UNIVERSIDADE FEDERAL DE MINAS GERAIS

ALLEXANDRE LUGÃO DO NASCIMENTO

AUDITORIA DE SISTEMAS E A LEI SARBANES-OXLEY:
ESTUDO EMPÍRICO COMPARATIVO ENTRE DUAS MINERADORAS PRESENTES NO INTERIOR MINEIRO

Belo Horizonte
2014

UNIVERSIDADE FEDERAL DE MINAS GERAIS

ALLEXANDRE LUGÃO DO NASCIMENTO

AUDITORIA DE SISTEMAS E A LEI SARBANES-OXLEY:
ESTUDO EMPÍRICO COMPARATIVO ENTRE DUAS MINERADORAS PRESENTES NO INTERIOR MINEIRO

Monografia apresentada ao Centro de Pós-Graduação e Pesquisas em Contabilidade e Controladoria, na Faculdade de Ciências Econômicas, da Universidade Federal de Minas Gerais como exigência parcial para obtenção do título de **Especialista em Auditoria**.

Orientadora: DEBORA LAGE MARTINS
Co-orientadora: ANA THEREZA N. MAGALHÃES

BELO HORIZONTE

2014

ALLEXANDRE LUGÃO DO NASCIMENTO

AUDITORIA DE SISTEMAS E A LEI SARBANES-OXLEY:
ESTUDO EMPÍRICO COMPARATIVO ENTRE DUAS MINERADORAS PRESENTES NO INTERIOR MINEIRO

Monografia apresentada ao Centro de Pós-Graduação e Pesquisas em Contabilidade e Controladoria, na Faculdade de Ciências Econômicas, da Universidade Federal de Minas Gerais como exigência parcial para obtenção do título de **Especialista em Auditoria**.

Belo Horizonte, 01 de agosto de 2014.

BANCA EXAMINADORA:

_____
Profª. Debora Lage Martins

_____
Profª. Ana Thereza N. Magalhães

_____
Juliano Vasconcelos Gomes

À minha família, noiva e amigos pela compreensão, estímulo e ajuda em todos os momentos.

AGRADECIMENTOS

Considerando esta monografia como resultado de uma jornada que não começou na UFMG, esses agradecimentos podem se tornar tarefa difícil e injusta. Para não correr o risco da injustiça, agradeço de antemão a todos que de alguma forma contribuíram para a construção de quem sou hoje.

Agradeço particularmente a algumas pessoas que me foram fundamentais para concluir este trabalho.

À minha mãe Marcia pela ajuda afetiva, acadêmica e profissional, se mostrando sempre presente quando mais precisei.

À minha irmã Priscilla e ao Jorge pelo incentivo constante.

Às professoras Ana Thereza e Débora Lage pela paciência, auxílio e pelos ensinamentos transmitidos.

Aos colegas de classe, mas especialmente às amigas Letícia, Patrícia e Tatiana que sempre foram companheiras e estavam juntas a todo momento.

Aos amigos e colegas da EY, por toda a ajuda, material concedido, além de apoio para que eu consiga todo o sucesso profissional que almejo, em especial ao Juliano Gomes e ao João Ervilha.

Aos meus amigos que mantenho desde o colégio, amigos de faculdade, trabalho, dança, enfim, todos os amigos que estão comigo todos esses anos.

E um agradecimento especial à Ana Carolina por todo carinho, apoio, compreensão, ajuda e por sempre me incentivar a crescer e me tornar uma pessoa e um profissional melhor.

"Não existem empresas sem falhas, existem empresas bem ou mal auditadas ou mal controladas."

Dr. Stephen Kanitz

RESUMO

Este trabalho tem por objetivo expor a importância da auditoria de sistemas após o surgimento da Lei Sarbanes-Oxley (Lei SOX) nos Estados Unidos e seus impactos para a auditoria financeira baseada testes de controles internos automatizados, na tentativa de redução do risco de controle. Para tanto, serão apresentadas as principais metodologias de testes para auditoria de sistema, fazendo relação com o que é requerido pela Lei SOX. Ainda, será apresentado um estudo empírico comparativo de duas mineradoras presentes no interior de Minas Gerais, além de evidenciar seus principais controles relacionados à segurança de seu ambiente automatizado.

PALAVRAS-CHAVE: Auditoria de Sistemas, Sarbanes-Oxley, Controles Internos, Riscos de Controle.

ABSTRACT

This report aims to explain the importance of systems audit after the emergence of the Sarbanes-Oxley Act (Sox Act) in the United States and its impacts on the financial audit based on tests of the automated internal controls in an attempt to reduce the risk of control. For this, we present the main test methodologies for systems audit, compared with the Sox Act requirements. Still, it will be presented a comparative empirical study of two mining companies, operating in Minas Gerais, besides highlighting its key controls related to the safety of their automated environment.

KEY-WORDS: Systems Audit, Sarbanes-Oxley, Internal Controls, Risk of Control.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Mudanças no ambiente de negócios são comuns quando se considera um cenário globalizado e altamente competitivo. As mesmas podem derivar tanto de fatores internos, quanto de fatores externos, a partir da imposição de novas regulamentações governamentais.

Neste panorama, temos a Lei Sarbanes-Oxley - SOX, criada em 2002, após a descoberta da geração de informações financeiras falsas por parte de algumas empresas do mercado americano, como Enron (energia), Worldcom (telecomunicações) e Arthur Andersen (auditoria), atingindo diversos investidores, causando prejuízos financeiros sem precedentes. Seu principal objetivo é retomar o equilíbrio dos mercados por meio de organismos que assegurem a responsabilidade da administração de uma empresa sobre a confiabilidade da informação por ela fornecida. Adicionalmente, a Lei determinou pela criação de um órgão, *Public Company Accounting Oversight Board* (PCAOB) responsável por regular as empresas de auditoria independente e estabelecer as normas a serem seguidas por elas.

