AUDITORIA DOS SISTEMAS DE INFORMAÇÃO COM FOCO NOS CONTROLES DE RISCOS

João Arlindo do Prado Gusmão[1]

RESUMO: O objetivo deste artigo é identificar a relevância e influencias dos riscos no uso das técnicas de auditoria em sistemas de informação para uma melhor gestão dos negócios informatizados, especialmente sob o aspecto da percepção e controle de riscos. Aplicou-se a metodologia de pesquisa empírica, com uso do método conhecido como levantamento de dados transversal, também chamado estudo transversal que é um tipo de pesquisa que envolve a coleta de informações de uma dada amostra de elementos da população somente uma vez. A população da pesquisa foram os analistas de sistemas responsáveis pela implantação de sistemas e informação vinculados a empresas cadastradas como fornecedoras de programas aplicativos de automação na Secretaria da Fazenda de Goiás. A coleta de dados foi realizada por meio de um questionário, de onde se obtiveram respostas de 17 analistas, tornando-se esta a amostra do estudo. Os resultados apontam a alta influência dos riscos, sejam eles inerentes, de controle ou de detecção, num ambiente informatizado quanto à possibilidade de que um ou mais elementos da integridade, disponibilidade ou confidencialidade da informação ou do procedimento sejam comprometidos, tornando imprescindível sua identificação e uso correto de controles. Entretanto, para que estes controles sejam eficientes e eficazes, precisam estar adequados ao seu grau de relevância em relação ao risco a que está vinculado. Pela pesquisa de campo evidenciou-se que os controles sobre os riscos possuem graus de relevância diferentes, com destaque para os controles que usam recursos manuais que obtiveram o menor grau de relevância.

PALAVRAS-CHAVE: Técnicas de Auditoria. Controle de Riscos. Sistema de Informações.

1 CONSIDERAÇÕES INICIAIS

Este estudo objetiva oferecer abordagens úteis sobre a importância e utilidade das técnicas de auditoria em sistemas de informação para uma melhor gestão dos negócios informatizados, especialmente sob o aspecto da percepção e controle de riscos.

Cada vez mais se torna necessária a utilização da auditoria nos sistemas informatizados para o desenvolvimento de uma boa sistematização do processo de identificação e controle de riscos em ambientes computacionais operacionais e de gestão utilizados pelas empresas, em virtude do aumento de falhas e crimes relacionados com o uso de sistemas de computadores. (ELEUTÉRIO, 2011 p. 17).

[1] Bacharel em Ciências Contábeis, pela UCDB e Sistemas de Informação, pela UEG, MESTRE em Administração (Mercado/Finanças), pela Faculdade Alves Faria - ALFA, Pós-Graduações (Lato Sensu) em "Auditoria e Perícia Contábil", pela UCDB e "Informática Pericial", pelo IPOG. Professor Universitário (Graduação e Pós-Graduação) de Perícia Contábil e outras disciplinas nos cursos de Ciências Contábeis e Administração das Faculdades UNIFAN, FNG e FACMAIS. Auditor Fiscal da Secretaria da Fazenda do Estado de Goiás em exercício interno na Gerência de Inteligência e Informações Econômico-fiscal - GIEF.

Conforme Eleutério (2011, p. 15), com o avanço tecnológico houve uma mudança significativa na dinâmica comercial dos contribuintes, que vêm aumentando em suas atividades a utilização de diversos equipamentos e sistemas informatizados, quer por adequação mercadológica quer por obrigação legal, tais como: computadores, emissores de cupom fiscal, terminais autônomos de venda, máquinas leitoras de cartão de crédito, leitor de código de barra, programas aplicativos e, principalmente, de sistemas de banco de dados, mudando a forma de armazenamento das informações de dados físicos documentais para dados digitais eletrônicos.

Deste modo, considerando-se que "a auditoria em ambiente de tecnologia de informação não muda a formação do auditor" (IMONIANA, 2008, p. 16), o auditor nas empresas depara-se com uma quebra de paradigmas, pois se observa que o computador vem ficando mais frequentemente relacionado ao *modus operandi* de falhas e crimes que afetam as operações e gestão das empresas (ELEUTÉRIO, 2011, p. 17).

Em virtude disso, também, vem-se mudando rapidamente a atuação do auditor, diminuindo a quantidade de informações físicas documentais tais como: notas fiscais, livros contábeis e fiscais em papel e aumentando a quantidade de dados e informações digitais eletrônicas tais como: nota fiscal eletrônica, memórias fiscais, memória de fita detalhe, livros contábeis e fiscais digitais, controles gerenciais e paralelos digitais.

