Políticas de Segurança em Sistemas de Informação Contábil: um estudo em cooperativas de crédito do estado de Minas Gerais

Security Policies in Accounting Information Systems: a study on credit cooperatives in the state of Minas Gerais

Adélio Carlos de Andrade
Centro de Pós-Graduação e Pesquisas em Contabilidade e Controladoria - UFMG - Brasil

Flávia Cristina Alves Sousa
Centro de Pós-Graduação e Pesquisas em Contabilidade e Controladoria - UFMG - Brasil

Romualdo Douglas Colauto
Centro de Pós-Graduação e Pesquisas em Contabilidade e Controladoria - UFMG - Brasil

Laura Edith Taboada Pinheiro
Centro de Pós-Graduação e Pesquisas em Contabilidade e Controladoria - UFMG - Brasil

Resumo
O objetivo do trabalho é prover um estudo sobre os mecanismos de segurança utilizados na manipulação de sistemas integrados de informação contábil-financeira como forma de prevenção e identificação de fraudes eletrônicas em cooperativas de crédito de Minas Gerais. A pesquisa caracterizou-se como descritiva, com utilização da abordagem quantitativa. O universo selecionado compreendeu 43 cooperativas de crédito mineiras. A técnica utilizada para avaliar os sistemas de segurança foram questionários, sendo que as variáveis analisadas correspondem aos procedimentos usualmente estabelecidos nas normas de segurança da informação. Concluiu-se que a avaliação dos procedimentos de segurança dos sistemas de informação contábil das grandes cooperativas de crédito mineiras apresentou resultados satisfatórios, podendo fornecer adequada confiabilidade quanto aos riscos de erros e fraudes eletrônicas.

Palavras-chave: Sistema de Informação, Contábil. Segurança da Informação, Cooperativas de Crédito.

Abstract
The objective of this work is to provide a study on the mechanisms of security used in the manipulation of integrated accounting financial information systems as a way of prevention and identification of electronic frauds in credit cooperatives in the state of Minas Gerais. The research was characterized as descriptive, having made use of the quantitative approach. The selected universe comprised 43 credit cooperatives of Minas Gerais. Questionnaires were used as a technique to evaluate the security systems and the variables analyzed correspond to the usual procedures established by the norms of the information security. The conclusion was that the evaluation of the security procedures of the accounting information systems of the largest credit cooperatives in Minas Gerais discloses satisfactory results and therefore it will be able to supply the adequate trustworthiness as regards the risks of errors and electronic frauds.

Key words: Accounting Information, System. Security of the Information, Credit Cooperatives.

1 Introdução

As cooperativas são incentivadas em diversos países nos quais foram, inclusive, alçadas ao altiplano constitucional. Tal fenômeno se explica, principalmente, pelo fato de elas representarem uma forma democrática de gerar e dividir a riqueza, de acordo com o trabalho realizado pelos cooperados e não somente com o capital de cada sócio. A Constituição Federal de 1988 refere-se às cooperativas como instrumento capaz de conciliar princípios da valorização do trabalho humano com os da livre iniciativa. Assim, determinou, expressamente, o incentivo à constituição de sociedades cooperativas e estabeleceu prioridade para o apoio e o estímulo ao cooperativismo e outras formas de associativismo.

Em outra vertente, a tecnologia provocou uma grande revolução nas relações sociais e culturais em todo o mundo. Nenhuma tecnologia se desenvolveu e se expandiu tanto quanto a informática, a qual já invadiu, em poucas décadas, todas as atividades exercidas pelo homem. Essa nova tendência tem feito com que as entidades adotem novos conceitos de gestão, que condicionam o seu desenvolvimento a sistemas adequados de informação.

A evolução tecnológica passou a criar diversas facilidades e possibilidades no ramo da informação, que afetam diretamente o indivíduo e a sociedade. A tecnologia da informação surgiu para o aperfeiçoamento das atividades do homem, sejam elas ligadas ao lazer, aos negócios, ao trabalho ou à comunicação. Porém, junto com tais inovações nas comunicações e informações, surgiram as fraudes eletrônicas, ou seja, mesmo que a tecnologia virtual disponibilize tais benefícios às organizações, o meio eletrônico também vem permitindo que usuários de má fé desviem as principais características do objetivo central dos serviços disponibilizados pela mesma.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos e estruturas organizacionais. As organizações - seus sistemas de informação e redes de computadores - são expostas a diversos tipos de ameaças à segurança, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo e incêndio. Danos causados por código malicioso, *hacker* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

Embora ainda não exista uma lei contra os crimes na área de informática no Brasil, há algumas tímidas iniciativas sendo tomadas através de projetos de lei que ora tramitam no Senado e na Câmara Federal. Entretanto, tais medidas ainda não atendem aos anseios dos usuários de computadores, que esperam uma legislação forte e efetiva à prevenção, repressão e punição dos atos lesivos praticados por agressores da área de informática. Assim, o objetivo do presente estudo é conhecer o grau de segurança dos sistemas de processamento eletrônico de dados como forma de prevenção e

combate de fraudes eletrônicas, com enfoque sobre as cooperativas de crédito de Minas Gerais. Com isso, espera-se contribuir com a apresentação de resultados de pesquisa empírica e bibliográfica, que descrevam sobre sistemas de informação contábil, segurança da informação, fraudes eletrônicas e auditoria de sistemas.

2 Procedimentos metodológicos

O estudo caracteriza-se como exploratório pois utiliza pesquisa bibliográfica, e estudo descritivo pois vale-se de fontes secundárias e primárias. O delineamento é um estudo qualitativo, visando a identificar aspectos teóricos e operacionais. Ademais, foram utilizadas uma entrevista semi-estruturada e uma análise de conteúdo para interpretação dos dados. A aplicação do questionário foi on-line, enviada por correio eletrônico, havendo o mesmo sido respondido na íntegra.

