dos erros provocados por previsões incorretas. A capacidade para responder melhor às necessidades dos clientes possibilita que a empresa cobre preços mais elevados. Quando se considera que o fabricante já está auferindo lucros maiores com estoques menores, menos refugos com ciclos de produção mais rápidos e com custos menores, a chance de poder cobrar preços mais altos vem como bônus extra. [...] Isto é possível por duas razões: o produto chega mais cedo ao mercado aumentando o valor percebido para os clientes em potencial e suas características se encaixam melhor às necessidades desses clientes (p. 110).*

**A "Economia Digital"**

Com a evolução tecnológica e o advento das redes, a economia passou a ser o que Tapscott chamou, em 1995, 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 *armazenadas em computadores e sendo transportadas à velocidade da luz através das redes. Usando este código binário, informação e comunicação transformam-se em dígitos um e zero. O novo mundo de possibilidades daí criado é tão relevante quanto a invenção da própria linguagem, o velho paradigma no qual todas interações baseadas fisicamente ocorriam* (p. 6).

A evolução tecnológica está fazendo surgir uma nova economia, segundo Tapscott (1995) e passamos a viver a "idade da areia". Doze temas ilustram a diferença entre a antiga e a nova economia:

1) *conhecimento - a nova economia é a economia do conhecimento - não exatamente de inteligência artificial, mas o conhecimento criado por seres humanos (a relação é de 3 trabalhadores técnicos para um operário).* [...]

2) *digitalização - a nova economia é uma economia digital - através da história, revoluções nos recursos naturais têm classificado novos paradigmas em ferramentas (ferro, bronze aço), que levam a novos modos de criação de riqueza e desenvolvimento social. A nova era 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. Todas informações são traduzidas em 1s e 0s. Na nova economia, informação está numa forma digital:* bits. [...]

3) *virtualização - com a substituição da informação de análoga para digital, as coisas físicas transformam-se em virtuais - mudando o metabolismo da economia, os tipos de instituições, potenciais relacionamentos e a natureza da própria atividade econômica.* [...]

4) *molecularização - a nova economia é molecular. As velhas corporações estão sendo desagregadas, substituídas por moléculas dinâmicas e agrupamentos de indivíduos e entidades que formam a base da atividade econômica. A organização não necessariamente desaparecerá mas se transformará. Massa transforma-se em molécula em todos aspectos da economia e vida social.* [...]

5) *integração / entreredes - a nova economia é uma rede, integrando moléculas em agrupamentos que agregam-se com outros para criação de riqueza.*[...]

6) *desintermediação - funções intermediárias entre produtores e consumidores estão sendo eliminadas através das redes digitais.* [...]

7) *convergência - na nova economia, o setor econômico dominante está sendo criado por 3 indústrias convergentes que, por sua vez, fornecem infra-estrutura para criação de riqueza em todos setores (computação, comunicação e entretenimento).* [...]

8) *inovação - a nova economia está baseada numa economia de inovação: torne seus próprios produtos obsoletos, porque se você não o fizer outros o farão.* [...]

9) *adequação às necessidades do cliente (*prosumption*) - na nova economia o intervalo entre consumidores e produtores desaparece porque o consumidor pode interferir diretamente no processo de fabricação.* [...]

10) *imediatismo ("imediacy") - em uma economia baseada em* bits, *imediatismo transforma-se em direção chave e variável para o sucesso do negócio - a nova empresa vive em tempo real, ajustando-se continuamente e imediatamente às condições comerciais. Os pedidos de compra chegam eletronicamente e são instantaneamente processados.* [...]

11) *globalização - a nova economia é uma economia global.* [...]

12) *discordância - questões sociais estão surgindo, causando traumas e conflitos. (p. 44 a 68).* [...]

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

**A Internet**

Laudon & 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" (p. 349):

> *Embora não exista uma definição unânime da* ***Internet****, pode-se com certeza dizer que ela é uma rede internacional de redes, e não apenas uma única grande rede. Estimativas indicam que mais de 31.000 redes diferentes, de mais de 100 países, estavam conectadas na primavera de 1995 e era usada por mais de 20 milhões de pessoas ao redor do mundo em educação, ciência, governos e negócios. [...] Ela não tem um proprietário e uma organização gerencial formal. Esta descentralização é intencional para torná-la menos vulnerável a ataques terroristas ou de inimigo - nasceu no Departamento de Defesa [*do Governo Americano*] para compartilhar dados de pesquisa. 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. Este é o motivo que este meio de comunicação é muito mais barato do que outros, como canal de voz, correio, [...] (p. 349 e 350).*

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

> *A World Wide Web é o coração da recente explosão no uso comercial da rede. A Web é um padrão para armazenamento, recuperação, formatação, e apresentação das informações usando arquitetura cliente/servidor. A Web usa interface gráfico para fácil visualização. É baseada 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. Usando estas ligações os usuários precisam apenas apontar para uma palavra chave, "clicar" nela e imediatamente são transportados para outros documentos, provavelmente em outros computadores em algum outro lugar do mundo. As empresas, por exemplo, oferecem informações técnicas de produtos; varejistas oferecem mercadorias e pessoas podem oferecer currículos a empresas que estejam efetuando recrutamento. (p. 351).*

Através desta *Information Superhighway*, pessoas podem se comunicar interativamente, 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 lógico 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.