Diante desse contexto, as empresas precisam enfrentar o desafio de como se adequar a esta nova realidade, tendo de encontrar meios eficientes e eficazes de identificação e controle desses destes riscos em seu sistema de informação utilizando técnicas de auditoria aplicadas a um ambiente operacional e de gestão informatizado.

Para compreender mais claramente o nível de percepção dos riscos, bem como a utilização de controles e a importância de auditoria nos sistemas de informação operacional e de gestão das empresas, foi aplicada a metodologia de pesquisa empírica do tipo qualitativa, e, visto ter a intenção de obter informações gerais sobre o assunto, utilizou-se o método exploratório para atingir esse objetivo (MENDOÇA *et al.,* 2008, p. 41).

O universo, ou população, da pesquisa foram os analistas de sistemas responsáveis pela implantação de sistemas e informação vinculados a empresas fornecedoras de sistemas, de todo o território nacional brasileiro, cadastradas como fornecedores de programas aplicativos de automação na Secretaria da Fazenda de Goiás e que atuam em empresas comerciais e industriais do norte goiano. A escolha deste grupo levou em conta o conhecimento técnico sobre o assunto e a responsabilidade legal ocasionada pelo fato de o

fisco Goiano os considerar solidariamente responsáveis por falhas ou crimes relacionados ao sistema de informação. Segundo Cervo, Bervian & Da Silva (2007, p. 66) "população pode referir-se a um conjunto de pessoas, de animais ou de objetos que representem a totalidade de indivíduos que possuam as mesmas características definidas para o estudo".

Para alcançar o objetivo de obter informações dos participantes, o presente estudo optou pelo método conhecido como levantamento de dados transversal, também chamado estudo transversal que é "[...] um tipo de pesquisa que envolve a coleta de informações de uma dada amostra de elementos da população somente uma vez." (MALHOTRA, 2006, p. 102)

A coleta de dados foi realizada por meio de um questionário que, segundo Lakatos e Marconi (2007, p. 111) é "constituído por uma série de perguntas que devem ser respondidas por escrito e sem a presença do pesquisador". A opção por este método de coleta de dados se deu em virtude da pouca disponibilidade de tempo dos membros do grupo pesquisado. Conseguiu-se contatar e coletar as respostas de 17 analistas, tornando-se esta a amostra do estudo.

2 SISTEMAS DE INFORMAÇÃO DE APOIO OPERACIONAL E GERENCIAL

Em sentido amplo os sistemas de informação "são considerados mecanismos que permitem acesso às informações neles registradas, informações cognitivo-sociais, que incluem as estruturas de conhecimento partilhadas por membros de um grupo social." (GONÇALVES; RICCIO, 2009, p. 5) Onde sistema, neste caso, é um grupo de elementos que se relacionam com uma finalidade: produzir controles internos que auxiliarão as decisões gerenciais. (IMONIANA, 2008, p. 16)

Vê-se que o conceito de sistemas de informação é bastante amplo. No entanto, os sistemas de informação considerados neste estudo são os sistemas em que, segundo Gonçalves & Riccio (2009, p. 6), os dados, entendidos como pedaços de informação, são processados com o uso de computadores por meio de *softwares*, e que para serem automatizados precisam possuir estruturas bem definidas e serem agrupados no que é conhecido como banco de dados.

Originalmente, os sistemas de informação eram utilizados basicamente para a automação de atividades repetitivas e estruturadas. No entanto, atualmente são amplamente utilizados para produção de informações vitais ao processo gerencial e estratégico.

(GONÇALVES; RICCIO, 2009, p.17) Diante disto, um plano estratégico deve estar vinculado a um planejamento dos sistemas de informação, visto que, para sobreviver em uma sociedade da informação em constantes mudanças, as empresas precisam de inteligência e o conceito de inteligência empresarial está diretamente vinculado a um bom planejamento dos sistemas de informação. (REZENDE, 2003, p. 59)

O objetivo desses sistemas de informação é gerar informações adequadas e importantes para uma determinada finalidade. Sendo, portanto, como comenta CORNACHIONE JÚNIOR (2001, p. 28), "um conjunto de recursos que visa à produção de informações oportunas com base em dados específicos, valendo-se de processos previamente definidos."

