FRAUDES POR COMPUTADORES

João Batista Mendes
Professor da Universidade Federal de Uberlândia
Luiz dos Santos lins
Professor da Universidade Cândido Mendes
Maurício Rocha Neves
Professor na Fundação Getúlio Vargas/RJ e no Instituto Brasileiro de Analistas de Mercado

A realidade da utilização

dos sistemas informatizados

sem a devida preocupação

com a segurança do sistema,

permitindo a prática

de diversos tipos

de fraudes aplicadas

com interesses diversos,

colocando as organizações fragilizadas

pela falta de sistemas

de segurança.

1 INTRODUÇÃO

1.1 Definição do problema

O problema de fraudes por computadores, considerado secundário até pouco tempo pela maioria dos usuários, começa a ser visto com crescente preocupação.

Um dado fundamental para esta preocupação é a progressiva tendência dos grandes usuários em evoluir para o processamento de dados descentralizados em tempo real *(on-line)* e a proliferação do uso de microcomputadores no ambiente de Processamento Eletrônico de Dados (PED).

Como resultado, um número cada vez maior de pessoas passam a ter acesso aos equipamentos que por sua vez, não havendo controles adequados, passam a ter acesso aos dados confidenciais guardados nos registros dos computadores, como estrutura de custos, folha de pagamento, lista de clientes, entre outros.

Os controles sobre o sistema central de PED de uma organização podem ser enfraquecidos pela difusão de conhecimentos sobre computadores, que é uma tendência geral. Os usuários podem ser capazes de redigir programas para tentar manipular dados armazenados no equipamento de grande porte.

Com a possibilidade de utilizar o microcomputador como terminal de grandes computadores a partir de circuitos de transmissão de dados (linha telefônica), é possível a uma pessoa não autorizada entrar no sistema (de computadores) de um banco, por exemplo, para tentar creditar uma quantia em uma determinada conta. Do mesmo modo, é possível a alguém, na tentativa de obter alguma informação confidencial, destruir registros ou informações valiosíssimas.

1.2 Objetivos do trabalho

Apesar das estimativas de perdas com crimes utilizando computador em nosso país parecerem pequenas, é certo que somente os grandes crimes são divulgados e comentados, ficando a maioria deles circunscritos aos limites das organizações vítimas das fraudes. Questões éticas e de segurança, podem ser alguns dos motivos da não divulgação.

Assim, este trabalho objetiva chamar a atenção dos auditores e dos usuários para a conscientização do problema, especialmente daqueles sem muita tradição em processamento de dados.

2 CONSIDERAÇÕES GERAIS

2.1 Ocorrência de fraude

Na criação e desenvolvimento de sistemas os encarregados de *"desenharem"* o sistema, freqüentemente concentram seus esforços para que os principais objetivos e finalidades a que o sistema se propõe sejam atingidos. Por conseguinte, essas pessoas costumam dar apenas uma consideração secundária aos requisitos de controles dos sistemas.

Desta forma, uma das maiores preocupações com que os gerentes, auditores e analistas de processamento de dados se deparam, é a identificação no ciclo de vida dos sistemas, dos problemas e riscos a que os mesmos estarão expostos, a repercussão que tais riscos terão nos sistemas e a probabilidade de sua ocorrência.

Concentrando nossa atenção num ambiente informatizado, podemos utilizar o raciocínio de ALLEN (1972) para ilustrarmos os riscos a que estão sujeitos os Centros de Processamento de Dados (CPD's). segundo o referido autor, os cinco itens que são os maiores causadores de problemas aos CPD's são:

a) fogo;

b) roubo

c) vandalismo;

d) fraude;

e) água.

Falando em sistemas de informações, dentre os cinco métodos de ataque aos sistemas anteriormente expostos, a fraude é sem dúvida o mais freqüente.

Para conceituarmos o que é fraude, podemos fazer uso de uma definição elaborada por PARENTE (1982, p. 41) em sua dissertação de mestrado:

> *"... uma quebra proposital das ligações existentes entre a realidade e a sua representação manual ou automatizada, com o fito de se obterem vantagens direta ou indiretamente."* (grifo nosso).