O questionário contém dez perguntas fechadas e foi aplicado em 43 (quarenta e três) cooperativas selecionadas através do Anuário de Cooperativas Mineiras de 2006. A seleção destas cooperativas foi feita através de avaliação quanto à classificação de desempenho em cinco variáveis distintas: maior faturamento, maiores ativos, maior patrimônio líquido, número de funcionários e número de associados. A seleção foi assim determinada pelos autores deste estudo com vistas a absorver, entre as maiores cooperativas de Minas Gerais, o maior número de informações acerca de segurança da informação. O questionário foi elaborado com base nas Normas da ABNT e IBRACON.

Ressalta-se que foram escolhidas as cooperativas do ramo Crédito em razão da necessidade de regulamentação, pelo Banco Central, da padronização de procedimentos, bem como por se tratar do segmento cooperativista com o maior nível de informação integrada. Para aplicação do questionário, inicialmente foi feito um contato telefônico com as duas centrais de Cooperativas de Créditos do Estado de Minas Gerais comunicando a intenção e a extensão do estudo, ocasião em que as mesmas se manifestaram favoráveis. Em seguida, o questionário foi enviado por e-mail, juntamente com a descrição e os objetivos da pesquisa, havendo recebido um retorno de apenas 20%. Foi, então, realizado um novo contado com as centrais solicitando que as mesmas enviassem os questionários eletronicamente. Assim, obteve-se 100 % de retorno.

3 Abordagem conceitual de sistema de informação

A informação é um ativo essencial para os negócios de uma organização. Conseqüentemente, necessita ser adequadamente protegida. Como resultado do aumento acelerado da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISSO/IEC 17799, 2005).

A potencialização das informações surge com a informática por meio da informação automatizada. De acordo com Cruz (2000), tecnologia da informação é todo dispositivo que tenha capacidade para tratar os dados e/ou informações tanto de forma sistêmica como esporádica, quer esteja aplicada ao produto, quer esteja aplicada ao processo.

Para Schmidt (2002), um sistema de informação representa um conjunto de procedimentos estruturados, planejados e organizados que, uma vez executados, produzem informações para suporte ao processo de tomada de decisão. Gil (1995) conceitua como um conjunto de recursos humanos, materiais, tecnológicos e financeiros agregados segundo uma seqüência lógica para o processamento dos dados e a correspondente tradução em informações. Para Cruz (2000), os sistemas de informações são processos e informações utilizadas na estrutura decisória da empresa que proporcionam a otimização dos resultados esperados.

3.1 Classificação do sistema de informação

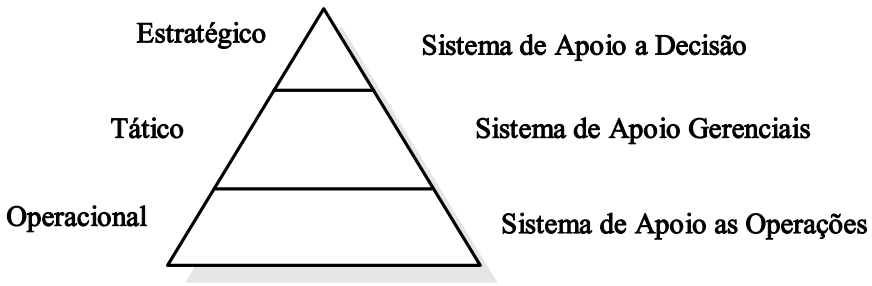
Diversas são as abordagens sobre a classificação do sistema de informação. Padoveze (1997) menciona que os sistemas de informação podem ser classificados em duas categorias: (a) como suporte ao apoio às operações e (b) como suporte ao apoio à gestão. O sistema de informação de apoio às operações objetiva auxiliar na execução das funções operacionais, enquanto o sistema de informação de apoio à gestão está voltado para as informações necessárias para a gestão econômico-financeira das organizações.

Stair (1998) reforça a premissa de Padoveze (1997) ao classificar o sistema de informação em: (i) sistemas de processamento de transações (SPT); (ii) sistemas de informações gerenciais (SIG); (iii) sistemas de apoio à decisão (SAD); e (iv) sistemas especialistas (SE). O SPT é um conjunto organizado de pessoas, procedimentos, bancos de dados e dispositivos usados para registrar transações de negócios completadas. O SIG é um agrupamento organizado de pessoas, procedimentos, bancos de dados e dispositivos usados para oferecer informações de rotina aos administradores e tomadores de decisões. Estes fornecem relatórios pré-programados gerados com dados e informações do sistema de processamento de transações. O SAD é um grupo organizado de pessoas, procedimentos, bancos de dados e dispositivos usados para dar apoio à tomada de decisões relevantes para problemas específicos. O foco do SAD é a eficácia na tomada de decisões. Por outro lado, o SE é um agrupamento organizado de pessoas, procedimentos, bancos de dados e dispositivos usados para gerar um parecer especializado ou sugerir uma decisão em áreas ou disciplinas específicas.

Outra forma de classificação dos Sistemas de Informação é proposta por Schmidt (2002), em três níveis diferentes de administração das organizações: operacional, tático

e estratégico. O autor expõe que, para a tomada da decisão adequada, as informações devem estar sempre disponíveis a quem requer, em forma facilmente acessível e compreensível, em tempo hábil e a custo razoável. Caso contrário, sua utilização é inviável. Manter a informação prontamente acessível para utilização futura representa um dos principais objetivos de um sistema de informação. A Figura 1 apresenta a classificação de acordo com os níveis descritos.

Figura 1 - Níveis em que se apresenta a informação



Fonte: adaptado de Schmidt (2002, p. 83).

Os sistemas de informações operacionais constituem sistemas de processamento das transações que correm em paralelo aos fluxos físicos e acompanham o dia-a-dia das operações das empresas. Nesses sistemas encontram-se concentrações de dados para serem processados. Os sistemas de informações gerenciais fornecem subsídio às diversas áreas funcionais da organização e suportam as tomadas de decisões com o objetivo de identificar e corrigir problemas de competência gerencial, de processo de planejamento e de controle empresarial em nível gerencial. Os sistemas de informações estratégicos são constituídos por sistemas voltados ao suporte das decisões empresariais relacionadas com o mercado em que a organização está inserida (SCHMIDT, 2002).