A comercialização pela Internet cresce aceleradamente, chegando a competir com as vendas tradicionais. Matéria publicada no *jornal O Estado de São Paulo* de 10/03/98, citando artigo de Peter Doyle em The Guardian cita que este comércio além de trazer vantagens sobre o tradicional (como estar livre de restrições de horários, tráfego, estacionamento ou distância para comprar), ainda pode ser feito por preços menores. Como exemplo comenta que, na Inglaterra, é possível comprar-se o último *best seller* americano, através da Internet (encomendando à Amazon), por preço 33% menor que numa livraria “real” (mesmo incluindo-se aí os serviços postais). Cita ainda que 11% dos veículos novos vendidos em 1997 nos Estados Unidos o foram pela Internet.

**O Que Pensar Quanto à Segurança**

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" (pág. 184). Esta falha foi criada em 2 de novembro de 1988 por um estudante de graduação de Cornell: Robert Tappan Morris. Ele descobriu que era possível obter acesso aos servidores Unix de toda rede Internet. Este acesso era obtido através de dois programas: um que processava no servidor sob ataque "(99 linhas em linguagem de programação C, chamado l1.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, na pág. 186, que provavelmente excederam 150.000 dólares, em uma época que a Internet estava praticamente restrita aos meios militares e acadêmicos).

Applegate (1995) aborda as preocupações associadas ao comércio eletrônico, dividindo-as segundo sua natureza em 6 classes (autorização, autenticação, integridade, privacidade, fraude/roubo e sabotagem). Um resumo de seu enfoque, que apresenta impacto para o negócio e possível solução para cada preocupação é apresentado no Quadro 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 | ▪ O remetente da mensagem realmente a enviou?<br>▪ O destinatário pode estar certo que a mensagem não foi trocada? | Assinatura digital |
| Privacidade | ▪ A minha conversação (ou transação comercial) é privativa?<br>▪ Existe alguém espionando? | Chaves públicas e privadas de criptografia |
| 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<br>*Firebreaks* – barreiras físicas através das quais não existe conexão eletrônica entre o servidor Internet e os sistemas de informações internos da empresa. |
| **Quadro 1 - Baseado em APPLEGATE, Lynda M. McFARLAN, F. Warren e McKENNEY, 1995, James L. Corporate Information Systems Management – Text and Cases – Irwin, 4ª Edition** | | |

Zboray (1998) aponta que os procedimentos de segurança na Internet podem ser agrupados nos seguintes tópicos:

***a) Autenticação e autorização***

*Para efetivar uma autenticação o usuário deve estar identificado de maneira confiável. Para a maioria das aplicações críticas, tais como as que envolvem grandes volumes financeiros, o recomendável é a utilização de produtos de autenticação dupla.* [O texto cita como exemplos produtos da Security Dynamics e da Secure Computing (respectivamente "SecurID" e "SaveWord"].

*Associada à necessidade de autenticação, existe a necessidade de controle do acesso dos usuários exclusivamente às informações a eles autorizadas. A técnica inicialmente usada para isto (tabelas de controle de acesso) nem sempre é aplicável em larga escala. Para contornar esta dificuldade, existem bancos de dados que permitem uma gestão centralizada de direitos de acesso.* [Como exemplo de fornecedores de tecnologia de gestão centralizada para autenticação e autorização, o texto cita a NeTegrity e a Blockade Systems].

***b) 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.* [Como exemplo de proteção nem sempre suficiente, pode-se citar a tecnologia baseada em chave de 40 *bits*. As mensagens que requerem maior proteção devem usar chaves de 128 *bits*]

***c) 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 ele 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. Como exemplo, os dados nunca devem estar armazenados no servidor Web: eles somente devem poder ser acessados por aplicativos exclusivos, em cumprimento às solicitações vindas dos usuários.*

*Para os aplicativos mais críticos, os sistemas operacionais do servidor Web não devem permitir conta de usuários privilegiados (com acessos amplos), mas apenas executar serviços em "compartimentos fechados". Esta proteção é avaliada pelo Departamento de Defesa do Governo Americano como nível B1. Tais restrições limitarão o poder de visualização e exploração das vulnerabilidades no caso de um acesso espúrio, mas têm como contra-partida elevação dos custos para administrar o ambiente.*

***d) Protegendo a Intranet***

*Finalmente, 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 (internos e externos) previamente definidos. Este procedimento de segurança, embora de eficácia pequena (porque não se pode garantir sempre a confiabilidade dos endereços externos), não deve ser desprezado.*

*Uma vez mais, para prevenção contra ataques, canais encriptados devem ser utilizados entre os servidores Web e os aplicativos. Este método protege contra ataques (internos e externos) que*