Como podemos observar, a fraude tem caráter intencional onde a ação premeditada que gera uma anormalidade no sistema, se distingue de um erro do qual, mesmo ocasionalmente também uma anormalidade, não é intencional.

As principais características que uma fraude pode assumir quando em atuação em um CPD, são as seguintes:

a) manipulação indevida de dados de entrada *(inputs)* ou informações geradas *(outputs);*

b) desenvolvimento de *"softwares"* para atuar em conjunto ou em substituição ao *"software"* do sistema;

c) alteração, revelação ou destruição de dados;

d) transmissão, interceptação, destruição ou desvio de informações para canais diferentes da empresa;

e) atraso do fluxo de informações necessárias a tomada de decisões;

f) provocação de pane nos equipamentos de suporte e nas instalações.

Apesar do conhecimento destas principais características, existe um fator dentro de toda e qualquer empresa que, embora seja subjetivo, influencia amplamente no grau de ocorrência de fraudes: é a atribuição de responsabilidade às diversas pessoas envolvidas no sistema.

As organizações, sejam elas grandes ou pequenas, ao projetarem seus sistemas de operação definem, de alguma forma, certos pontos de controle com os quais seus administradores objetivam tomar conhecimento do estado em que se encontram os sistemas de que se utilizam. Em outras palavras, existe um certo grau de controle sobre os indivíduos de uma organização, que via de regra está mais voltado para aqueles menos graduados. Geralmente a intensidade dos controles existentes em uma organização, varia em fun-

ção dos níveis hierárquicos. Os níveis mais elevados costumam ter maior responsabilidade e menor controle, ao passo que os níveis mais baixos apresentam uma posição inversa, ou seja, mais controles e menos responsabilidades.

E para deter a ação do fraudador, o fator determinante é o grau de controle que sobre ele é exercido. Por esta razão, estudos realizados nos casos detectados de fraude nos EUA levaram a duas conclusões:

a) as fraudes de maior valor são elaboradas por funcionários do alto escalão da empresa, onde o controle é fraco ou até inexistente;

b) as fraudes menores ocorrem com maior freqüência, e são perpetradas por funcionários de nível hierárquico baixo.

3 CLASSIFICAÇÃO DAS FRAUDES

A maioria dos textos sobre o assunto se limita a descrever o que é fraude, quais são suas características principais e a citar alguns exemplos de controles baseados nestas características. Mas, foi em *"Crime by Computer"* PARKER (1977, p. 48-49) que encontramos uma classificação para as fraudes:

a) pelas funções dos agentes da fraude;

b) pelos atos criminosos praticados.

No primeiro tipo, incluem-se tanto os funcionários como pessoas externas à empresa. Uma das limitações desta classificação seria as denominações de alguns cargos, comum nos EUA, porém não familiares à nossa cultura.

O segundo tipo de classificação, além de apresentar maiores detalhes, está mais de acordo com os propósitos do presente trabalho, razões pela qual adotaremos a mesma.

Desta forma, podemos classificar as fraudes como:

a) sabotagem;

b) roubo de informação ou propriedade e uso ou venda de serviço não autorizado;

c) fraude financeira.

3.1 Sabotagem

Incluídos nesta modalidade estão todos os atos praticados para danificar ou destruir os próprios equipamentos, ou os dados e informações que eles manipulam. É importante ressaltar que a sabotagem se distingue do vandalismo. Este, como sendo um ato praticado sob um estado de espírito, e a sabotagem como o ato praticado com a finalidade de se obter algum benefício. A diferença, apesar de sutil, compara-se de maneira análoga a distinção entre erro e fraude.

Assim, dois tipos principais de sabotagem podem ser caracterizados: quebra de equipamento e deleção de dados.