As informações corretamente estruturadas colaboram para o dinamismo da empresa, pois informações adequadas em tempo hábil influem numa eficaz tomada de decisão gerencial ou controle operacional. Estas informações podem ser operacionais ou gerenciais. Informação operacional é a relacionada com a execução de uma função ou operação, enquanto que informação gerencial é o grupo de informações operacionais disponíveis a um gerente que lhe possibilite tomar uma decisão, ambas fazendo parte do controle interno da empresa. (CASSARRO, 2010, p. 34)

Uma vez que um sistema de informação é utilizado para conseguir informações úteis em tempo hábil, e estas informações são conjuntos de dados organizados (CASSARRO, 2010, P. 35) armazenadas em bancos de dados, torna-se clara a sua importância, visto que "a base estrutural para se obter um bom sistema de informações é possuir um bom banco de dados." (CORNACHIONE JÚNIOR, 2001 p. 31)

Entende-se que informação é todo dado processado, com valor de significância agregada a ela e com utilidade para seu usuário. Já o dado é um elemento da informação, um grupo de letras, números ou dígitos guardados, que, analisados separadamente, não possuem significado claro. Sendo o processamento o trabalho que transforma o dado em informação, como demonstrado no diagrama abaixo. (REZENDE, 2003, p. 61)

Dados → Processamento → Informações

Por muito tempo, os sistemas vinculados ao processamento computacional de informações e os sistemas de apoio gerencial foram tratados distintamente. Embora sejam conceituados separadamente, não devem ser entendidos como duas classes distintas de

sistema, visto que as informações geradas pelo processamento de dados e armazenadas nos bancos de dados transacionais da empresa são as que servem ao apoio gerencial.

Assim fica claro que é com o uso de bons sistemas de informações que as empresas mantêm um controle interno eficiente (GONÇALVES; RICCIO 2009, p.13). Diante disso, vê-se que o sistema de informação de apoio operacional e gerencial faz a interação da tecnologia da informação com os usuários, com o objetivo de informar e dar suporte à parte operacional e administrativa da organização, auxiliando a tomada de decisão e o controle em todos os níveis da administração. Este sistema tem como componentes básicos Hardware, Software, Banco de dados e Procedimentos.

3 FUNDAMENTOS DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Este tipo de auditoria apresenta um amplo campo de atuação devido à popularização dos sistemas informatizados e, quanto a seu objetivo, Castro e Lima (1999, p.70) entendem que é "assegurar a adequação, privacidade dos dados e informações oriundas dos sistemas eletrônicos de processamento de dados, observando as diretrizes estabelecidas e a legislação específica".

Na execução do trabalho de auditoria o auditor poderá encontrar controles internos processados computacionalmente. Será necessário, portanto, um bom conhecimento deste sistema informatizado para que haja uma correta avaliação destes controles e para execução de testes nos dados encontrados. Será também preciso entender corretamente, em todos os seus aspectos, quais são os principais objetivos do sistema geral do controle interno informatizado, visando "salvaguardar o ativo da organização, manter a integridade, correção e confiabilidade dos registros contábeis, promover a eficiência operacional e encorajar o cumprimento dos procedimentos e políticas da gerência." (IMONIANA, 2008, p. 41)

Para atingir este fim, o auditor muitas vezes recorre a um "especialista em PED (Processamento Eletrônico de Dados) para completar o seu entendimento e avaliação do controle interno daquela companhia" (CASTRO; LIMA, 1999, p. 16). Porém, em alguns trabalhos onde o sigilo é fundamental, o auditor deve ter capacidade de executá-lo, valendo-se apenas de consultas técnicas desvinculadas do trabalho em execução.

"Esse entrosamento da área contábil com o PED torna-se cada vez mais indispensável, uma vez que a grande maioria das organizações já está utilizando controles por Processamento Eletrônico de Dados". (CASTRO; LIMA, 1999, p. 16). Para Attie (1998, p.

63) a utilização do sistema informatizado pela organização altera a forma de processamento e armazenamento de informações, afetando a organização e os procedimentos adotados pela entidade na realização de adequados controles internos. Neste contexto conclui-se que:

O auditor deve dispor de compreensão suficiente dos recursos de PED e dos sistemas de processamentos existentes, a fim de avaliá-los e planejar adequadamente seu trabalho. O uso de técnicas de auditoria que demandem o emprego de recursos de PED requer que o auditor os domine completamente, de forma a implementar os próprios procedimentos ou, se for o caso, orientar, supervisionar e revisar o trabalho de especialistas." (ATTIE,1998, p.63).