A Lei SOX, através de sua seção 404, impõe que as empresas passem por revisões anuais de seus ambientes de controle, com o objetivo da emissão de relatórios financeiros mais confiáveis. Neste contexto, surge a necessidade de maior transparência por parte das empresas, e isso pode se dar, por exemplo, com a estruturação e monitoramento de seus controles internos. Para tanto, as organizações cada vez mais se valem de processos de tecnologia de informação, com sistemas de informação que assegurem a integridade, a disponibilidade e a confidencialidade das informações de negócio. A estrutura de controles torna-se cada vez mais automatizada, com o crescente número de controles automáticos totalmente dependentes de sistemas. Além disso, mesmo atividades que dependem do conhecimento dos empregados e que ocorrem em sua maior parte fora dos sistemas de informação passam por eles em algum momento. Cabe ressaltar que até mesmo relatórios, informações que suportam controles manuais e decisões estratégicas são extraídos em sistemas.

Por isso, dizer que os controles internos de Tecnologia da Informação (TI) suportam todos os demais controles da organização e consequentemente permitem o desenho de um ambiente robusto de controles internos. Eles possuem efeito

pervasivo e intenso por estarem presentes em praticamente todos os controles internos da organização. Para exemplificar, se um controle de TI relevante falhar, como falha no controle de acesso a transações e dados financeiros, ele poderá provocar impacto na confiabilidade das demonstrações financeiras.

Desenvolver e implementar um sistema de controle interno eficaz tende a ser desafiador, devido a um maior uso e dependência de tecnologias informatizadas a emergência de novos modelos de negócios que buscam incrementar o desempenho e a governança das empresas. Nesse sentido, a avaliação dos controles gerais de TI em uma empresa se torna bastante complexa, pois engloba não apenas os componentes tecnológicos, mas também o modelo e o ambiente de negócios da empresa, bem como a interação desses com os sistemas informatizados. Essa questão deve ser ponderada e avaliada pelas empresas de auditoria independente, uma vez que os processos e controles tornam-se cada vez mais automatizados, o que impacta não somente a operação, mas a gestão e governança das empresas.

O reflexo dessa preocupação é evidente nas normas de auditoria do PCAOB (2007, p.30) – órgão americano criado para regular as empresas de auditoria independente – que orienta: “como parte da avaliação do final do ano fiscal para o processo de reporte, o auditor deve avaliar [...] a extensão do envolvimento da tecnologia da informação para o processo de reporte [tradução livre do autor]”.

Publicações do PCAOB (2004) e estudos de Soares (2006) já demonstravam a importância da avaliação dos controles internos pela auditoria independente, inclusive, quando se trata dos sistemas informatizados. Nesse sentido, cria-se a necessidade de que as empresas de auditoria possuam razoável segurança quanto ao ambiente de controles internos e quanto à confiabilidade dos sistemas de informação. Dito isso, surge um maior rigor quanto ao nível de maturidade esperado dos ambientes de TI das empresas, uma vez que são componentes fundamentais para a análise das Demonstrações Financeiras.

Em linha com as orientações do PCAOB, órgãos como a Associação de Auditoria e Controle de Sistemas de Informação (ISACA) e a Federação Internacional dos Contadores (IFAC) se propuseram a criar guias práticos para auxiliar a governança em TI e a estruturação de controles relacionados ao ambiente informatizado. Esses documentos também servem como norteadores das empresas de auditoria independente para análise da estrutura de controles internos de TI no

âmbito do escopo SOX. Como exemplos desses documentos têm-se o COBIT – Objetivos de Controle para Informações e Tecnologia Relacionada – e o ISA 315 – Normas Internacionais de Contabilidade número 315.

Esses guias, baseados em literaturas como o COBIT e o ISA 315, além de auxiliar na construção de procedimentos de auditoria independente para o ambiente de Tecnologia da Informação, podem auxiliar as empresas a estruturarem os controles internos relativos aos ambientes informatizados e que possuem interação com o ambiente de negócio. Os modelos de governança para Tecnologia da Informação, como o COBIT e as próprias recomendações da auditoria, são fontes importantes para orientar as empresas na construção de seus controles gerais de TI e na estruturação de seu ambiente informatizado.

Considerando que os trabalhos e recomendações da auditoria possuem papel relevante na construção e aprimoramento da governança corporativa e consequentemente na estrutura de controles internos de uma organização, torna-se relevante investigar qual o nível de maturidade das empresas auditadas, sejam elas reguladas ou não pela Lei SOX, no que tange seus controles e ambientes de TI, através da ótica do trabalho de auditoria independente. Adicionalmente, é relevante avaliar se o fato de uma empresa ser regulada pela SOX impacta ou não na construção de controles mais robustos e eficazes.

Nesse estudo, o foco será dado à análise dos ambientes de tecnologia da informação e seus controles gerais que são auditados pelas empresas de auditoria independente, a fim de compreender se existe uma relação entre a maturidade atingida pelas companhias auditadas em relação ao seu ambiente e o rigor e a estrutura de controles internos exigidos pela Lei SOX.

Para cumprir esse objetivo, serão analisadas duas empresas de mesmo ramo, sendo uma regulada pela lei americana e outra que não precisa cumprir as exigências dessa lei, tendo como base os controles gerais de TI, por acreditar que o ambiente da empresa regulada pela Lei SOX é mais robusto e eficaz.

A proposta desse trabalho, portanto, é investigar as diferenças entre os ambientes de TI dentro de empresas reguladas pela SOX e empresas que não precisam cumprir as exigências da Lei, do ponto de vista da auditoria independente, uma vez que a mesma também é responsável pela análise dos controles gerais de TI, além do nível de maturidade de cada uma delas referentes a esses controles.

Para alcançar esse objetivo será necessário cumprir os seguintes objetivos específicos:

- Analisar os procedimentos de auditoria utilizados para a avaliação dos controles gerais de tecnologia da informação, para entender se existe alguma diferença na avaliação de ambientes distintos.
- Comparar os controles gerais de tecnologia da informação (ITGCs) e o ambiente de TI de empresas reguladas pela SOX e empresas não reguladas pela Lei.
- Avaliar se o fato de uma empresa ser regulada pela Lei SOX impacta no nível de maturidade de seus controles de TI.