Segundo Gil (1995), o sistema de informação contábil deve produzir informações que possam atender não apenas aos níveis empresariais acima relacionados, mas também aos aspectos do ciclo administrativo de planejamento, execução e controle. E, ainda, aos aspectos concernentes aos níveis de estruturação da informação. O autor classifica os níveis em estruturados, semi-estruturados e não-estruturados.

3.2 Sistemas integrados de informação contábil-financeira

A Contabilidade detém dados necessários às análises para as tomadas de decisões, portanto, o objetivo principal da Contabilidade é fornecer informação econômica relevante para que cada usuário possa tomar suas decisões e realizar seus julgamentos com segurança (IUDÍCIBUS, 2006). Desse modo, os sistemas de informações devem ser criados com o objetivo de apresentar os fluxos de informações

e estabelecer vinculações com o processo decisório da organização.

Padoveze (1997) destaca a importância da integração e navegabilidade dos dados. Para o autor, um sistema de informação contábil é considerado integrado quando todas as áreas necessárias para o gerenciamento da informação contábil estão abrangidas por um único sistema de informação e todos utilizam um mesmo sistema de informação. Acrescenta que o fator principal para caracterizar um sistema de informação contábil integrado é a navegabilidade dos dados, ou seja, quando os dados operacionais são coletados e disponibilizados para todos os segmentos da organização. Stair (1998) destaca a possibilidade de a integração sistêmica gerar eficiências organizacionais. A integração de sistemas envolve a determinação de quais sistemas devem ser combinados, quais devem estabelecer as ligações de comunicações e quais elementos adicionais são necessários para maximizar a atuação de todos os sistemas dentro de uma organização.

Barbosa (2003), citando Riccio (1989), afirma que a integração do sistema de informação contábil é possível mediante a utilização de interfaces entre os bancos de dados, de forma a permitir o acesso tanto do sistema de informação contábil para um outro banco de dados como em sentido inverso. Assim, aponta dois tipos de integrações necessárias: (1) funcional e (2) física. A integração funcional implica diferentes funções de suporte que sejam fornecidas por um único sistema. Por exemplo: comunicação com bancos de dados externos e manipulação de dados que possam ser acompanhados por várias estações de trabalho. A integração física refere-se ao empacotamento de hardwares, softwares, e comunicações requeridas para a realização da integração funcional.

Alguns dos benefícios que estes sistemas de informações proporcionam às empresas são: melhoria no acesso das informações; melhoria na produtividade; melhoria na tomada de decisões por meio do fornecimento de informações rápidas e precisas; estímulo à interação entre os tomadores de decisões; melhoria na estrutura organizacional ao facilitar o fluxo de informações; redução do grau de centralização de decisões na empresa; otimização da prestação dos seus serviços aos clientes; interação com fornecedores. Frezatti (1999) ressalta que a integração entre os sistemas de informações das organizações torna-os mais úteis e potencializa os benefícios às organizações.

3.3 Fraudes eletrônicas

De acordo com Gil (1996), as fraudes eletrônicas correspondem a uma ação prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física ou jurídica, com o objetivo de alcançar benefício ou satisfação psicológica, financeira ou material. A fraude é tanto mais perigosa quanto mais sofisticado for o meio usado para praticá-la (SÁ, 1982). Lago Junior (2001) afirma que a fraude eletrônica é considerada, entre todas as condutas

ilícitas, a invasão de rede de informação mais perigosa e temida, não apenas devido à sensação de insegurança que gera, mas também devido ao potencial danoso que representa para o sistema.

Para Nogueira (2001), alguns estudos afirmam que atualmente nenhuma nação do mundo tem a capacidade de promover plena eficácia à segurança da informação no espaço cibernético por si própria devido à transnacionalidade, volatilidade, velocidade e simultaneidade com que o hacker ataca. Novas regras, leis e procedimentos precisam ser criados para que os sistemas se tornem eficientes e viáveis.

Segundo Gil (1996), alguns fatores propiciam maior ocorrência de fraudes nos sistemas de informação contábil-financeira, como por exemplo, a intensa integração da informática em nível interno da organização que enfoque o conceito de segregação de funções. Outro fator é a qualificação profissional nas diversas áreas organizacionais com maior conhecimento da tecnologia. O autor afirma que políticas, diretrizes, objetivos e metas de controle são importantes para uma adequada tecnologia de controle das fraudes. Tais políticas devem reunir conceitos e práticas de controles lógicos em planos de contingência que fixem como diretriz a segurança contra fraudes.

Em um sentido prático, as principais formas de prevenção de fraudes eletrônicas se baseiam na existência de um bom controle interno e nas auditorias de sistemas. Para Gil (2000), a auditoria é a validação e a avaliação do controle interno de informações em processamento eletrônico de dados relacionado à fidelidade da informação quanto aos dados, à segurança física e lógica, confidencialidade, segurança ambiental, obediência à legislação em vigor, eficiência e eficácia e, ainda, quanto à obediência às políticas da alta direção da empresa. Portanto, a organização precisa ser cuidadosa com os controles na implementação de recursos de sistemas informatizados devido às facilidades oferecidas pelo computador para criar informações rapidamente, como também estabelecer mecanismos que permitam mapear as vulnerabilidades do sistema e realizar ações para saná-las.

3.4 Segurança da informação

A Associação Brasileira de Normas Técnicas (ABNT) é o Fórum Nacional de Normalização; em outras palavras, pode ser entendido como um código brasileiro de normas. O conteúdo destas normas é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CEET). As normas são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte produtores, consumidores e neutros (universidades, laboratórios e outros).