3.2 Roubo de informação ou propriedade e uso ou venda de serviço não autorizado

Uma das modalidades mais freqüentes de fraude, consiste no agente fraudador ter acesso a ativos da empresa, incluindo-se aqui as informações. A partir do momento em que uma grande quantidade de dados passam a ser manipulados por sistemas automatizados, diversas operações conduzidas por computadores ficam sujeitas a fraudes se não existirem controles adequados. É o caso por exemplo, de vendas, compras, estocagem de mercadorias, dentre outros. Desta forma, a fraude enquanto roubo de informações pode ser executada para uso próprio ou de terceiros ao passo que o roubo de propriedade poderá ser de *"hardware"*, *"software"* ou ainda de outros ativos cujo controle seja exercido por computador.

3.3 Fraude financeira

A área financeira, por motivos óbvios, é sempre a que corre maiores riscos, pois, além de ter atualmente uma dependência maior da informática, as informações manipuladas pelos computadores representam dinheiro. Segundo pesquisas realizadas nos EUA no período de 1973 a 1975, este tipo de fraude é que a mais acontece. Principalmente em função do aspecto principal envolvido (dinheiro), os esforços dos agentes fraudadores costumam ser maiores nesta modalidade tendo em vista o benefício direto que eles procuram alcançar na maior parte dos casos.

A fraude financeira é em geral perpetrada sob duas formas: a alteração de dados e o desvio de numerário.

4 CONTRAMEDIDAS POR CATEGORIA

Uma vez identificados os tipos de fraudes, torna-se possível estabelecer alguns controles vi-

sando evitar a ocorrência destes atos. Ressalte-se que não é nosso propósito fornecer todas as formas possíveis para evitar que hajam fraudes, mas sim abordar os principais controles que podem ser utilizados em função da classificação abordada no tópico anterior.

4.1 Contramedidas para sabotagem

Com base na idéia exposta sobre a sabotagem como uma modalidade de fraude, podemos constatar a necessidade intrínseca de produção física principalmente para os equipamentos e instalações.

Portanto, podemos mencionar seis aspectos básicos voltados para a segurança física de um CPD:

a) na portaria do prédio onde se localizar o CPD, não deve constar no quadro informativo de salas em que andar está situado o CPD;

b) ao mesmo tempo, deve haver identificação de pessoas externas que tenham acesso ao prédio, na própria portaria do edifício;

c) a porta que dá acesso ao CPD deve ser do tipo "corta-fogo", e a sua abertura só deve ser possível mediante *"password"* (senha);

d) uma vez dentro da própria sala do CPD, é recomendável o monitoramento constante do ambiente através de câmeras de circuito fechado de TV;

e) proteção contra incêndio, sendo ultimamente recomendado o sistema de gás *halon;*

f) constituição de um plano de contingência a fim de não ter problemas operacionais como ficar inoperante em função de uma danificação nos equipamentos do CPD.

4.2 Contramedidas para roubo de informação ou propriedade uso ou venda de serviço não autorizado – fraude financeira

Em virtude das características similares que estas modalidades de fraudes possuem, abordaremos um conjunto de procedimentos de controle aplicáveis a todos os tipos.

Quando nos referimos a um sistema computadorizado, existem três pontos básicos que merecem atenção especial quanto ao aspecto de controle: lógica do programa; variações de execução do sistema e acesso físico ao sistema.

4.2.1 Lógica do programa

Para este ponto devem estar presentes os seguintes tipos de controles:

a) **verificação de dados chaves:** entende-se por dados chaves (ou dados críticos) aquele tipo de dado que é prontamente identificável como passível de manipulação em caso de fraude; por exemplo, um dado chave em um programa que processa vendas, seria o número de identificação do vendedor tendo em vista a comissão sobre as vendas;

b) **relatório de confirmação:** nos casos necessários, deve haver uma forma de se confirmar junto à(s) pessoa(s) diretamente interessada(s) se determinada ação é valida; seria o caso de uma ordem de compra emitida pelo funcionário "João" em nome do funcionário "José" sem que este soubesse; o relatório de confirmação endereçado para "José" sanaria este problema;