O presente trabalho divide-se em capítulos para melhor expor o tema em questão, sendo o segundo capítulo reservado para revisão teórica, apresentando os principais conceitos relacionados ao objeto desta monografia, incluindo uma análise do COBIT, do ponto de vista das metodologias utilizadas pelas principais empresas de auditoria independente do mundo, com o intuito de demonstrar o que é avaliado em uma auditoria de sistemas.

O terceiro capítulo trará a metodologia do trabalho, contendo o método de pesquisa, além das estratégias de coleta e análise dos dados.

Já o quarto capítulo trará o estudo empírico comparativo entre duas mineradoras presentes no estado de Minas Gerais, sendo uma listada em bolsas de valores americanas e, portanto, obrigada a seguir o que determina a Lei Sarbanes-Oxley e outra que não necessita seguir as mesmas regras impostas pelo governo americano. Neste estudo empírico, serão comparados os ambientes de tecnologia da informação e os procedimentos de auditoria, no que tange o processo de auditoria de sistemas.

Por fim, o quinto capítulo traz as conclusões da análise comparativa realizada no quarto capítulo.

2 REVISÃO TEÓRICA

2.1 Contextualização

O trabalho do auditor independente e a auditoria externa estiveram em evidência após os escândalos ocorridos nos anos 2000 envolvendo empresas como a Enron (energia) e Arthur Andersen (auditoria), que “geraram inúmeros prejuízos financeiros atingindo milhares de investidores” (SILVA; MACHADO, 2008, p.2). Ainda, de acordo com os mesmos autores “tornou-se necessária a ação de autoridades americanas para evitar maiores prejuízos com a descapitalização das empresas e recuperar, assim, a credibilidade do mercado. Desta forma, o congresso americano aprovou em 30 de julho de 2002 a Lei Sarbanes – Oxley” (SILVA; MACHADO, 2008, p.2).

A Lei criada em 2002 pelos senadores Paul Sarbanes e Michel Oxley, “foi uma tentativa de proteger o investidor público de corrupções corporativas e restaurar a confiança dos investidores no mercado de capitais [tradução livre pelo autor]” (BRYAN, 2009, p.1). Para Soares (2006, p.23):

> A SOX foi criada com o objetivo de readquirir a confiança pública nos líderes empresariais norte-americanos e de enfatizar a importância dos padrões éticos na preparação das informações financeiras reportadas aos investidores, sobretudo, devidos aos recentes escândalos financeiros ocorridos no mundo dos negócios, que levam organizações a falência e custaram bilhões de dólares, acarretando em prejuízos incomensuráveis aos acionistas e investidores.
>
> (SOARES, 2006, p.23)

Como retratado pelo estudo da Deloitte (2003, p.3) a Lei Sarbanes-Oxley (SOX) tem como principal objetivo desencorajar “atividades duvidosas” das companhias, através de diversas medidas que incentivam a melhoria do ambiente de controles internos, além de exigir maior transparência por parte das empresas, além de aumentar a responsabilidade dos executivos que as comandam. Além disso, o mesmo estudo trata que a “Lei Sarbanes-Oxley muda fundamentalmente o ambiente empresarial e regulador”, trazendo maior rigor e responsabilidade às companhias.

De acordo com Danta (2006, p.56) a Lei SOX foi “uma forma encontrada pelo governo para estabelecer recursos legais nos preceitos básicos da boa governança

corporativa e das práticas empresariais éticas". Também de acordo com Soares (2006, p.23) "[a] Lei Sarbanes-Oxley afeta diretamente as regras para a Governança Corporativa, relativas à divulgação e a emissão de relatórios financeiros de sociedades de capital aberto que possuem ações negociadas em bolsas de valores dos EUA".

Cabe ressaltar, ainda, que "os efeitos da Lei Sarbanes-Oxley serão bastante significativos não só nos Estados Unidos. A legislação determina que as empresas que não são norte-americanas, mas que possuem cotação secundária em uma Bolsa de Valores norte-americana, devem também seguir as novas leis, assim como seus auditores." (KPMG, s.n.t., p.1).

A lei, composta por 11 capítulos (Quadro 1), tem abrangência tanto do ponto de vista da auditoria, tratando da independência do auditor, até a responsabilidade empresarial, tratando de Contabilidade e Fraudes Corporativas.

Quadro 1 – Títulos da Lei SOX.

Títulos da Lei Sarbanes-Oxley de 2002	
Título	**Seção**
Title I	Public Company Accounting Oversight Board
Title II	Auditor Independence
Title III	Corporate Responsibility
Title IV	Enhanced Financial Disclosures
Title V	Analyst Conflict of interest
Title VI	Commission Resources and Authority
Title VII	Studies and Reports
Title VIII	Corporate and Criminal Fraud Accountability
Title IX	White-Collar Crime Penalty Enhancements
Title X	Corporate Tax Returns
Title XI	Corporate Fraud and Accountability

Fonte: RAIBORN, C.; SCHORG, C., 2004, p.20.

De acordo com Bryan (2009, p.2) a "SOX não foi desenhada apenas para fortalecer os controles internos, mas também para regular a profissão contábil [tradução livre pelo autor]". Tanto que, como forma de garantir que outros casos como os da Enron e Arthur Andersen não se repetissem, a Lei determinou, ainda, o acompanhamento das empresas de auditoria independente por um órgão, também independente, denominado *Public Company Accounting Oversight Board*. O mesmo é uma entidade privada, sem fins lucrativos, criado para "fiscalizar auditores e, consequentemente, proteger os interesses dos investidores" (TIBÚRCIO, 2008, p.1)

Como forma de regulamentar os procedimentos de auditoria, ainda foram criados os padrões de auditoria (AS), sendo o mais conhecido, produzido pelo PCAOB, o AS nº5 que trata por "prover direção que se aplica quando o auditor está engajado em realizar a auditoria quanto à efetividade dos controles internos sobre as demonstrações financeiras [tradução livre do autor]" (PCAOB, 2007, p.1)