Em se tratando de segurança da informação, a ABNT publicou a NBR ISO/IEC 17799, 2005 como o código de referência para a gestão e segurança da informação. Segundo a ABNT, a informação é um ativo essencial para os negócios de uma

organização e necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades, possibilitando a manipulação de dados e, em conseqüência, fraudes.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. Os pilares da organização, de acordo com a ABNT NBR ISO/IEC 17799, 2005, devem ser avaliados e controlados de forma a evitar o acesso indevido, a manipulação dos dados sem o devido acompanhamento, as restrições dos sistemas de informação, dentre outros.

De forma resumida, apresentam-se, a seguir, alguns procedimentos que devem ser observados e implantados a fim de se estabelecer uma política de segurança. Tais procedimentos serão alvo de observação para aplicação deste estudo.

3.4.1 Conformidade legal

Violações aos direitos de propriedade intelectual podem conduzir a ações legais, que podem envolver processos criminais. Assim, procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e de uso de produtos de software proprietários como: (1) adquirir softwares por meio de fontes conhecidas para assegurar que o direito autoral não será violado; (2) manter os registros adequados para proteger os direitos de propriedade intelectual e notificar sobre as ações disciplinares que serão aplicadas às pessoas que violarem tais direitos; (3) manter provas e evidências da propriedade das licenças, discos-mestre, manuais; (4) implementar controles para assegurar que o número máximo de usuários permitidos não excederá aos da licença adquirida; (5) assegurar que somente softwares autorizados e licenciados serão instalados; (6) utilizar ferramentas de auditoria apropriadas; (7) cumprir termos e condições para utilização de softwares obtidos a partir de redes públicas; (8) não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral; (9) não copiar, no todo ou em parte, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Os direitos de propriedade intelectual incluem direitos de software ou documento, direitos de projeto, marcas, patentes e licenças de códigos-fonte. Produtos de software proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições da licença. Por exemplo, os contratos podem restringir o uso dos produtos ou limitar as cópias apenas por motivos de segurança (backup).

3.4.2 Cópias de seguranças

As cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente, além de verificar se há recursos adequados para restauração das cópias, se necessário.

Fatores diversos devem ser considerados para a geração das cópias de segurança, tais como: (1) produção de documentação apropriada sobre os procedimentos de restauração; (2) definição de uma freqüência de geração das cópias de segurança que reflita a necessidade de fato da organização, além dos requisitos de segurança envolvidos na criticidade da informação para a continuidade das operações da organização; (3) disponibilidade de meios para que as cópias sejam armazenadas em localidades remotas, com vistas a se distanciarem de desastres ocorridos no local das atividades principais da empresa; (4) testes regulares das cópias para garantir que as mesmas são suficientemente confiáveis para uso de emergência, quando necessário; (5); proteção das cópias por meio de criptografias em situações em que a confidencialidade é importante e imprescindível.

Em ambientes mais críticos, os mecanismos de cópias de segurança devem ser automatizados para facilitar os processos de geração e recuperação das cópias de segurança. Vale ressaltar, ainda, a importância de tais soluções automatizadas serem suficientemente testadas antes da implementação e serem verificadas em intervalos regulares.

3.4.3 Segregação de funções

A segregação de funções é um método para redução do risco de uso indevido acidental ou deliberado dos sistemas. É imprescindível tomar certos cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção. Convém que o início de um evento seja separado de sua autorização, atentando-se, ainda, para a possibilidade de existência de conluios.

As pequenas organizações podem considerar difícil de se implantar a segregação de funções, mas o seu princípio é sempre possível e praticável. Onde a segregação for difícil, convém que outros controles - como monitoração das atividades, trilhas de auditoria e acompanhamento gerencial – sejam aplicáveis. É importante que a auditoria de sistema permaneça como uma atividade independente. A intenção é que funções e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação ou de uso indevido ou não autorizado de dados e/ou informações.

3.4.4 Senhas de acesso

A senha é um dos principais meios de validar a autoridade dos usuários para acesso a serviços informatizados. Para gerenciamento de acessos aos sistemas de

informações, convém a utilização de identificador de usuário (ID de usuário) e senhas individuais a fim de lhes atribuir maiores responsabilidades. Além disso, o sistema deve permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo procedimentos de confirmação das mesmas e mecanismos para recomendar escolhas de senhas com qualidade.

Outros fatores que merecem destaque são: obrigação de trocas de senhas periodicamente, isto é, incluir procedimentos que estabeleçam prazos máximos de utilização das senhas; manter registros das senhas anteriormente utilizadas; bloquear a reutilização de senhas; não viabilizar a visualização das senhas na tela quando forem digitadas; armazenar os arquivos de senha separadamente dos dados do sistema e, se possível, mantê-la protegida por meios criptográficos.

3.4.5 Monitoramento

O uso de procedimentos de monitoramento é necessário para assegurar que os usuários executem somente atividades explicitamente definidas, bem como utilizem softwares autorizados. Além disso, o sistema de informação deve ser monitorado para detectar atividades não autorizadas de processamento da informação. Poderá, ainda, ser utilizado para avaliar a eficácia dos controles adotados e os acessos ao sistema.

3.4.6 Registros de sistema

Os registros no sistema contendo todas as atividades dos usuários devem ser produzidos e mantidos por um período de tempo suficiente para servir de auxílio a futuras investigações e monitoramento de controle de acesso. Tais registros devem permitir identificar: (1) usuários, datas, horários e detalhes de eventos-chave, como o horário de entrada (log-on) e de saída (log-off) no sistema; (2) terminais e sua localização geográfica; (3) registros de tentativas de acesso ao sistema; (4) registros de tentativas de acesso a outros recursos do sistema não permitido ao usuário detentor de senhas com acessos restritos; (5) alterações na configuração do sistema; (6) utilização de privilégios; (7) arquivos acessados e o tipo de acesso; (8) endereços e protocolos de rede; (9) alarmes provocados pelo sistema de controle de acesso; (10) ativação e desativação dos sistemas de proteção, tais como sistemas de antivírus e sistemas de detecção de intrusos e de firewall.