c) **controle de seqüência das gerações/versões de relatórios e arquivos:** presumindo-se a existência de um grupo de controle de dados, é importante que no decorrer do processamento, o programa desenvolva contagens dos vários tipos de registros acessados, rejeitados, alterados e incluídos;

d) **parâmetro de tempo de utilização:** convém que haja uma espécie de padrão temporal para utilização de um determinado programa e sua periodicidade; exemplo: folha de pagamento (três vezes por mês com seis horas diárias);

e) **modificação de dados:** um sistema computadorizado deve possuir programas flexíveis o suficiente para alterar dados chaves susceptíveis a mudanças rápidas tais como limite de crédito para clientes; estas modificações devem ser efetuadas mediante código de identificação e de autorização do funcionário encarregado.

4.2.2 Variações de execução do sistema

É vital que existam controles instalados de tal forma que seja possível confirmar, por evidência física, que todos os programas foram executados na seqüência apropriada utilizando a versão correta de cada arquivo; esta evidência física é possível mediante um relatório de "log" do sistema. Segundo CHRYSLER, KELLER (1988, p. 30-31)

> *"Este* 'log' *documenta quais arquivos foram utilizados como* 'input' *para cada trabalho, e a seqüência em que os trabalhos foram executados, dentre outras informações".*

4.2.3 Acesso lógico ao sistema

Além da ótica de proteção física aprovada nas contramedidas para sabotagem, é necessário pensar em controles quanto ao acesso lógico comum, por parte dos usuários, ao sistema. Desta forma é importante que haja:

a) *obsolescência automática de* "passwords": as senhas utilizadas não devem permanecer por longos períodos, mas sim serem substuídas por novos códigos de segurança em pequenos espaços de tempo;

b) *criptografia:* uma espécie de linguagem conhecida apenas pelo portador da senha, evitando assim a exibição do código de segurança;

c) *validade do usuário, do terminal e do período de acesso:* em grande parte dos casos, é possível estabelecer o terminal (ou terminais) regularmente utilizado(s) para acessar o sistema, os dias da semana e os horários de utilização nestes dias; assim sendo, é importante que estas três condições sejam controladas para o acesso às informações; qualquer anormalidade deve ser bloqueada pelo sistema até a correspondente autorização;

d) *autenticação de terminais:* evita-se assim a chance de terminais não autorizados realizarem transações ou acessarem informações;

e) "log" *das variações de acesso ao sistema:* assim como se deve controlar a execução do sistema, o acesso físico também deve ser "loggado" evidenciando todos os passos de acesso ao sistema.

Além desses três pontos básicos com relação a sistemas computadorizados, existem alguns procedimentos que devem ser desenvolvidos e aplicados como forma de proteção da informação.

A utilização de controles internos paralelos, cuja importância não pode ser desmerecida pelo advento da informática, são essenciais numa organização. Sem entrar no mérito de exemplificá-los, vamos apenas citar aquele controle que nos parece fundamental: segregação de funções. A este respeito, BEQUAI (1988, p. 31) comenta que:

> *"o melhor que existe em termos de medidas de segurança – física, eletrônica, software e tudo mais – são na verdade de valor limitado. A primeira, a melhor e a verdadeira linha de defesa que eu sugiro aos empresários é a adequada segregação de pessoal dentro da empresa".*

Um segundo aspecto a mencionar seria a utilização de *"softwares"* aplicativos de controle, também conhecidos como *"software"* de segurança para computadores. Tais *"softwares"* são desenvolvidos para efetuar tarefas específicas de proteção de informações e existe uma gama deles. A título de exemplos, podemos citar: RACF, ACF2/ VM, *Top Secret, Guardian,* etc.