Além disso, de acordo com o estudo produzido pela Deloitte (2003), dentro da Lei SOX, existe a seção 404, que:

> Determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Além disso, o auditor independente da companhia deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.
>
> (DELOITTE, 2003, p. 4)

Claramente, o que se tem como um dos pontos chave para o entendimento da Lei Sarbanes-Oxley, pela percepção do *IT Governance Institute* (2006) é a preocupação com controles internos nas companhias. Isso se deve, também, pelo fato de que a AS nº5, do PCAOB, define que a "auditoria de controles internos sobre os relatórios financeiros deve ser integrada à auditoria de demonstrações financeiras [...] os objetivos sejam diferentes, no entanto, o auditor deve planejar e realizar o trabalho para atingir os objetivos de ambas as auditorias [tradução livre do autor]" (PCAOB, 2007, p.30).

Geralmente, os cuidados relativos ao acompanhamento e monitoramento dos controles internos são desempenhados pela função de Auditoria Interna, que, de acordo com Franco e Marra (2001, p.137):

> [...] é aquela exercida por funcionário da própria empresa, em caráter permanente. Apesar de seu vínculo à empresa, o auditor interno deve exercer sua função com absoluta independência profissional, preenchendo todas as condições necessárias ao auditor externo, mas também exigindo da empresa o cumprimento daquelas que lhe cabem. Ele deve exercer sua função com total obediência às normas de auditoria e o vínculo de emprego não lhe deve tirar a independência profissional, pois sua subordinação à administração da empresa deve ser apenas sob o aspecto funcional.
>
> (FRANCO; MARRA, 2001, p.137)

Ademais, verifica-se que a auditoria interna pode definir-se como:

> [...] uma atividade independente, de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Assiste a organização na consecução dos seus objetivos, através de uma abordagem sistemática e disciplinada, para a avaliação e melhoria da eficácia dos processos de gestão de risco, controle e governança.
>
> (PRADAS; SALVADOR, 1995 apud COSTA, 2008, p.8)

A função de Auditoria Interna ou Controles Internos passa por diversas adaptações ao longo dos anos, ainda mais com as diversas mudanças que as organizações sofrem para se adaptar a um ambiente mais informatizado. De acordo com o que foi publicado no COSO (2012), desenvolver e implementar um sistema de controle interno eficaz e operá-lo com eficiência e eficácia requer conhecimentos e trabalhos específicos relacionados ao ambiente de tecnologia da empresa, uma vez que exige-se um sistema de controle mais ágil. Uma análise de controles internos, de acordo com Gherman (2005), engloba controles automatizados e de grande dependência de tecnologia da informação, levando a uma maior necessidade de avaliação do ambiente virtual das empresas.

Com o que foi exposto, demonstra-se uma maior necessidade de mudanças no próprio trabalho de auditoria, uma vez que requer um maior tratamento e análise das ferramentas e aplicações que suportam o trabalho, de modo que garantam razoável segurança sobre a informação auditada.

Além do que foi apontado:

> [...] em virtude da contínua e crescente utilização dos serviços e recursos tecnológicos, a TI passa a ser um componente fundamental para o processo de elaboração e apresentação dos relatórios financeiros, tanto pela aplicação de eficazes controles internos quanto pela reparação da documentação que atesta a eficácia dos controles internos sobre os relatórios financeiros.
>
> (SOARES, 2006, p.66).

De acordo com o PCAOB (2004, p.34), os controles gerais de TI são “parte de atividades de controle dos componentes de controles internos”.

A partir do que foi exposto e, pelo o que é determinado pela Seção 404 da Lei SOX, é de grande importância que a organização “declare que o auditor independente da companhia atestou e reportou a avaliação feita pela administração sobre seus controles e procedimentos internos para a emissão de relatórios financeiros” (DELOITTE, 2003, p.9), ou seja, necessita-se avaliação do auditor quanto à efetividade dos controles da organização, o que inclui a análise dos

controles relacionados à TI. Para uma análise mais completa quanto a controles internos, principalmente quando existe análise de um ambiente regulado pela Lei SOX, é importante tratar e comentar sobre a necessidade e dependência de tecnologia por parte das organizações. Nesta nova cultura, as auditorias, interna e externa, precisaram se adaptar a esse novo tipo de análise, que considera o ambiente informatizado como base do processo de auditoria.

Com a necessidade deste novo tipo de abordagem por parte das auditorias, o PCAOB (2007, p.30) determina que "como parte da avaliação do final do ano fiscal para o processo de reporte, o auditor deve avaliar [...] a extensão do envolvimento da tecnologia da informação para o processo de reporte [tradução livre do autor]". Além disso, a norma AS nº5 do PCAOB discorre sobre a necessidade de discussão sobre os efeitos da TI para os controles internos no que tange as demonstrações financeiras.

No trabalho produzido por Bryan (2009), destaca-se que existe produção literária muito limitada, disponível, no que se refere aos controles gerais de TI necessários para cumprir com os requerimentos da SOX, necessitando prover o mercado de maiores e melhores políticas e procedimentos relacionados a sistemas de informação.

Apesar da escassez de produção literária sobre controle de Tecnologia da Informação, o guia produzido pelo ITGI (2006), recomenda a utilização de *frameworks* como o COBIT (*Control Objectives for Information and related Technology*), a ISO 17799 (*The Code of Practice for Information Security Management*) e o ITIL (*Information Technology Infrastructure Library*), pois esses três guias trazem a objetivos operacionais e financeiros. Esses *frameworks* buscam analisar o ambiente de TI das organizações para atendimento à SOX, avaliando não apenas as aplicações envolvidas no trabalho de auditoria, mas as operações que são automatizadas, suportando o processo de negócios, garantindo, com razoável segurança, que as informações providas ao auditor contábil são íntegras e precisas.