3.4.7 Controles criptográficos

O uso de controles criptográficos tem a finalidade de proteger a confidencialidade, a autenticidade e a integridade das informações por meios de códigos. O principal objetivo é evitar o acesso não autorizado aos sistemas por parte dos usuários. Esses recursos devem permitir: (1) autenticação de usuários autorizados conforme a política de controle de acesso definida pela empresa; (2) registro das tentativas de autenticação

no sistema com sucesso ou falha; (3) registro do uso de privilégios especiais do sistema; (4) disparo de alarmes quando as políticas de segurança do sistema são violadas.

3.4.8 Análise crítica independente

É necessário que o enfoque da organização para gerenciar a segurança da informação e a sua implementação seja analisado criticamente, de forma independente, em intervalos planejados e quando houver mudanças significativas no processo de implementação da segurança da informação. Tal análise crítica independente faz-se necessária para assegurar a contínua pertinência, adequação e eficácia da organização no gerenciamento da segurança da informação. Convém que a análise crítica inclua a avaliação contínua das oportunidades de se promover melhorias no sistema de segurança da informação e o estabelecimento de objetivos para otimizar os controles.

Nesse sentido, a análise crítica deve ser executada por pessoas independentes da área avaliada, como por exemplo, auditores internos, gerentes de outros setores ou organizações especializadas terceirizadas. Assim, é completamente imprescindível que as pessoas que realizem tal análise crítica possuam habilidade e experiência apropriadas. Os resultados da análise devem ser registrados e relatados para a direção que a iniciou. Se a análise crítica independente identificar que o enfoque da organização e a implementação para gerenciar a segurança da informação são inadequados ou não-conformes com as orientações estabelecidas pela segurança da informação, convém reforçar que a direção considere ações corretivas para assegurar maior efetividade nas políticas de segurança dos sistemas de informações.

4 Contextualização do cooperativismo de crédito

O cooperativismo é um processo associativo pelo qual os indivíduos aglutinam forças de produção, capacidade de consumo e poupanças para desenvolverem-se econômica, financeira e socialmente. O objetivo das cooperativas não é simplesmente constituir um conjunto de pessoas, mas focalizar o indivíduo através do conjunto de pessoas. Assim, as cooperativas representam uma forma de união de forças de vários pequenos produtores, conferindo-lhes condições de sobrevivência em meio aos grandes concorrentes.

As cooperativas buscam satisfazer as necessidades de consumo de bens ou serviços, além de contemplar as necessidades sociais e educativas. Representam uma sociedade criada por um pequeno grupo de pessoas que utilizam recursos individuais para constituir um capital coletivo que busca garantir as demandas próprias (GAWLAK e RATKE, 2001). Diferenciam-se dos demais tipos de sociedades por serem, ao mesmo tempo, uma associação de pessoas e um negócio. Por isso, tendem a conseguir melhores resultados em comparação às empresas convencionais ao equilibrarem dupla característica: aspecto social e aspecto econômico.

A livre adesão, a singularidade do voto e a distribuição de sobras financeiras caracterizam a cooperativa sob a perspectiva da natureza jurídica. Os valores e princípios do cooperativismo, segundo a Organização das Cooperativas Brasileiras (OCB), podem ser aplicados em todas as atividades econômicas. No Brasil existem cooperativas em diversos setores da economia, ocupando lugar importante na economia brasileira como instrumento de geração de emprego e distribuição de renda. De acordo com o Anuário do Cooperativismo Mineiro de 2006, o movimento cooperativista brasileiro, em 2005, apresentou os seguintes números, conforme apresentados no Quadro 1.

Quadro 1 - Movimento cooperativista brasileiro em 2005

Segmentos	Dezembro em 2005	
	Cooperativas	Cooperados
Agropecuária	1.514	879.918
Consumo	147	2.181.112
Crédito	1.101	2.164.499
Educação	319	73.951
Especial	10	529
Habitação	335	91.299
Infra-estrutura	160	600.399
Minérios	44	15.212
Produção	173	17.569
Trabalho	1.994	425.181
Saúde	899	287.868
Transporte	783	50.600
Turismo e Lazer	19	2.917
Totais	7.518	6.791.054

Fonte: Anuário do Cooperativismo Mineiro (2006).

No Brasil, o cooperativismo de crédito surgiu no início do século XX, com ações principalmente nos estados de São Paulo e Rio Grande do Sul. Em 1902, na localidade de Linha lmperial, município de Nova Petrópolis, Rio Grande do Sul, surgiu a primeira cooperativa de crédito da América Latina, criada pelo padre suíço Theodor Amstadt.

As cooperativas de crédito estão estruturadas nos termos de instituição financeira, porém constituídas por um grupo de pessoas, com forma e natureza jurídica própria, sem fins lucrativos e não sujeitas à falência. Quando um grupo de pessoas constitui uma cooperativa de crédito, o objetivo é propiciar crédito e prestar serviços de modo mais simples e vantajoso para seus associados. Caracteriza-se por ser sociedade de pessoas em que o associado tem prioridade, comprovada pelo fato de cada um ter um voto nas deliberações das Assembléias Gerais, independentemente do capital subscrito e integralizado por ele. Ao contrário das Sociedades Anônimas, em que os votos nas Assembléias Gerais são proporcionais ao montante do capital integralizado de cada sócio, pois a cota-parte do sócio tem papel secundário dada a preponderância da colaboração individual do cooperado.

