REVISTA DE TECNOLOGIA APLICADA (RTA)
Vol. 3, No.3, Set-Dez 2014, p.03-12
ISSN: 2237-3713

# Auditoria baseada em risco de penalidades tributárias em ambiente de sistemas de informação

# Audit based on risk of tax penalties in information systems environment

**Mariano Yoshitake**[*]
Faculdades Alves Faria – ALFA/Goiás.

**João Arlindo do Prado Gusmão**[†]
Faculdades Alves Faria – ALFA/Goiás

**Marinette Santana Fraga**[‡]
Universidade Federal de Juiz de Fora - UFjF/MG

**Resumo**
O objetivo deste artigo é identificar o grau de relevância dos controles para o risco de penalidades tributárias em procedimentos de auditorias fiscais. Aplicou-se a metodologia de pesquisa empírica, com uso do método conhecido como levantamento de dados transversal. 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, a serem respondidas por escrito. Os resultados indicam que os controles de riscos de penalidades tributárias em procedimentos de auditorias fiscais sobre os riscos obtiveram o maior grau de relevância. Este resultado provavelmente ocorreu devido ao fato de o fisco estar utilizando em suas ações fiscais técnicas de informática pericial, tais como a utilização de programas forenses para captura e análise de banco de dados.

**Palavras-chave:** auditoria baseada em riscos; penalidades tributárias; procedimentos de auditorias fiscais.

**Abstract**
The purpose of this paper is to identify the degree of relevance of the controls to the risk of tax penalties on tax audits procedures. Applied to empirical research methodology, using the method known as cross data. The research population were systems analysts responsible for the implementation of systems and information related to companies registered as suppliers of automation application programs in the Finance Department of Goiás. Data collection was conducted through a questionnaire to be answered by written. The results indicate that the risk controls of tax penalties on procedures for tax audits on risks obtained the highest degree of relevance. This result was probably due to the fact that the tax authorities are using in their

[*] Mariano Yoshitake, é professor do Mestrado Profissional em Administração de Empresas e Mestrado em Denvolvimento Regional das Faculdades Alves Faria – ALFA/Goiás. e-mail: kimimarinamariano@gmail.com
[†] João Arlindo do Prado Gusmão é Mestre em Administração Profissional, Faculdades Alves Faria – ALFA/Goiás. e-mail: joao.arlindo.gusmao@gmail.com
[‡] Marinette Santana Fraga é Mestre em Contabilidade – FVC/Bahia. É professor da Universidade Federal de Juiz de Fora - UFjF/MG. e-mail: marinettefraga@gmail.com

expert computer technical inspection activities, such as the use of forensic programs to capture and database analysis.

**Keywords:** audit risk-based; tax penalties; procedures for tax audits.

## 1. INTRODUÇÃO

Este estudo apresenta abordagens 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 , em especial os ligados a sonegação fiscal, relacionados com o uso de sistemas de computadores. (ELEUTÉRIO, 2011 p. 17).

### 1.1 Justificativa do estudo

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, mudando a forma de armazenamento das informações de dados físicos documentais para dados digitais eletrônicos.

Deste modo, vem-se mudando rapidamente a atuação do auditor, diminuindo a quantidade de informações físicas documentais e aumentando a quantidade de dados e informações digitais eletrônicas. Considerando-se que “a auditoria em ambiente de tecnologia de informação não muda a formação do auditor” (IMONIANA, 2008, p. 16), a sua atuação 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, incluindo os fiscais tributários, afetado as operações e gestão das empresas. (ELEUTÉRIO, 2011, p. 17).

Assim, as empresas devem lidar, além dos tradicionais riscos de auditoria, com o risco de se sofrer penalidades tributárias em procedimentos de auditorias fiscais pelo fisco.

### 1.2 Problema

Diante desse contexto, as empresas, em especial suas equipes de auditoria, precisam enfrentar o desafio de adequar-se a esta nova realidade. E para tanto se deparam com o seguinte problema: qual o grau de relevância dos controles de riscos de penalidades tributárias em seu sistema de informação para uma eficiente e eficaz utilização das técnicas de auditoria aplicadas a um ambiente informatizado?