De acordo com o ITGI (2006), a governança de TI, antes de tudo, determina a alçada de decisão, sendo a administração, por outro lado, o processo de tomar e implementar tais decisões. O estabelecimento dos direitos decisórios e das responsabilidades pela TI é feito pela alta gerência da organização, com o intuito final de estimular os comportamentos desejáveis na empresa.

Uma vez que existe a necessidade em estimular comportamentos mais desejáveis, surge uma nova necessidade de se melhorar o ambiente de controles da empresa, o que inclui uma melhor estruturação e eficiência da governança de TI. Nesse âmbito, surge o COBIT, criado pelo ISACA (*Information Systems Audit and Control Association*), que possui o intuito de divulgar, desenvolver, pesquisar e disponibilizar uma biblioteca de boas práticas de TI, padronizada e reconhecida internacionalmente, o que o tornou o guia mais comumente utilizado por gestores de TI. O *framework* é utilizado pelas auditorias internas, mas, também, serve como guia para a análise das auditorias externas quanto à análise do ambiente de TI das companhias auditadas. O COBIT foi desenvolvido para ser guia tanto para usuários, quanto para prestadores de TI e executivos, sendo também um *framework* abrangente para a alta direção e donos de processos de negócio, quando necessitam prover tomada de decisão. Seu tema principal é o foco em negócios e, nessa esfera, baseia-se em alguns princípios, tais como: requisitos de negócios, recursos de TI, processos de TI e informação organizacional, conforme demonstrado na Figura 2.

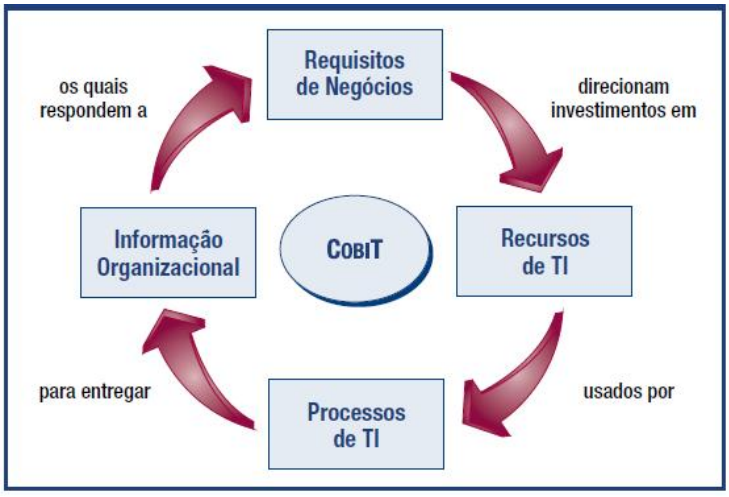

Figura 1 - Princípios básicos do COBIT.
Fonte: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Downloads.aspx.

De acordo com Gherman (2005, p.3):

> [...] COBIT procura ocupar o espaço entre a Gestão de Riscos voltada para o Negócio, atendida , por exemplo, pelo COSO, a Gestão de Serviços em TI , por meio do ITIL, e a Gestão da Segurança da Informação, tratada pela

> BS7799. Esses modelos de gestão consistem de boas práticas específicas segundo sua área foco, e possuem funções complementares.
>
> (GHERMAN, 2005, p.3)

Focada no controle e gerenciamento das informações, a metodologia COBIT contribui para o alinhamento da TI com as necessidades do negócio, sendo, portanto, orientada a processos, possuindo um modelo de procedimentos genéricos com quatro domínios para definir as atividades de TI, sendo: i) Planejamento e organização; ii) Aquisição e Implementação; iii) Entrega e Suporte; e iv) Monitoração.

O primeiro domínio traz estratégias relacionadas ao uso da TI na organização abordam diversos processos, como por exemplo, investimentos, tecnologias, arquitetura, riscos, gerência de projetos e qualidade, etc. Dentre os processo do domínio de Aquisição e Implementação estão a manutenção, substituição e/ou aquisição de hardware e software, o mapeamento e desenvolvimento de procedimentos, a gerência de mudanças, etc. No domínio seguinte encontram-se questões operacionais relacionadas ao uso da TI no atendimento e fornecimento dos serviços para os clientes, bem como as garantias e manutenções. Os processos desse domínio definem os níveis de acordo de serviço, a gestão de fornecedores, a continuidade de serviços, o treinamento aos usuários, a gestão da configuração e dados e demais processos necessários para garantir a disponibilidade de todos os serviços prestados e suportados pela TI. No último domínio, de Monitoração, as principais atribuições relacionadas são as de supervisionar as atividades dos outros processos, bem como coletar e sopesar os dados, de forma a garantir que a estratégia definida pela organização está sendo seguida.