Outra característica das cooperativas de crédito é a independência da autorização governamental. Nos termos do art. 5º, XVIII, da Carta Constitucional, a criação de associações cooperativas independe de autorização, sendo vedada a interferência estatal em seu funcionamento. As cooperativas de crédito são, basicamente, regulamentadas pela Lei nº 5.764, assim definindo a política nacional de cooperativismo e instituindo o regime jurídico das sociedades cooperativas. No entanto, a Resolução nº 2.788 do Conselho Monetário Nacional (CMN) dispõe sobre a constituição e o funcionamento de bancos comerciais e bancos múltiplos sob controle acionário de cooperativas centrais de crédito; a Resolução nº 3.321 do Conselho Monetário Nacional (CMN) trata dos requisitos e procedimentos para a constituição, a autorização para funcionamento e as alterações estatutárias, bem como para o cancelamento da autorização para funcionamento de cooperativas de crédito.

5 Apresentação e análise dos dados

O universo pesquisado foi definido através do Anuário do Cooperativismo Mineiro 2006: Maiores Cooperativas de Minas Gerais, publicado pelo Sindicato das Organizações Cooperativas de Minas Gerais /Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais - OCEMG/SESCOOP-MG.

As cooperativas selecionadas, do ramo de crédito, estão destacadas nesse Anuário seguindo os seguintes critérios de classificação: faturamento; ativo total; patrimônio líquido; número de empregados diretos e número de associados. Os dados referem-se ao ano de 2005. Este estudo selecionou apenas as cooperativas que se enquadram em algumas destas cinco variáveis, pois não necessariamente todas elas disponibilizam dados nas variáveis citadas.

Para a coleta de dados foi enviado um questionário para 43 (quarenta e três) cooperativas de crédito, obtendo-se 100% de retorno. Para o questionário foram elaboradas 10 (dez) perguntas fechadas, seguindo as principais técnicas de segurança de sistemas integrados como base para avaliação dos níveis de segurança adotados

em cooperativas de crédito, os quais objetivam a prevenção e a identificação de possíveis fraudes eletrônicas.

Na Figura 2, apresentam-se os gráficos da pesquisa empírica que identificam (1) controles em relação à utilização de softwares legalizados e/ou autorizados pelas Cooperativas de Crédito; (2) verificações periódicas nas máquinas para se certificar que somente softwares autorizados e licenciados pela cooperativa de crédito estão sendo instalados; (3) controles para proteção de dados contra perda dos dados e cópias de segurança; (4) softwares de proteção ao sistema de informação, como certificados digitais, dados criptografados e sistemas de firewall; (5) controles de segregação de função, bem como os níveis de acesso ao sistema; e (6) periodicidade das revisões de acessos, concedendo, restringindo e alterando senhas.

Na Figura 3, apresentam-se os gráficos da pesquisa para identificar (1) a tempestividade na concessão e exclusão de acesso em caso de admissão ou demissão; (2) a avaliação das ferramentas auxiliares do sistema como detecção de intrusos, inspeção de conteúdo e outras formas de monitoração; (3) o sistema integrado de informação contábil- financeira para identificar registros de usuário, dia, hora e todas as transações realizadas através de trilhas que possam ser rastreadas; (4) a periodicidade de testes de invasões e avaliações de vulnerabilidade realizados por profissionais independentes.

Percebe-se um alto nível de implementação de políticas de segurança de sistemas integrados de informação contábil-financeira nas cooperativas de crédito mineiras. Todas as variáveis analisadas foram avaliadas entre os níveis "bom" e "excelente", evidenciando que existe uma clara percepção da importância de tais medidas para a proteção do sistema de informação das entidades.

Uma consideração importante é que em nenhum dos quesitos analisados as cooperativas de crédito apontaram níveis inferiores ao "bom", o que reforça a adequação destes sistemas aos procedimentos considerados básicos. Nas questões relativas à legalidade dos softwares e à proteção de dados e cópias de segurança, os níveis de avaliação foram considerados "excelentes" na totalidade das cooperativas analisadas.

Com relação às verificações periódicas das máquinas para assegurar a utilização somente de softwares licenciados e/ou devidamente autorizados, à segregação de funções, à periodicidade das revisões de acessos e tempestividade para concessão ou restrição de acessos, à avaliação das ferramentas auxiliares do sistema para detecção de intrusos e inspeção de conteúdo, o nível considerado "excelente" fica entre 65% e 79%, demonstrando que a política de segurança do sistema é apropriada.

Os procedimentos que atingiram menor avaliação foram relativos à utilização de softwares de proteção, tais como: certificação digital, criptografia de dados e sistema de firewall; identificação, por parte do sistema de informação, de registros de usuário e transações realizadas; e periodicidade de avaliação de vulnerabilidades por parte de profissionais independentes, onde o nível "excelente" ficou abaixo de 40%.

Figura 2: Resultado da pesquisa empírica quanto a *softwares* legalizados, verificações periódicas das máquinas, proteção de dados, proteção do sistema de informação, segregação de função e acesso ao sistema.

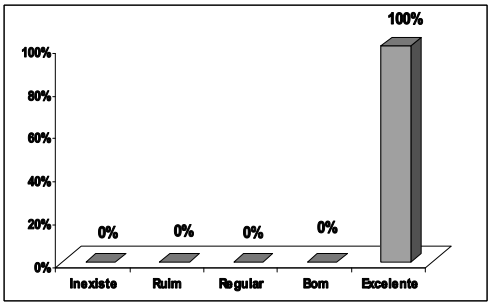


Gráfico 1: Nível de avaliação da utilização somente de *softwares* legalizados.

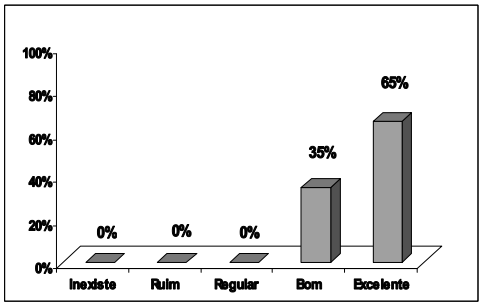


Gráfico 2: Nível de verificações periódicas nas máquinas para se certificar que somente *softwares* autorizados e licenciados pela cooperativa de crédito estão sendo instalados.