É um procedimento que não está diretamente ligado ao aspecto de controle, mas é fundamental, é um trabalho de conscientização dos funcionários da empresa fazendo uso do *"marketing"* na proteção da informação. É importante que esta conscientização se inicie de forma verticalizada, da mais alta esfera até aquele empregado que manuseia diretamente as informações de processamento de dados. Apenas deve-se ter cautela quanto ao que FANTINATTI (1988, p. 20) comenta:

> *"... a velha tática de usar o positivismo ajuda a se conseguir a aceitação do processo de proteção dentro da organização, mas não nos esqueçamos de sempre procurar ter um racional claro e preciso para os pontos negativos que podem surgir".*

Pelos fatores expostos temos que o maior desafio é o de se desenvolver rotinas capazes de identificar e utilizar técnicas automáticas para preservar de modo adequado as informações e evitar a ocorrência de fraudes. Como não existem duas organizações idênticas no que se refere às

necessidades de proteção ou de meios para implementar tais rotinas, torna-se praticamente impossível a elaboração e adoção de uma solução padronizada.

Neste campo o que existem são diretrizes genéricas de como trabalhar. mas um ponto é claro: a análise de cada caso é obrigatória, e sem dúvida deverá haver uma assessoria de profissionais especializados no assunto.

5 ESTUDO DE CASO

5.1 Descrição da fraude

O funcionário Sr. Abravanel utilizou um terminal "loggado" de um colega de departamento (quando o mesmo estava no *toillete)* e descobriu que havia um sistema de controle de estoque que controlava as mercadorias para venda e os valores pagos.

Sabendo disso ele passou a utilizar, em conivência com o colega, um programa pirata que "interfaceava" tal sistema com o objetivo de desviar valores para sua conta, através de simulação de pagamentos de mercadorias (fantasmas).

Tal situação perdurou até o momento que "Abravanel", viu que podia inclusive desviar mercadorias reais, o que passou a fazer colocando endereços de firmas de amigos seus.

Após 1 ano, por um acaso (fiscalização estadual) a fraude foi descoberta, gerando um minucioso trabalho de auditoria. Após um tempo, a auditoria concluiu que somente esses dois funcionários poderiam fazer tal ação e a empresa demitiu-os formalmente, exigindo porém que os mesmos permanecessem na área, colocando todos os papéis em ordem, a fim de amenizar parcialmente os danos que causaram.

Revoltados, esses dois funcionários entraram nos vários sistemas os quais eram autorizados e deletaram vários dados, além de danificarem propositalmente o micro utilizado na emulação de terminal.

5.2 Levantamento dos pontos fracos do sistema e recomendação de melhorias

Com base no caso apresentado, relacionamos, por ordem de ocorrência as principais falhas de controle interno bem como as referidas recomendações de melhorias:

1) A inexistência de *"time out"* permitiu ao Sr. Abravanel a utilização do terminal do colega de departamento, terminal este que era "loggado".

   Recomendação: A existência de controles que "derrubem" o acesso ao programa, após algum tempo sem utilização, evitando assim a entrada de pessoas não autorizadas durante a ausência do operador (usuário) possuidor da *"password"*.

2) A falta de *"softwares"* aplicativos de controle, tais como os citados nas páginas anteriores deste trabalho, permitiu a utilização de um programa pirata.

   Recomendação: A existência de controle com tarefas específicas de proteção às informações, não permitindo acessos por programas não autorizados.

3) A inexistência de agregação e de rodízio de funções facilitou a conivência de dois funcionários.

   Recomendação: Segregação e rodízio de funções.

4) A inexistência de controles de acesso físico às dependências do CPD permitiram que os funcionários demitidos entrassem em vários sistemas, aos quais tinham acesso anteriormente autorizado, e deletassem diversas informações além de danificarem o *"hardware"* utilizado.

   Recomendação: A existência de controles de acesso mais rígidos, dificultaria a ocorrência dos prejuízos causados pelos funcionários demitidos; ao menos um desses controles seria que ao ser emitido um aviso prévio, uma via deve ser remetida imediatamente ao CPD para o cancelamento automático das senhas de acesso.

Ressalta-se que em todo e qualquer caso onde sejam feitas recomendações visando cobrir pontos falhos em um sistema, é fundamental a análise de custo x benefício em torno das recomendações propostas. A análise econômica dessas sugestões precisa ser considerada em função dos pontos que elas vão cobrir.