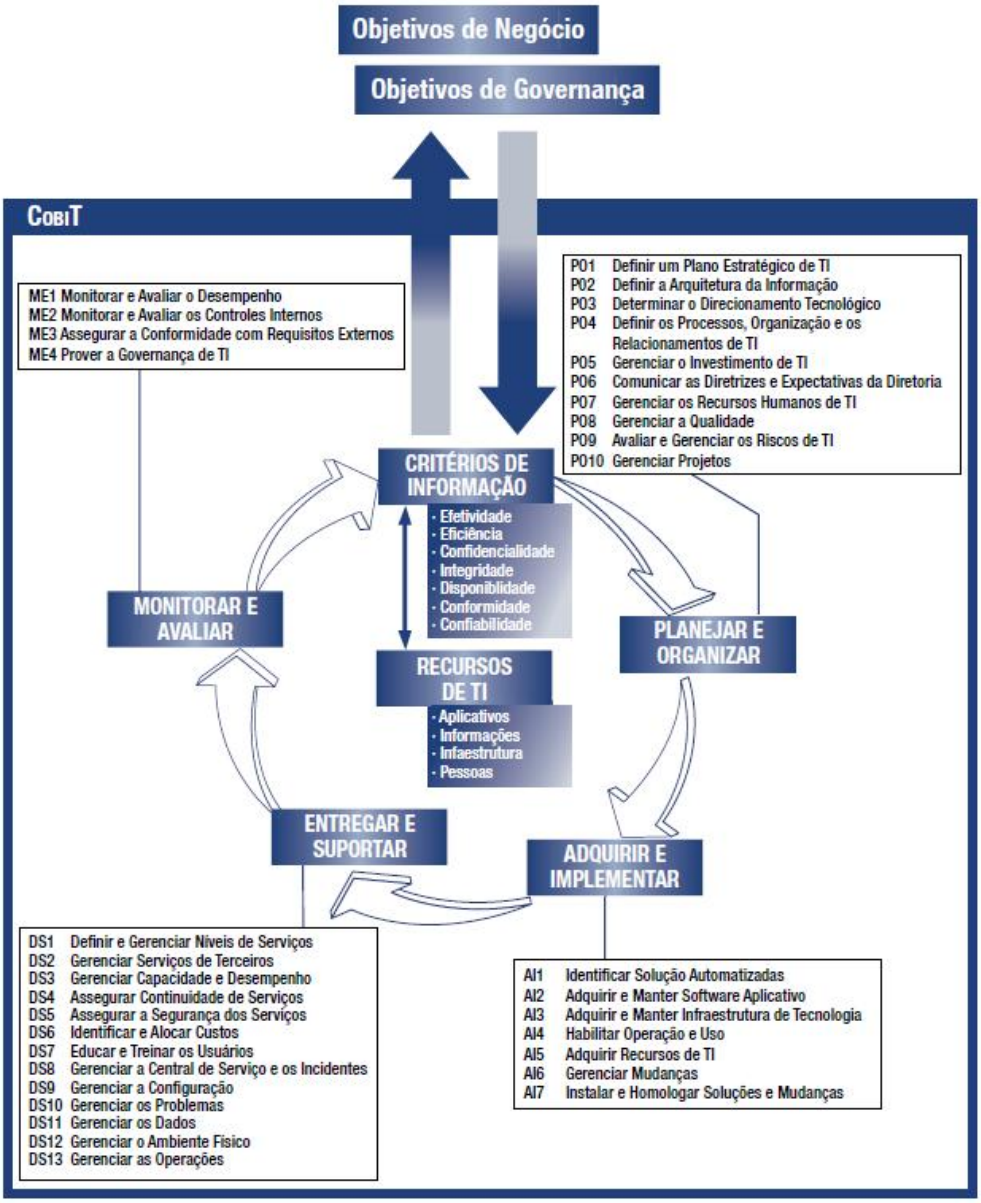

Figura 2 - Visão global do COBIT 4.1
Fonte: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Downloads.aspx.

Através do COBIT, e conforme debatido nas publicações do ITGI (2006) e do ISACA (s.d.), a análise de uma organização está relacionada a avaliação de controles ligados ao ambiente decisório da empresa e de controles voltados à atividade e operação da mesma. O que pode-se perceber é que, mesmo quando trata-se de uma auditoria relacionada a TI, o objetivo é o de avaliar o processo de negócios e não, simplesmente, uma aplicação de maneira isolada.

Os conceitos mencionados acima, relacionados ao COBIT e a avaliação do ambiente de TI das organizações, são comumente utilizados pelas empresas de

auditoria para a prática de auditoria de sistemas, na qual se avalia dois pontos: ITGC (*IT General Controls* ou Controles Gerais de TI) e os *Application Controls* (Controles de Aplicação), sendo o segundo totalmente dependente do primeiro. Pela metodologia apresentada pela EY (2013, p.15) “caso os controles gerais de tecnologias da informação não sejam efetivos e gerem razoável segurança para o auditor, não são necessários procedimentos de análise dos controles aplicação”. Tal afirmação torna-se lógica, uma vez que, para que se tenha razoável segurança quanto aos controles de negócio, mas que são suportados por sistemas informatizados, é necessário que o ambiente de tecnologia, avaliado pelos controles gerais de TI, também seja efetivo. Caso contrário, serão analisados controles e informações que não me trazem conforto quanto a sua integridade.

De modo geral, a auditoria de sistemas se subdivide, de acordo com a EY (2013), em Gerenciamento de Mudanças, Gestão do Acesso Lógico e Operações em TI, a partir das premissas do COBIT. Tal subdivisão também é evidente na norma de auditoria n^{o} 2 do PCAOB (2004) que determina que os ITGCs devam ser categorizados nos componentes de desenvolvimento de programas, mudanças em programas (sendo os dois relativos à Gerenciamento de Mudanças), operações computacionais e acesso a programas (Gestão do Acesso Lógico).

Não foram identificadas, até o momento da elaboração deste trabalho, referências teóricas quanto às diferenças de abordagem no processo de auditoria de sistemas, quando compara-se uma empresa regulada pela Lei Sarbanes-Oxley e uma empresa que segue a mesma regulamentação.

2.2. Controles Auditados e Metodologia COBIT

Este capítulo visa analisar a principal metodologia para avaliação dos controles gerais de tecnologia da informação (ITGC), que é o COBIT. Serão discutidos os principais domínios e pontos analisados por três das quatro principais empresas de auditoria existentes: Ernst & Young, KPMG e Pricewaterhouse Coopers.

O COBIT sinaliza a necessidade de haver governança sobre a operação de TI para um adequado suporte das demonstrações financeiras. Neste sentido, é essencial estabelecer políticas e procedimentos para assegurar que as respostas aos riscos sejam executadas com eficácia. Utilizou-se a versão 4.1 do COBIT para este trabalho.

A gerência de TI deve focar seus esforços na criação e divulgação de políticas e procedimentos que suportem as práticas apropriadas de atividades operacionais (infraestrutura e sistemas), comerciais (contratos de fornecimento e serviços) e de recursos humanos (contratação, retenção e treinamento). No entanto, as políticas e procedimentos não possuem valor se não houver controles implementados para garantir a efetividade destes.

2.2.1 Gerenciamento de Mudanças

Os sistemas de informação são peças fundamentais para a gestão das empresas, pois permeiam todos os setores operacionais das mesmas. Tais sistemas são constantemente aprimorados, atualizados e alterados, expondo as companhias a riscos relacionados a integridade e exatidão de seus dados.