Como visto até agora, é, geralmente, com o uso sistemas de informações que as empresas mantêm seu controle interno, gerencial e operacional. Nestes casos o auditor terá que efetuar um levantamento minucioso no sistema de informação, englobando a contabilidade e o controle interno, tornando possível, com isso, atingir três objetivos: uma correta análise, definir quais normas de auditoria deverão ser aplicadas e o melhor momento da execução. Assim, nestes casos, a análise do controle interno em uma auditoria envolve um bom conhecimento dos sistemas de informação em que este controle está inserido. (GUIMARÃES, 2002, p. 149)

Com base nisso, concluímos que não haveria informações se não existissem dados a serem processados. Embora os dados não sejam a informação propriamente dita, eles são uma representação física e dividida de características de objetos do mundo real, armazenados nos bancos de dados dos sistemas de informação (GONÇALVES & RICCIO 2009, p. 22) Portanto, conforme Machado e Abreu (2004, p. 1), "o dado é uma representação, um registro de uma informação". Este conceito é fundamental em auditorias, pois quaisquer alterações nestes dados afetarão diretamente a informação gerada pelo sistema que será usada operacional ou gerencialmente.

Uma vez que ficou clara a importância da informação como um elemento fundamental para tomada de decisões gerenciais e controle operacional da empresa em todos os seus processos e, visto que as empresas estão cada vez mais dependentes das tecnologias de informação, estas precisam proporcionar confidencialidade, integridade e disponibilidade. (LAUREANO; MORAES, 2005, p.4)

Precisa-se constantemente controlar os riscos de segurança dos sistemas de informação. Isso pode ser feito através de auditorias que visem a análise detalhada e rigorosa de equipamentos, programas, funções e procedimentos. Estas têm como objetivo determinar com que eficiência e eficácia o sistema como um todo está funcionando, principalmente com

relação à garantia de fatores como confidencialidade, integridade e disponibilidade da informação. (CAMPOS, 2007, p.17)

Os sistemas de informação, segundo Freitas (2013, p. 30), devem guardar a fonte original da informação que pode ser nova, alterada ou vir a ser apagada. O registro histórico destas operações recebe nome de trilhas de auditoria, contendo o usuário, a data da operação, o objeto da operação e o tipo de operação e visam o controle de riscos da informação.

Algumas razões que tornam as trilhas de auditoria necessária são:

• informações relevantes;

• responsabilização;

• detecção de comportamento suspeito. (FREITAS, 2013. p. 30).

Segundo Castro & Lima (1999, p.252), essas são algumas considerações importantes para uma eficiente e eficaz auditoria de sistemas de informação.

4 CONSIDERAÇÕES SOBRE RISCOS

Os gestores de negócios das empresas quase nunca compreendem os riscos pelos quais passa a informação em um sistema de informação. Conhecer os tipos de riscos e seus principais - e possíveis - mecanismos de controle, ajudará os gestores a compreender a necessidade da segurança da informação e da gestão de riscos. E mostrará como a auditoria de sistemas é uma importante ferramenta na verificação de riscos, vulnerabilidades e controle destes riscos. (FREITAS, 2013, p. 30)

Conforme a NBR 17799/2003, os princípios básicos para que uma informação seja considerada segura, são:

Integridade: propriedade de salvaguarda da exatidão e da totalidade do conjunto de ativos.

Disponibilidade: propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

A ideia de risco num ambiente informatizado aparece com a possibilidade de que um ou mais elementos da integridade, disponibilidade ou confidencialidade da informação ou do procedimento sejam comprometidos. É fundamental conhecer estes riscos para garantir a segurança da informação. (CAMPOS, 2007, p.29)

Cita-se a seguir riscos que devem ser avaliados de acordo com Castro & Lima (1999, p. 252):

Risco Inerente. A tendência das demonstrações financeiras a erros ou irregularidades relevantes, antes de se analisar a eficácia dos sistemas de controle.

Risco de Controle. É o risco de falhas no sistema de controle em relação à prevenção ou identificação, em tempo hábil, de erros ou irregularidades significativas.

Risco de Detecção. É o risco da não descoberta de um eventual erro de irregularidade relevante pelos procedimentos de Auditoria utilizados. Este risco pode ser reduzido, se houver o devido zelo e habilidade profissional, que pode ser conseguida através de um bom planejamento, supervisão e revisão.

Na tabela 1 indica os resultados da pesquisa que fizemos sobre a relevância de riscos inerentes, de controle e de detecção relacionados com sua influência em um ambiente de sistema de informação quanto ao comprometimento de elementos da integridade da informação ou do processamento. O maior percentual foi dos que consideraram os riscos inerentes e de detecção como de alta relevância e o risco de controle como de média/alta relevância. No entanto, quanto aos riscos de controle e detecção não foi, em nenhum caso, considerado como de baixa relevância.