## 2. FUNDAMENTOS DO ESTUDO

### 2.1. 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 B. (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)

## 2.2. 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, colocando a empresa em risco.

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).

## 2.3. 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 ABNT NBR/ISSO/IEC 27002/2007, que normatiza conceitos de segurança da informação, 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 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2007).

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)

## 2.4 Risco de auditoria

Segundo a *International Standard Auditing* (ISA) nº 6, das normas internacionais de auditoria, e a Resolução CFC (Conselho Federal de Contabilidade) nº. 1.203/09 que aprovou a NBC-TA 200 (Normas Brasileiras de Contabilidade – Técnicas de Auditoria nº 200) risco de auditoria significa o risco ao qual o auditor dá uma opinião inapropriada de auditoria quando os demonstrativos contábeis estão materialmente errados. O risco de auditoria possui três componentes: risco inerente, risco de controle e risco de detecção. (IFAC, 2012, p. 76)

O risco em auditoria significa que o auditor aceita algum nível de incerteza no desempenho da função de auditoria. O auditor reconhece, por exemplo, que há incerteza a respeito da competência da evidência, incerteza a respeito da efetividade da estrutura de controle interno do cliente, e incerteza quanto às demonstrações contábeis se estão representadas adequadamente no término dos trabalhos da auditoria.

O caminho primário para o auditor lidar com risco no planejamento da evidência de auditoria é por meio da aplicação do modelo de risco de auditoria. A fonte do modelo de risco de auditoria é a literatura profissional da *Statements on Auditing Standards* (SAS), especificamente a SAS 39 sobre amostragem de auditoria, a SAS 47 sobre materialidade e risco e a norma internacional de auditoria ISA nº 6 sobre avaliação de risco e controle interno.

O modelo de risco de auditoria é usado primariamente para finalidades de planejamento da decisão sobre a quantidade de evidência a acumular em cada ciclo. É definido como segue: RDP = Risco de detecção; RAA = Risco de auditoria; RINE = Risco inerente e RCO = Risco de controle, chegando à Equação 1.

$$RDP = \frac{RAA}{(RINE\ X\ RCO)}$$

Um exemplo numérico servirá para discussão, mesmo que não seja prático medir tão precisamente os riscos, quanto esses números fazem supor. Considerando os valores

seguintes: RINE = 100%; RCO = 100%; RAA = 5%, observe a identificação do risco de detecção, através da execução da Equação 1.

$$RDP = \frac{0{,}05}{(1{,}0\ X\ 1{,}0)} = 0{,}05 = 5\%$$

### 2.4.1 – Risco de detecção

Risco de detecção é uma medida do risco de que a evidência de auditoria para um segmento falhará na detecção de erros que excedem um montante tolerável, se tais erros existirem.

A ISA nº 6 e a Resolução CFC nº. 1.203/09 que aprovou a NBC-TA 200 conceituam risco de detecção como o risco de que os procedimentos substantivos de um auditor não detectará um erro que existe em um saldo de conta ou classe de transações que poderiam ser material, individualmente ou quando agregado com erros em outros saldos. (IFAC, 2012, p. 76)

### 2.4.2 – Risco inerente

Segundo Yoshitake (2013, p. 119) Risco inerente é uma medida da avaliação do auditor da probabilidade de erros excedentes, a um montante tolerável, existir em um segmento antes de considerar a efetividade dos controles contábeis interno.

De maneira semelhante, a ISA nº 6 e a Resolução CFC nº. 1.203/09 que aprovou a NBC-TA 200 conceituam o risco inerente como a susceptibilidade de um saldo de conta ou classe de transações a erro que poderia ser material, individualmente ou quando agregado com erros em outros saldos ou classes, assumindo a ausência de controles internos. (IFAC, 2012, p. 78)

Se o auditor conclui que há alta probabilidade de erro, ignorando os controles internos, o mesmo concluiria que o risco inerente é alto. Os controles internos são ignorados no estabelecimento do risco inerente em razão de serem considerados separadamente no modelo de risco de auditoria como risco de controle.