Neste tópico serão apresentados os pontos que envolvem gestão de desenvolvimento e mudanças; com o objetivo de facilitar o entendimento deste tópico, segue, na Figura 3, um fluxo ilustrativo das principais etapas para gestão e controle desses processos.

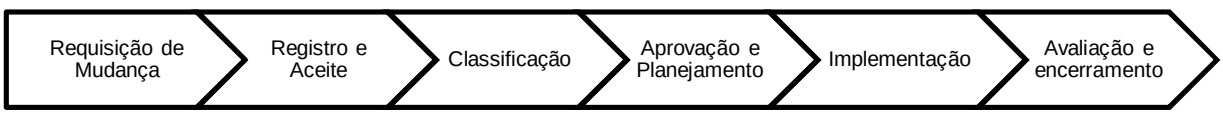

Figura 3 - Principais Atividades – Gestão de Desenvolvimento e mudanças.
Fonte: Fluxo desenvolvido para fins deste trabalho.

Desejável seria que todos os desenvolvimentos e mudanças implementados seguissem fluxo de registro, aceite ou rejeição, classificação, priorização, aprovação, planejamento e avaliação e encerramento.

Um modelo para a gestão eficaz de desenvolvimentos e mudanças é o conjunto de boas práticas e controles do framework COBIT, que objetiva reduzir a quantidade de erros e inconsistências na entrega de produtos e serviços de TI, assim como a redução do retrabalho e o melhor alinhamento com as estratégias de negócio das organizações.

No *framework* a gestão de desenvolvimentos e mudanças é tratada em dois processos dentro do domínio AI (Adquirir e Implementar): i) AI 6 – Gerenciar Mudanças; e ii) AI 7 – Instalar e Homologar Soluções de Mudanças. Ambos os processos estão destacadas na Figura 4:

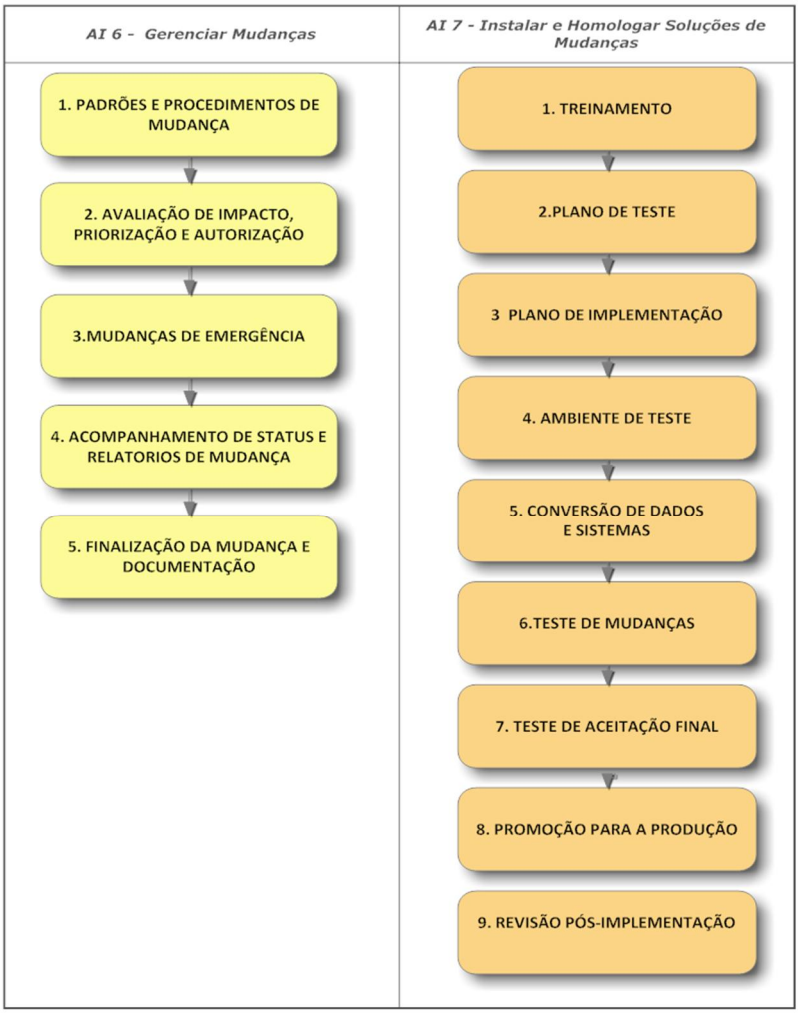

Figura 4 - Processos dos domínios AI 6 e AI 7.

Fonte: COBIT 4.1

A partir do livro COBIT, apresentado pelo ISACA (s.n.t.) é possível verificar que o responsável por TI deve implementar procedimentos e controles para atender aos objetivos de controle do COBIT, resumidos abaixo, que serão auditadas para avaliação de sua efetividade:

- Todas as solicitações de desenvolvimento e/ou mudanças devem ser registradas e formalizadas, preferencialmente através de ferramentas de chamados (Service Desk Tools);
- Todos os desenvolvimentos e/ou mudanças devem ser aprovados por responsável da área de negócio que será impactada;
- Todos os desenvolvimentos e/ou mudanças devem ser documentados e esta documentação retida por período apropriado a ser definido pela empresa, respeitando as boas práticas de mercado;
- Todos os desenvolvimentos e/ou mudanças devem ser testados pelos usuários-chave da área demandante, e a homologação por parte destes usuários deve ser formalizado e registrado;
- Deve ser garantida a segregação de funções entre o desenvolvedor da mudança/programa e o usuário que realizará o transporte para o ambiente de produção (respeitando ainda que os desenvolvedores não tenham acesso ao ambiente de produção e que profissionais com acesso a esse ambiente não tenham acesso ao ambiente de desenvolvimento);
- Todos os desenvolvimentos e/ou mudanças emergenciais devem passar por procedimentos de regularização conforme descrito acima, diferindo das demais demandas apenas pelo tempo em que serão tratados.
- Todos os desenvolvimentos e/ou mudanças devem ser validados pelos usuários após o *go live*.