Tabela 1 – Grau de influência dos riscos em um sistema de informação

	Baixa Influência	Média Baixa Influência	Média Alta Influência	Alta Influência	Total de Respostas	Avaliação Maior %
Risco Inerente	17,65% 3	17,65% 3	29,41% 5	35,29% 6	17	Alta Influência
Risco de Controle	0% 0	23,53% 4	41,18% 7	35,29% 6	17	Média/Alta Influência
Risco de Detecção	0% 0	29,41% 5	35,29% 6	35,29% 6	17	Alta Influência

Fonte: Organizada pelos autores

Torna-se cada vez mais necessário que os auditores, visando o bom cumprimento de suas atividades, tenham um bom conhecimento das tecnologias e das implicações de risco e controles decorrentes, visto que o uso da tecnologia da informação apresenta riscos para a integridade da informação e do processamento, riscos estes que necessitam ser reduzidos por meio de inserção de controles, preferencialmente, de baixo custo (CASTRO; LIMA, 1999, p. 253). Estes controles precisam ser revisados pelos auditores para confirmar sua presença e funcionamento contínuo.

5 CONSIDERAÇÕES SOBRE CONTROLES EM AMBIENTES INFORMATIZADOS

Um ambiente informatizado nunca é totalmente seguro. Mesmo que se use todo recurso tecnológico de segurança, sempre vai haver o elemento humano. E mesmo usando-se as melhores e mais eficientes ferramentas de controle, nem todos os riscos e as vulnerabilidades são conhecidas em um momento específico no tempo, dificultando a aplicação de controles específicos. (FREITAS, 2005, p. 34)

No entanto, o reconhecimento e a análise de riscos relacionados aos ambientes específicos de sistemas devem servir de referência para implementação de controles harmônicos com o nível de risco detectado. Neste campo, a relação custo/benefício do controle deve ser considerada uma questão gerencial. (CASTRO; LIMA 1999, p. 253)

Estes controles devem diminuir, a níveis aceitáveis, os riscos relacionados a fatores como o grau de ameaça, grau de vulnerabilidade e de se envolver, direta ou indiretamente, a integridade, disponibilidade e confidencialidade da informação e do processamento. (CAMPOS, 2007, p. 28).

Para isso, devem-se analisar os seguintes aspectos que podem didaticamente ser utilizados para evidenciar a integridade da informação (CASTRO; LIMA, 1999, p. 253):

Autorizado. Um dado de informação, desde uma operação até um sistema inteiro, é corretamente inserido, desenvolvido, modificado ou usado, com a respectiva autorização.

Exato. Os processos relacionados e a informação são precisos e podem ser utilizados para o fim que foi criado.

Completo. Todas as informações necessárias estão presentes. Não há duplicidade de informação. As operações rejeitadas são localizadas, controladas e novamente inseridas corretamente.

Oportuno. O trabalho é rapidamente processado.

Tempestividade. Processado, registrado e relatado em prazo suficiente.

Seguro. Há proteção contra acesso, atualização, revelação ou destruição não autorizada da informação e dos processos.

Existe uma relação complexa entre os riscos e os controles. Para se diminuir um risco, talvez diversos controles sejam necessários ou um só controle seja suficiente para diversos riscos. Este controle utiliza-se do limite lógico, ou seja, confirmação da exatidão dos dados e dos testes de racionalidade que verificam a autenticidade de uma informação (IMONIANA,

2008, p. 49). Necessita-se, portanto, considerar os riscos e controles no conjunto do sistema total de controle interno.

Todas as atividades dos sistemas, incluindo as do ambiente, da aplicação e as das áreas do usuário, devem ser englobadas pelo sistema de controle interno.

Veja segundo Castro & Lima (1999, p. 253) os controles gerais que estão incluídos nos sistemas de aplicação inseridos no ambiente geral da informação:

- Associação adequada do sistema de informação;
- Controles sobre o equipamento, o sistema operacional e os outros programas do sistema;
- Métodos de controle de mudança e alterações dos sistemas;
- Controle para acessos autorizados.

Tabela 2 - Grau de importância dos controles num sistema de aplicação

Importância/ Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Organização adequada do sistema de informação.	0% 0	0% 0	29,41% 5	70,59% 12	17	Alta Importância
Controle sobre os computadores, os sistemas operacionais ou outros programas do sistema.	11,76% 2	0% 0	47,06% 8	41,18% 7	17	Média/Alta Importância
Procedimentos de controle de alterações dos sistemas.	0% 0	17,65% 3	17,65% 3	64,71% 11	17	Alta Importância
Controles de acesso.	5,88% 1	11,76% 2	23,53% 4	58,82% 10	17	Alta Relevância

Fonte: Organizada pelos autores

6 PRINCIPAIS RISCOS EM SISTEMAS DE INFORMAÇÃO COMPUTADORIZADOS E POSSÍVEIS CONTROLES

Descrevem-se, de acordo com Castro e Lima (1999, p. 254), alguns riscos e dicas dos respectivos controles que podem nortear uma eficaz Auditoria dos Sistemas Informatizados:

RISCO 1 - pessoas não autorizadas com acesso às operações do sistema ou manuseio dos arquivos, com permissões que possibilitem ler, modificar, incluir ou apagar informações ou escrever informações não autorizadas para processamento. (LAUREANO; MORAES, 2005, p.4)

Possíveis controles:

- Criação de regras de acesso, tais como uso de senhas;
- Criar painéis com definições de perfis de acesso;
- Instalar programas de monitoramento de acesso à rede corporativa.