### 2.4.3 – Risco de controle

Yoshitake (2013, p. 125) define Risco de controle como uma medida da avaliação do auditor da probabilidade de que erros excedentes a um montante tolerável em um segmento não será evitado ou detectado pela estrutura de controle interno da auditada.

Segundo a ISA nº 6 e a Resolução CFC nº. 1.203/09 que aprovou a NBC-TA 200 risco de controle é o risco de que um erro que poderia ocorrer em um saldo de conta ou classe de transações e que poderia ser material individualmente ou quando agregado com erros em outros saldos ou classes, não será evitado ou detectado e corrigido em tempo pelos sistemas de contabilidade e controle interno. (IFAC, 2012, p. 78)

## 3. METODOLOGIA

Para compreender 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 (MENDONÇA, at all, 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 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, cujo modelo pode ser observado no Anexo I 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. Conseguimos contatar e coletar as respostas de 17 analistas, tornando-se esta a amostra do estudo.

## 4. PESQUISA SOBRE RISCO FISCAL

Uma vez que estar clara a importância de identificação dos riscos de auditoria sejam eles de detecção, inerentes ou de controle, incluímos na pesquisa, aos tradicionais riscos já citados, o risco das empresas sofrerem penalidades tributárias em procedimentos de auditoria fiscal em seu sistema de informação e os possíveis controles, no intuito de identificar seu grau de relevância, cujos resultados estão demonstrados no Quadro 1.

Quadro 1 - Grau de relevância dos possíveis controles para o risco de penalidades tributárias em procedimentos de auditorias fiscais

| **Relevância/Controles** | **Baixa** | **Media Baixa** | **Media Alta** | **Alta** | **Total de Respostas** | **Avaliação Maior %** |
|---|---|---|---|---|---|---|
| Consultar a legislação tributária pertinente com especialista. | 5,88%<br>1 | 5,88%<br>1 | 23,53%<br>4 | 64,71%<br>11 | 17 | Alta Relevância |
| Conferir se todas as funções dos programas aplicativos são permitidas pela legislação tributária. | 0%<br>0 | 5,88%<br>1 | 5,88%<br>1 | 88,24%<br>15 | 17 | Alta Relevância |
| Verificar se a documentação exigida pelo fisco para o sistema informatizado esta regular. | 5,88%<br>1 | 0%<br>0 | 0%<br>0 | 94,12%<br>16 | 17 | Alta Relevância |

| | | | | | | |
|---|---|---|---|---|---|---|
| Verificar se os equipamentos de emissão de cupom fiscal foram devidamente autorizados. | 0%<br>0 | 0%<br>0 | 5,88%<br>1 | 94,12%<br>16 | 17 | Alta Relevância |
| Verificar a regularidades da emissão de notas fiscais eletrônicas. | 0%<br>0 | 11,76%<br>2 | 5,88%<br>1 | 82,35%<br>14 | 17 | Alta Relevância |
| Certificar se o registro de todos os documentos fiscais foram para o SPED e demais informativos fiscais. | 0%<br>0 | 0%<br>0 | 17,65%<br>3 | 82,35%<br>14 | 17 | Alta Relevância |
| Certificar que não há registro nos bancos de dados de controle paralelo ao fiscal. | 5,88%<br>1 | 11,76%<br>2 | 0%<br>0 | 82,35%<br>14 | 17 | Alta Relevância |
| Certificar da inexistência de aplicativos que adulterem ou simulem documentos fiscais. | 5,88%<br>1 | 0%<br>0 | 23,53%<br>4 | 70,59%<br>12 | 17 | Alta Relevância |

Fonte: elaboração própria, de acordo com dados colhidos na pesquisa empírica

### 4.1 Análises dos resultados

Como observado no resultado da pesquisa, os controles de riscos de penalidade tributárias em procedimentos de auditorias fiscais foram considerados de alta relevância. Acredita-se que isto ocorreu devido ao fato de que a utilização por parte das empresas de sistemas informatizados que envolva emissão de documentos fiscais a consumidor, ou de qualquer sistema eletrônico de processamento de dados no recinto de atendimento, dependa de prévia autorização do fisco, ficando sujeitos a sua total fiscalização. E mesmo os sistemas informatizados que não dependam de prévia autorização, estarão, quando em uso, sujeitos à fiscalização de acordo com as normas previstas na legislação tributária pertinente.