*utilizem servidores Web autênticos mas com autorizações indevidas.*

Embora existam estas recomendações de segurança, as mesmas não são facilmente implementáveis no mundo. Como exemplo de dificuldade, pode-se destacar a resistência do Governo Americano em permitir livre comercialização de técnicas de criptografia. Em texto de Hallawell (1998), divulgado pelo Gartner Group dá conta desta barreira. Este texto, explorava a pergunta "quais as melhores práticas que as organizações de segurança de informações irão adotar para evitar responsabilidade legal potencial na salvaguarda de informações?" A resposta foi que:

> *com 80% de probabilidade, o governo americano não iria aliviar as restrições de exportações de mecanismos de criptografia até o ano 2001. Esta posição é decorrente do fato de encararem estes mecanismos como armas, já que foram usados por séculos, pelas forças militares para se comunicar e para decifrar as comunicações dos inimigos. Tal preocupação governamental vem desde 1917, com o "Trading With the Enemy Act" e, apesar de terem ocorrido algumas concessões, a preocupação do Governo em evitar disseminação da técnica de criptografia ainda continua bastante grande.*

Assim como a tecnologia para comércio eletrônico está evoluindo, também estão sendo desenvolvidas, a cada dia, ferramentas para permitir maior controle e segurança das transações. Como exemplo de produtos desta natureza pode-se destacar o SET - Secure Electronic Transaction. Este padrão é um protocolo mundial de segurança, que já está disponível na Internet, e permite que haja verificação do portador do cartão, do emissor e do estabelecimento comercial onde está se realizando a compra. Para cobrir este objetivo, usa tecnologias de criptografia e autenticação digital. Segundo a revista Internet World, nº 35, de jul/98 "o Bradesco usa esta tecnologia para garantir a segurança das transações comerciais na rede".

## CONCLUSÃO

A realidade trazida pela nova tecnologia mudou significativamente os antigos métodos de realizar negócios. O deslocamento físico não é imprescindível, a validação para confirmar a identidade do parceiro deixou de ser visual ou baseada em documentos físicos, a velocidade em que as transações ocorrem aumenta a cada dia. Dentro deste contexto, o auditor precisa se capacitar para poder continuar cumprindo sua missão. Apenas através desta capacitação, será possível que ele atue de maneira adequada frente aos novos riscos trazidos pela nova tecnologia.

A propósito desta mudança do perfil do auditor, o Editor Chefe do IS AUDIT & CONTROL JOURNAL, Michael P. Cangemi comenta, em editorial do *IS Audit & Control Journal*, Volume I, 1998, p. 5, que a busca por segurança na Web está fazendo surgir um novo mercado. Segundo ele, o AICPA – American Institute of Certified Public Accountants e o CICA – Canadian Institute of Certified Accountants desenvolveram o selo "WebTrust", para garantir que um *site* é de confiança, pois atende aos princípios e critérios para negócios através de comércio eletrônico. Segundo o AICPA, o "WebTrust" é um serviço visando quebrar as barreiras de resistência dos consumidores em aceitar o comércio eletrônico. O "WebTrust" foi desenvolvido de acordo com um conjunto de princípios divulgado pelo Grupo Executivo do Governo Americano através do documento "A Framework for Global Electronic Commerce". Este selo de garantia, que será exposto na página Web, pode ser concedido por um auditor (CPA ou CA). Para isto, tal profissional terá que completar um treinamento especial que o qualificará a emitir o "Selo de Segurança WebTrust".

Como parte significativa da capacitação citada acima, a familiarização com novas técnicas de controle pode ser buscada em literatura especializada. Em função da limitação de espaço prevista para este estudo, não se pretende apresentar uma discussão extensa de bibliografia tratando o assunto, mas apenas efetuar alguns destaques.

Inicialmente pode-se citar um livro, supostamente escrito por um *hacker* bastante experiente,

que obviamente não se identifica. Ele mostra com riqueza de detalhes (usando aproximadamente 900 páginas) as proteções existentes em diferentes plataformas. Esta publicação é interessante também porque fornece relação de vários *sites* na Internet com endereços de consultores de segurança. O nome deste livro é *Maximum Security - A Hacker's Guide to Protecting Your Internet Site and Networking.*

Outra publicação a ser destacada, de autoria de Garfinkel & Spafford, também mostra diversos aspectos a considerar na segurança do comércio eletrônico. Este livro examina as novas tecnologias, os riscos associados e as estratégias para minimizar tais riscos.

Além destas fontes citadas anteriormente, existe uma publicação, divulgada pela ISACA - Information Systems Audit and Control Association & Foundation (www.isaca.org), que auxilia o trabalho do auditor: *o COBIT - Control Objectives for Information and Related Technology*. O ISACA é uma associação mundial sem fins lucrativos que congrega mais de 17.000 auditores de informática.

Um último fato que merece destaque é que, em função do próprio dinamismo do ambiente que fornece a infra-estrutura técnica para comércio eletrônico, as recomendações contidas nestas publicações geralmente não têm vida útil muito extensa. Portanto, é fundamental que o auditor continue permanentemente se atualizando.

## REFERÊNCIAS BIBLIOGRÁFICAS


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

**CANGEMI**, Michael P. *IS Audit & Control Journal*, Volume I, 1998

**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

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

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

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

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

**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

**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 de Indústira Automobilística, Comércio e Serviços)

**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

**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

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