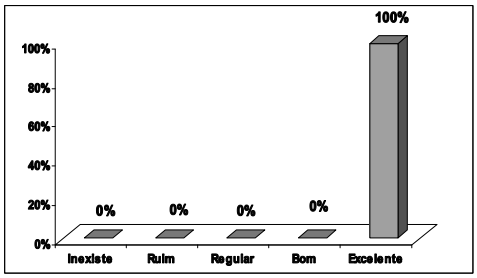


Gráfico 3: Nível dos controles para proteção de dados contra perda, destruição e/ou falsificação.

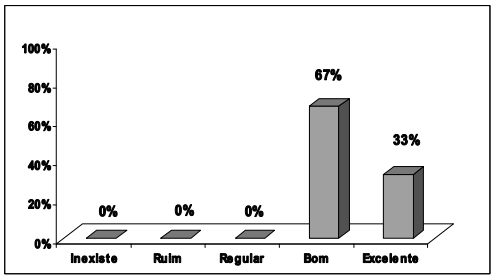


Gráfico 4: Nível de utilização de *softwares* de proteção ao sistema de informação, como certificados digitais, dados criptografados e sistemas de *firewall*.

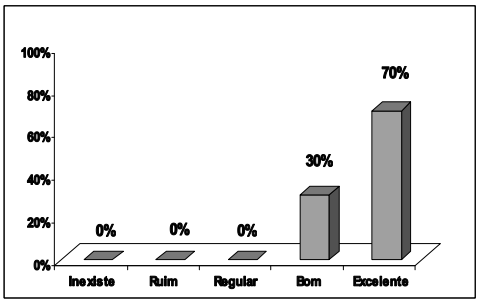


Gráfico 5: Nível dos controles de segregação de funções, bem como níveis de acesso ao sistema.

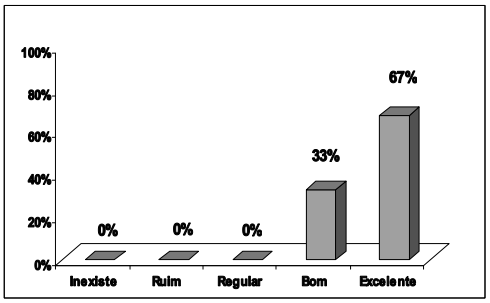


Gráfico 6: Nível das periodicidades das revisões de acessos, concedendo, restringindo e alterando senhas.

Fonte: Elaborado pelos autores.

Figura 3: Resultado da pesquisa empírica quanto à concessão e exclusão de acesso, ferramentas de detecção de intrusos, sistema integrado de informação contábil-financeira, periodicidade de testes de invasões.

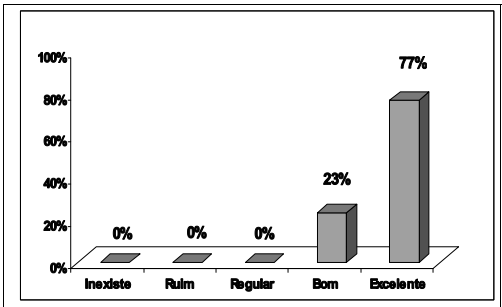


Gráfico 7: Nível de tempestividade na concessão e exclusão de acesso em caso de admissão ou demissão.

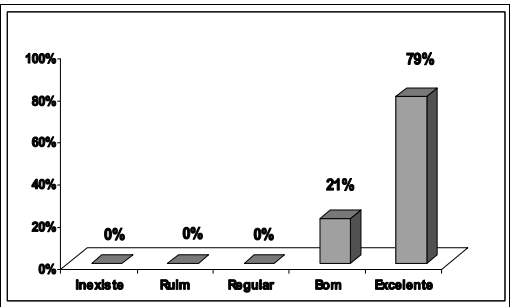


Gráfico 8: Nível das ferramentas auxiliares do sistema como detecção de intrusos, inspeção de conteúdo e outras formas de monitoração.

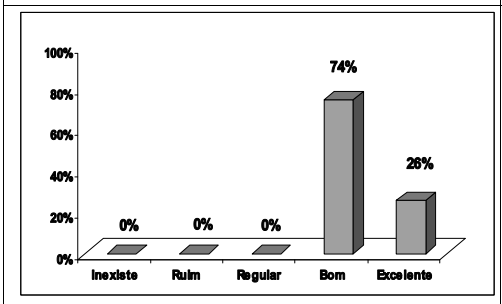


Gráfico 9: Nível de identificação pelo sistema integrado de informação contábil-financeira de registros de usuário, dia, hora e todas as transações realizadas através de trilhas que possam ser rastreadas.

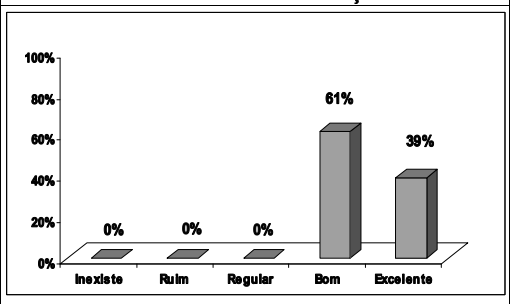


Gráfico 10: Nível da periodicidade de testes de invasões e avaliações de vulnerabilidade realizados por profissionais independentes.

Fonte: Elaborado pelos autores.

Diante dos dados apresentados, observa-se que os procedimentos de segurança dos sistemas integrados de informação contábil-financeira das cooperativas de crédito analisadas estão em níveis satisfatórios. Entretanto, em se tratando de segurança da informação, pode-se afirmar que não existe segurança 100%, mas sim procedimentos que, se adotados, reduzem as possibilidades de utilização inadequada.

6 Conclusões

A evolução tecnológica possibilitou que muitos processos e atividades sejam absorvidos pelos sistemas informatizados simplificando, organizando e agilizando todas

as atividades internas e externas das organizações.