Os fiscos estaduais, em todo território nacional, precisam obedecer ao disposto nos Convênios ICMS 1/98, 23/00, 84/01, 85/01 e 16/03 e nos Convênios ECF 1/98 e 2/03, que disciplina o uso de sistemas informatizados nas empresas e cujas normas devem estar incorporadas as respectivas legislações tributárias. No estado de Goiás o uso de sistemas informatizados é normatizado pelo Regulamento do Código Tributário Estadual - RCTE, decreto nº 4.852, de 29 de dezembro de 1997 no ANEXO X do sistema eletrônico de processamento de dados (art. 158, I) e no ANEXO XI do equipamento emissor de cupom fiscal (art. 158, II). Nesta legislação encontram-se normas técnicas especificas sobre a utilização de sistemas de informação e sobre funções que os programas aplicativos obrigatoriamente devem possuir e as que são proibidos.

O não cumprimento destas normas caracterizaria utilização irregular de sistemas de informação, com penalidades para o contribuinte, ficando solidariamente responsável o analista/programador cadastrado no fisco como responsável técnico pelo sistema. Este fato que pode ter justificado a alta percepção de risco de penalidades tributárias verificada.

Outro fator identificado, que pode ter colaborado para o resultado dessa pesquisa, foi a utilização de técnicas de informática pericial pelo fisco em suas auditorias fiscais, tais como o uso de ferramentas e programas forenses para captura e análise de banco de dados, aumentando a chance de falhas

serem descobertas nos sistemas de informação das empresas e identificadas ou confundidas com crimes fiscais gerando altas penalidades.

## 6. CONCLUSÕES

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. (IMONIANA, 2008, p.41).

No entanto, verificou-se que 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 ficou evidenciada uma alta influência dos riscos de penalidades tributárias, além dos tradicionais 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.

Através da pesquisa de campo evidenciou-se que os controles sobre os riscos possuem graus de relevância diferentes. No entanto as resposta às questões constantes do questionário demonstraram que os controles de riscos de penalidades tributárias em procedimentos de auditorias fiscais são considerados, em média, como de alta relevância, em mais de 80% dos pesquisados, embora costumeiramente estes não constem no rol de riscos e controles clássicos na literatura especializada.

Este resultado provavelmente ocorreu devido à previsão legal de penalidades pela não adequação das empresas as normas tributárias relacionadas aos seus sistemas de informação e ao fato de o fisco estar utilizando em suas ações fiscais técnicas de informática pericial, tais como a utilização de programas forenses para captura e análise de banco de dados.

A presente pesquisa não pretendeu esgotar o assunto, dadas sua extensão e alta complexidade. Assim, sugere-se aos pesquisadores em auditoria de sistemas de informação a continuarem a investigação, em especial, à relacionada com a importância de auditorias preventivas sobre os controles de riscos de penalidades tributárias em ambientes de sistemas de informação nas empresas.

## Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR/ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2007.

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. CENGAGE Learnig, 2010.

CASTRO, Róbison Gonçalves de. LIMA, Diana Vaz de. **Auditoria para concursos com aplicação nas áreas governamental e empresarial**. 1. ed. Brasília: Vestcon, 1999.

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

CORNACHIONE Jr., B. E.. **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**. 1. ed. 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.

MENDONÇA, Alzino Furtado de. ROCHA, Cláudia Regina Ribeiro. NUNES, Heliane Prudente. **Trabalhos acadêmicos: planejamento, execução e avaliação**. Goiânia: Faculdade Alves Faria, 2008.

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.

IFAC. International Federation of Accountants. **Handbook of international auditing, assurance and ethic pronouncements.** New York: IFAC, 2012.

YOSHITAKE, Mariano. **Auditoria Contábil: metodologia de processo de auditoria**. Curitiba: Juruá Editora, 2013.