6 CONCLUSÃO

A preocupação com as fraudes por computador é recente e os conhecimentos sobre segurança em informática estão sempre em processo de aprendizado. Este processo consiste em um certo atraso tecnológico das metodologias de segurança em relação as tecnologias de *"softwares"* e *"hardwares"*.

O problema da segurança das informações (prevenção contra fraudes ou qualquer outro ataque ao sistema) é um assunto que não deve ficar restrito a área de responsabilidade do pessoal do CPD. A alta administração da empresa deve se preocupar seriamente e dedicar tempo, esforços e recursos financeiros para sobrepor as perdas em potencial devido as falhas no sistema computadorizado.

Por estes aspectos, é necessário que se tenha um profissional que coordene as atividades de proteção das informações, ou seja, um analista de segurança em computação. Outros profissionais que também devem estar inseridos no contexto da proteção dos sistemas computadorizados são, o analista de qualidade em computação e o auditor de sistemas.

Entretanto, é necessário que esses profissionais se preocupem também com o aspecto cultural, quanto aos conceitos de segurança por parte dos usuários. Por falta de uma consolidação da cultura de segurança em nosso país, muito já deve ter se perdido, em termos de tempo e recursos monetários.

Esta falta de cultura de segurança está presente em nosso dia-a-dia, quando observamos o número de acidente de trabalho causado por falta ou mau uso dos equipamentos de segurança a nossa relutância em utilizar cintos de segurança em automóveis ou capacete de proteção para motocicletas, etc.

Ao transpormos este problema para a área de informática (que é uma tecnologia relativamente nova em nosso país, podemos inferir que aqui também existe uma deficiência da cultura de segurança em informática. Podemos flagrar em alguns bancos por exemplo, funcionários utilizando cartões magnéticos e senhas exclusivas de outros funcionários e não raramente clientes fazendo o mesmo, sem se preocupar com a proteção de seus dados, tais como números da conta, senha e saldo existente.

É preciso conscientizar as pessoas de que a proteção das informações se faz necessária, quer as mesmas constem de documentos mantidos em gavetas quer em arquivos magnéticos.

Ao desenvolvermos a nossa cultura de segurança em informática, estaremos criando condições para que haja uma total participação do computador na vida das organizações, de uma forma correta, segura e eficiente, dando assim a nossa parcela de contribuição para o nosso próprio desenvolvimento.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, B. Computer security. *Data Processing,* Jan./Feb. 1972.

ANDRADE, J. G. A. O banco de dados como suporte de auditoria. CONGRESSO NACIONAL DE INFORMÁTICA, 14, 1981, São Paulo.

BEQUAI, A. What can accountants do?. In: Preventing computer fraud, op.cit., p. 31.

BIO, S. *Sistemas de informações gerenciais.* São Paulo: Atlas, 1985.

CHRYSLER, E., KELLER, D. E. Preventing computer fraud. *Management Accounting,* p. 30-31, April 1988.

FANTINATTI, J. M. *Auditoria em informática:* metodologia e prática. São Paulo: McGraw-Hill, 1988.

-----. *Segurança em informática:* metodologia e prática. São Paulo: McGraw-Hill, 1988.

GIL, A. L. *Auditoria de computadores.* São Paulo: Atlas, 1989.

LE GRAND, C. H. Discourging fraud through system deseign. *The Internal Auditor,* April 1986.

LOVIZZARO, C. A segurança no computador. *Dados e Idéias,* São Paulo, out. 1984.

PARENTE, F. A. F. *Auditoria de sistemas automotizados.* Fortaleza : Banco do Nordeste do Brasil, 1982.

PARKER, D. B. Crime by computer. New York: Charles Scribners, 1977. In: PARENTE, op.cit. p. 48-49.

SILVA, R. C. Auditoria de sistemas aplicativos em produção.

TAKABAUASHI, M., HERSAN, H. Tendência da auditoria de sistemas no futuro. In: CONGRESSO NACIONAL DE INFORMÁTICA, 18, 1985, São Paulo.

TOUCHE ROSS. *Controle interno e auditoria em ambiente de PED.* São Paulo, 1988.