Tabela 3 - Relevância controles para o risco de acesso não autorizados

Relevância / Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Regras de acesso.	0 % 0	11,76% 2	11,76% 2	76,47% 13	17	Alta Relevância
Menus com perfis de acesso.	0 % 0	11,76% 2	29,41% 5	58,82% 10	17	Alta Relevância
Programas de controle de acesso.	0 % 0	11,76% 2	29,41% 5	58,82% 10	17	Alta Relevância

Fonte: Organizada pelos autores

RISCO 2 – Erro de digitação dos dados para processamento ou duplicidade de digitação. (LAUREANO; MORAES, 2005, p.4)

Possíveis controles:

- Solicitar repetição da digitação;
- Controlar o formato específico para um dado;
- Indicar campos faltantes, impedindo sequencia de ação até a correção;
- Controlar o tamanho limite de um campo;
- Controlar a validação que determine a exatidão lógica da informação;
- Controlar o processamento repetitivo;
- Testar a correlação de campos;
- Controles de balanceamento;
- Verificar dígitos de controle;
- Realizar verificação manual.

Tabela 4 - Relevância dos possíveis controles para o risco dos dados digitados para processamento serem inexatos.

Relevância / Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Controlar Dupla digitação.	17,65% 3	11,76% 2	11,76% 2	58,82% 10	17	Alta Relevância
Controlar o formato para um dado.	0% 0	11,76% 2	41,18% 7	47,06% 8	17	Alta Relevância
Controlar campos faltantes.	11,76% 2	17,65% 3	23,53% 4	47,06% 8	17	Alta Relevância
Controlar limite ou razoabilidade.	11,76% 2	23,53% 4	47,06% 8	17,65% 3	17	Média/Baixa Relevância
Controlar validação	0% 0	6,25% 1	25% 4	68,75% 11	16	Alta Relevância
Controlar processamento em duplicata.	5,88% 1	23,53% 4	11,76% 2	58,82% 10	17	Alta Relevância
Realizar testes de combinação ou correlação de campos.	5,88% 1	35,29% 6	11,76% 2	47,06% 8	17	Alta Relevância
Controlar balanceamentos.	17,65% 3	11,76% 2	52,94% 9	17,65% 3	17	Média/Alta Relevância
Verificar dígito de controle.	17,65% 3	11,76% 2	29,41% 5	41,18% 7	17	Alta Relevância
Realizar conferência manual.	41,18% 7	35,29% 6	11,76% 2	11,76% 2	17	Baixa Relevância

Fonte: Organizada pelos autores

RISCO 3 - os dados recusados e os itens em suspenso podem não ser isolados, analisados e corrigidos.

Principais controles:

- Impressão por completo de movimentos de itens em suspenso para obter um indício de auditoria completa;
- Analisar, frequentemente, todos os itens;

- Verificar os ajustes efetuados pelo usuário com a documentação autorizada dos dados de acesso;
- Fiscalizar os itens de exceção apontados pelo sistema;
- Registrar os itens recusados mantendo-os arquivados, inclusive os de seu futuro reprocessamento;
- Dividir em lotes as transações recusadas, facilitando assegurar que sejam verificadas e corrigidas.

Tabela 5 - Relevância dos possíveis controles para o risco de dados recusados e dos itens em suspenso não serem identificados, verificados e corrigidos.

Relevância / Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Imprimir toda movimentação de itens em suspenso para ter uma pista de auditoria completa.	12,50% 2	6,25% 1	31,25% 5	50% 8	16	Alta Relevância
Analisar, frequentemente todos os itens.	6,25% 1	25% 4	31,25% 5	37,50% 6	16	Alta Relevância
Verificar ajustes efetuados pelo usuário com a documentação.	6,25% 1	12,50% 2	43,75% 7	37,50% 6	16	Média/Alta Relevância
Fiscalizar os itens de exceção apontados pelo sistema.	0% 0	0% 0	40% 6	60% 9	15	Alta Relevância
Registrar os itens recusados os mantendo arquivados.	0% 0	18,75% 3	50% 8	31,25% 5	16	Média/Alta Relevância
Dividir em lotes as transações recusadas, facilitando assegurar que sejam verificadas e corrigidas.	18,75% 3	6,25% 1	31,25% 5	43,75% 7	16	Alta Relevância

Fonte: Organizada pelos autores

RISCO 4 - as transações fidedignas, digitadas para processamento ou produzidas pelo sistema, podem perder-se, não serem totalmente processadas, processadas de modo ou no período errado.