Os sistemas integrados de informação contábil passaram a representar um ativo intangível valiosíssimo para as entidades e, com o aumento da interconectividade, a informação está exposta a perigosas ameaças e vulnerabilidades. Neste cenário de processamento eletrônico de dados, as possibilidades de ocorrência de fraudes eletrônicas, em virtude das fortes transformações no processamento da informação, causadas por avançadas tecnologias, sistemas de comunicação e inúmeras trocas de dados, passaram a ser uma realidade, razão por que a implementação de políticas de segurança dos sistemas de informação é extremamente necessária.

Em função dessa realidade, o objetivo do estudo foi conhecer o grau de segurança aplicado nos sistemas de processamento eletrônico de dados como forma de proteção contra fraudes eletrônicas no âmbito das Cooperativas de Crédito de Minas Gerais. O estudo realizado nas maiores cooperativas de crédito mineiras permite concluir-se que há um elevado nível de segurança dos sistemas de informação contábil em virtude dos altos níveis de implementação dos procedimentos básicos de segurança estabelecidos pelas normas.

Por fim, o cooperativismo de crédito mineiro, de certa forma, está se adequando aos requisitos básicos de segurança em seus sistemas integrados de informação contábil-financeira. Pode-se considerar como outro fator desta adequação sua regulamentação pelo Banco Central, onde todos os processos e procedimentos são padronizados e pré-estabelecidos para as instituições financeiras, além da obrigatoriedade de auditorias externas regulares que, de certa forma, contribui para minimizar as possibilidades de fraudes eletrônicas. Mas, embora a obrigatoriedade exista, acredita-se que, quanto maior a confiança no sistema, menor será a aplicação de controles de prevenção de fraudes em meios eletrônicos.

Referências

ABNT, NBR 17799:2005.Tecnologia da Informação: código de prática para a gestão da segurança da informação. ABNT, 2005.

BARBOSA, Alexandro. **Avaliação dos sistemas integrados de informação contábil das fundações de apoio vinculadas às instituições federais de ensino superior:** um estudo de caso no nordeste do Brasil. 2003. Disponível em: <http://www.unb.br/cca/pos-graduacao/mestrado/dissertacoes/mest_dissert_022.pdf> Acesso em: 14 jan. 2007.

BRASIL. Constituição. **Constituição da República Federativa do Brasil,** 1988. Brasília: Senado Federal, centro gráfico, 1988. Disponível em: <http://www.planalto.gov.br/>. Acesso em: 22 out. 2006.

BRASIL. Lei Ordinária. **Lei Ordinária nº 5.764**, 1971. Brasília: Senado Federal, centro

gráfico, 1971. Disponível em: <http://www.planalto.gov.br/>. Acesso em: 16 set. 2006.

CRUZ, Tadeu. **Sistemas de informações gerenciais**: tecnologias da informação e a empresa do século XXI. 2. ed. São Paulo: Atlas, 2000.

FREZATTI, Fábio.**Orçamento empresarial:** planejamento e controle gerencial. São Paulo: Atlas, 1999.

GAWLAK, Albino e RATZKE, Fabianne. **Cooperativismo: filosofia de vida para um mundo melhor**. 3. ed. Belo Horizonte: ? ,2001. 115 p.

GIL, Antônio de Loureiro. **Auditoria de computadores.** 5. ed. São Paulo: Atlas, 2000. 236 p.

_____. **Fraudes informatizadas.** São Paulo: Atlas, 1996. 202 p.

_____.**Sistemas de informações contábil/financeiros.** São Paulo: Atlas, 1995. 203 p.

IUDÍCIBUS, Sérgio de. **Teoria da contabilidade.** 6. ed. São Paulo: Atlas, 2006.

LAGO JÚNIOR, Antônio. **Responsabilidade civil por atos ilícitos na internet**. São Paulo: LTR, 2001. 127 p.

MAIORES COOPERATIVAS DE MINAS GERAIS. **Anuário do cooperativismo mineiro.** Ano 2006.

NOGUEIRA, José Helano Matos. Um tribunal cibernético? **Perícia Federal**, n. 9, p. 20, jun 2001.

ORGANIZAÇÃO DAS COOPERATIVAS BRASILEIRAS - OCB. Site (2006) **O cooperativismo.** Disponível em: <http://www.ocb.org.br/>. Acesso em: 22 abr. 2006.

PADOVEZE, Clóvis Luís. **Contabilidade gerencial:** um enfoque em sistema de informação contábil. São Paulo: Atlas, 1997.

RICCIO, Edson Luiz. **Uma contribuição ao estudo da contabilidade como sistema de informação.** Tese (Doutorado em Administração). Faculdade de Economia, Administração e Contabilidade. Universidade de São Paulo, São Paulo, 1989.

SÁ, Antônio Lopes de. **Fraudes contábeis.** Rio de Janeiro: Ediouro, 1982.

SCHMIDT, Paulo. **Controladoria: a**gregando valor para a empresa. Porto Alegre: Bookman, 2002.

STAIR, Ralph M. **Princípios de sistemas de informação:** uma abordagem gerencial. Rio de Janeiro: LTC, 1998.

Artigo recebido em: Maio de 2007 e
Artigo aprovado para publicação em: Julho de 2007.

Endereço dos autores

Adélio Carlos de Andrade
adelioandrade@bol.com.br

Rua Henrique Gorceix, 2110 – Apto. 203 – Caiçara
Belo Horizonte – MG – Brasil
CEP 30720-360

Flávia Cristina Alves Sousa
flaviacrisas@hotmail.com

Rua Içana 118 – Apto. 302 – Nova Suíça
Belo Horizonte – MG – Brasil
CEP 30460-220

Romualdo Douglas Colauto
rdcolauto@face.ufmg.br

Rua Curitiba 832 – Sala 703 – Centro
Belo Horizonte – MG – Brasil
CEP 30170-120

Laura Edith Taboada Pinheiro
ltaboada@face.ufmg.br

Rua Curitiba 832 – Sala 703 – Centro
Belo Horizonte – MG – Brasil
CEP 30170-120