Principais controles:

- Implantar controles em lote;

- Fazer reconciliação dos totais de dados de entrada com totais dos dados de saída;
- Realizar revisão manual, com uso de teste de cálculos;
- Revisão e execução do follow-up dos relatórios de exceção relevantes.

Tabela 6 - Relevâncias dos possíveis controles para o risco de transações fidedignas perderem-se ou serem processadas erroneamente.

Relevância / Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Implantar controles de lote.	11,76% 2	23,53% 4	41,18% 7	23,53% 4	17	Média/Alta Relevância
Fazer reconciliação dos totais de dados de entrada com os de saída.	11,76% 2	5,88% 1	17,65% 3	64,71% 11	17	Alta Relevância
Realizar revisão manual, com uso de teste de cálculos.	5,88% 1	47,06% 8	41,18% 7	5,88% 1	17	Média/Baixa Relevância
Revisão e execução do follow-up dos relatórios de exceção relevantes.	11,76% 2	29,41% 5	35,29% 6	23,53% 4	17	Média/Alta Relevância

Fonte: Organizada pelos autores

RISCO 5 – Verificar se os funcionários do departamento de tecnologia da informação não executam funções incompatíveis.

Pode controlar os funcionários deste setor segregando suas funções da seguinte forma:

- Gerente de departamento;
- Analista e projetista de sistemas e programação;
- Responsável por manutenção do programa de base e sistema operacional;
- Operador;
- Controlador de dados;
- Responsável pela segurança de dados;

- Verificar se as atividades dos programadores e demais usuários do sistema estão sendo supervisionadas e o uso de programas está sendo controlado adequadamente.

Tabela 7 - Relevância do possível controle para o risco de funcionários de TI executarem funções incompatíveis.

Relevância / Controle	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Controle das responsabilidades e autorizações por divisão de funções.	0% 0	23,53% 4	23,53% 4	52,94% 9	17	Alta Relevância

Fonte: Organizada pelos autores

RISCO 6 – os programadores conseguem fazer modificações inexatas ou não autorizadas nos programas, o que diminuirá a confiabilidade nas informações processadas pelo sistema.

Principais controles:

- Impedir o acesso dos analistas de sistemas e programadores da equipe de desenvolvimento às bibliotecas de programas ou aos arquivos de dados utilizados para produção;
- Implementar uma supervisão apropriada;
- Delimitar as áreas de desenvolvimento e produção;
- Utilizar programas especializados em controle de acesso e segurança.

Tabela 8 - Relevância dos possíveis controles para o risco de programadores fazerem modificações inexatas ou não autorizadas nos programas, diminuindo a confiabilidade das informações geradas no sistema.

Relevância / Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Impedir o aceso de programadores da equipe de desenvolvimento às bibliotecas de programas.	6,25% 1	18,75% 3	56,25% 9	18,75% 3	16	Média/Alta Relevância
Implementar uma supervisão apropriada.	0% 0	6,25% 1	12,50% 2	81,25% 13	16	Alta Relevância
Delimitar as áreas de desenvolvimento e produção.	0% 0	12,50% 2	18,75% 3	68,75% 11	16	Alta Relevância
Utilizar programas especializados em controle de acesso e segurança.	0% 0	12,50% 2	31,25% 5	56,25% 9	16	Alta Relevância

Fonte: Organizada pelos autores

RISCO 7 – Funcionários não autorizados ou pessoas estranhas fora do grado funcional podem ter acesso fácil aos arquivos ou aos programas, o que as possibilitaria fazer alterações não autorizadas nos dados ou programas.

Principais controles:

- Restringir ao acesso por senhas e outros; (FREITAS, 2013, p.38)
- Implementação de rotinas adequadas relacionadas à rotação de tarefas, arranjos para feriados e férias, desligamento da empresa ou alteração de função;
- Implantar uma supervisão apropriada;
- Uso de controle físico de acesso, tais como crachás, carteiras funcionais e outros.

Tabela 9 - Relevância dos possíveis controles para o risco de funcionários não autorizados ou pessoas estranhas ao quadro funcional terem fácil acesso aos arquivos e programa podendo alterá-los

Relevância / Controles	Baixa	Média Baixa	Média Alta	Alta	Total de Respostas	Avaliação Maior %
Restringir o acesso por senhas.	0% 0	0% 0	11,76% 2	88,24% 15	17	Alta Relevância
Implementação de rotinas adequadas relacionadas a rotação de tarefas, arranjos de ferias e outros.	0% 0	5,88% 1	41,18% 7	52,94% 9	17	Alta Relevância
Implantar uma supervisão apropriada.	0% 0	5,88% 1	23,53% 4	70,59% 12	17	Alta Relevância
Uso de controle físico de acesso, tais como crachás, carteiras funcionais e outros.	11,76% 2	17,65% 3	29,41% 5	41,18% 7	17	Alta Relevância

Fonte: Organizada pelos autores

7 CONSIDERAÇÕES FINAIS

Pelo exposto neste artigo, verificou-se que as principais finalidades de um sistema geral de auditoria para controle interno em ambientes de tecnologia da informação são: proteger o ativo de uma empresa, manter a integridade das informações, a correção de dados errados e a confiabilidade dos registros, no intuito de promover a eficiência e eficácia operacional e gerencial da empresa. Sendo, portanto, fundamental boa prática de auditoria com a verificação da efetiva utilização destes controles sobre os riscos nos sistemas de informação operacional e gerencial da empresa, tornado complexa esta atividade.

No entanto, a complexidade envolvida na auditoria aplicada aos sistemas de informação relaciona-se com a correta compreensão dos riscos e dos controles deste sistema. Neste estudo confirmou-se a alta influência dos riscos, sejam eles inerentes, de controle ou de detecção, num ambiente informatizado quanto à possibilidade de que um ou mais elementos da integridade, disponibilidade ou confidencialidade da informação ou do procedimento sejam comprometidos, tornando imprescindível sua identificação e uso correto de controles.

Entretanto, para que estes controles sejam eficientes e eficazes, devem estar adequados ao seu grau de relevância em relação ao risco a que está vinculado.

Por meio da pesquisa de campo evidenciou-se que os controles sobre os riscos possuem graus de relevância diferentes, com destaque para os controles que usam recursos manuais que obtiveram o menor grau de relevância.

A presente pesquisa não pretende esgotar o assunto, dadas sua extensão e alta complexidade. Sugere-se aos entusiastas em auditoria de sistemas de informação a continuarem a pesquisa, em especial a relacionada com a importância de auditorias preventivas sobre os controles de riscos de penalidades tributárias em procedimentos de auditorias fiscais sobre os sistemas de informação das empresas.

REFERÊNCIAS

ATTIE, Willian. **Auditoria conceitos e aplicações**. 3. ed. São Paulo: Atlas, 1998.

CAMPOS, André. **Sistema de segurança da informação**: Controlando os Riscos. 2. ed. Florianópolis: Visual Books, 2007.

CASSARRO, A. Carlos. **Sistemas de informações para tomadas de decisões**. 4. ed. São Paulo: CENGAGE Learnig, 2010.

CASTRO, Róbison Gonçalves de; LIMA, Diana Vaz de. **Auditoria para concursos**. Brasília: Vestcon, 1999.

CERVO, A.; BERVIAN, P.A.; DA SILVA, R. **Metodologia Científica**. 6 ed. São Paulo: Pearson Prentice Hall, 2007.

CORNACHIONE JÚNIOR, Edgard Bruno. **Informática aplicada às áreas de contabilidade, administração e economia**. 3. ed. São Paulo: Atlas, 2001.

ELEUTÉRIO, Pedro Monteiro da silva. MACHADO, Marcio Pereira. **Desvendando a computação forense**. São Paulo: Novatec, 2011.

FREITAS, Eduardo Antônio Mello. **Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação**. Disponível em: <http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/3564/gestao_riscos_freitas.pdf> acesso em 13 de mar. de 2013.

GONÇALVES, Rosana C. M. Grillo. RICCIO, Edson Luiz. **Sistemas de informação: ênfase em controladoria e contabilidade**. São Paulo: Atlas, 2009.

GUIMARÃES, Marcos Freire. **Manual de auditoria**. Brasília: VESTCON, 2002.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. 2. ed. São Paulo: Atlas, 2008.

LAKATOS, E.M.; MARCONI, M.A. **Fundamentos de metodologia científica**. 4. ed. São Paulo: Atlas, 2001

LAUREANO, Marcos Aurelio Pchek. MORAES, Paulo Eduardo Sobreira. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, Curitiba, v.8, n.3, p. 38-44, 2005.

MALHOTRA, N. **Pesquisa de marketing**: uma orientação aplicada. 4. ed. Porto Alegre: Bookman, 2006.

REZENDE, Denis Alcides. **Planejamento de sistemas de informação e informática**. São Paulo: Atlas, 2003.