Adicionalmente, a partir do mesmo Livro COBIT apresentado pelo ISACA (s.n.t.) o auditor buscará obter conforto em seus trabalhos avaliando também o modelo de governança de TI para obter respostas às seguintes perguntas:

- Como a administração assegura que um processo coerente será seguido em todas as mudanças nos sistemas por meio de programas de aplicação, componentes de infraestrutura, unidades de gerenciamento e locais?

- Como a administração documentou e comunicou as políticas e procedimentos de gestão de mudanças?
- Como a administração documentou e comunicou os papéis e responsabilidades da gestão da mudança?
- Como a administração avalia o cumprimento dos controles da mudança no programa implementado?
- Como a administração assegura que a documentação técnica e do usuário serão atualizadas para todos os desenvolvimentos e mudanças em seus sistemas?
- Como a administração assegura que os usuários e o pessoal de TI receberão treinamento adequado sobre quaisquer mudanças significativas nos sistemas corporativos?

Para satisfazer as demandas do COBIT é necessário implementar políticas e procedimentos que garantam que todo o ciclo de gerenciamento de mudanças e desenvolvimentos seja registrado, monitorado e validado pelas pessoas responsáveis.

2.2.2 Acessos a programas e dados

As informações são ativos das companhias, por seu valor inestimável e sua alta importância, o que leva com que uma entidade as resguarde de forma a garantir que não sejam alteradas ou acessadas por pessoas não autorizadas.

Controles deste domínio incluem os processos utilizados pela entidade para adicionar, excluir e alterar o acesso a programas e dados não apenas de funcionários do negócio, mas também o dos profissionais de Tecnologia da Informação. Adicionalmente, contempla a análise dos direitos de acesso, que visa garantir que o acesso foi adequadamente concedido e é restrito, além de verificar se há adequada segregação de funções.

O COBIT, através do ISACA (s.d., p.17), define controle de acesso como “processo que limita e controla o acesso a recursos de um sistema de computador; um controle lógico ou físico com a finalidade de proteger contra entrada ou uso não autorizados [tradução livre pelo autor]”.

Antes de abordarmos, de maneira efetiva, os controles, ressaltamos que a implantação de um adequado modelo de gestão de acessos depende do estabelecimento de procedimentos que expressem, claramente, as diretrizes de segurança de informação da organização. Estas políticas devem conter a classificação das informações e endereçar os controles de acesso lógico (virtual) e físico às mesmas. Os procedimentos operacionais de gestão de acessos devem cobrir todas as fases do ciclo de vida dos acessos dos usuários, desde a inscrição inicial de novos usuários (concessão) até o cancelamento (revogação) do registro de seus perfis, que já não requerem acesso a sistemas de informação e serviços. Além disso, registrar as mudanças ocorridas no período garantindo a rastreabilidade do processo.

Frente ao evidenciado acima, apresentamos, abaixo, os principais pontos de controle na gestão de acessos a programas e dados para garantir a segurança e suportar as demonstrações financeiras de uma organização.

2.2.2.1 Gestão de identidades

Entende-se ser importante para o departamento de TI, implementar e controlar as operações conforme os seguintes objetivos de controle do COBIT DS 5 – Garantir a Segurança dos Sistemas.

Para Gestão de Identidade (DS 5.3) é importante avaliar a necessidade de que os usuários e suas atividades são de fácil identificação e rastreabilidade, de maneira exclusiva. Os direitos de acesso dos usuários aos sistemas e dados devem estar em conformidade com as necessidades dos negócios e com os requisitos da função definidos e documentados.

Já os direitos de acesso devem ser providos pela gestão de usuários, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança, garantindo, ainda, adequada segregação de funções. Cabe ressaltar que as identidades e os direitos de acesso dos usuários devem ser mantidos em um repositório central, sendo monitorados periodicamente, com o intuito de manter atualizadas as contas utilizadas pelos funcionários.

O tema de Gestão de Contas de Usuário (DS 5.4) objetiva garantir que atividades de solicitação, emissão, suspensão, modificação e bloqueio de contas de

usuário e seus privilégios são mantidas e monitoradas de maneira tempestiva, através de validações periódicas de usuários em conjunto com os procedimentos de concessão e revogação de acessos.

Já a Segurança de Rede (DS 5.10) busca por técnicas de segurança que sejam utilizadas para autorizar o acesso e controlar os fluxos de informação entre redes e seus componentes.

2.2.2.2 Segregação de Funções (SoD) e acesso a transações críticas

A segregação de funções consiste, basicamente, na divisão de atividades conflitantes ou incompatíveis entre dois ou mais indivíduos. Os objetivos deste tipo de controle são os de reduzir o grau de exposição ao risco de fraude, erros e omissões, além de reduzir a quantidade de problemas não detectados, limitar as oportunidades de apropriações indevidas e mitigar o volume de erros nas demonstrações contábeis.

Caso a organização não suporte a segregação de funções em todas as suas atividades, independente de seu motivo, é de grande importância que outros controles, como a monitoração das atividades, trilhas de auditoria ou o acompanhamento da gestão, sejam utilizados como controles compensatórios à exposição ao risco.

A existência de um volume elevado de subversões em nível de segregação de funções e acessos críticos indevidos expõe as organizações a riscos de fraudes, erros ou omissões. Estes riscos, caso materializados, podem gerar perdas financeiras e de ativos, além de erros nas demonstrações financeiras e, em um cenário mais pessimista, na paralisação de processos.

Pelos motivos apresentados acima, que surge a recomendação de que sejam realizadas revisões dos perfis de acesso aos sistemas, utilizando-se uma matriz de riscos aderente ao negócio, para tratamento dos conflitos de segregação de funções e acessos a transações (programas) críticas.

Os principais passos para estabelecimento de controles de segregação de funções e restrição de acessos críticos foram demonstrados na Figura 5:

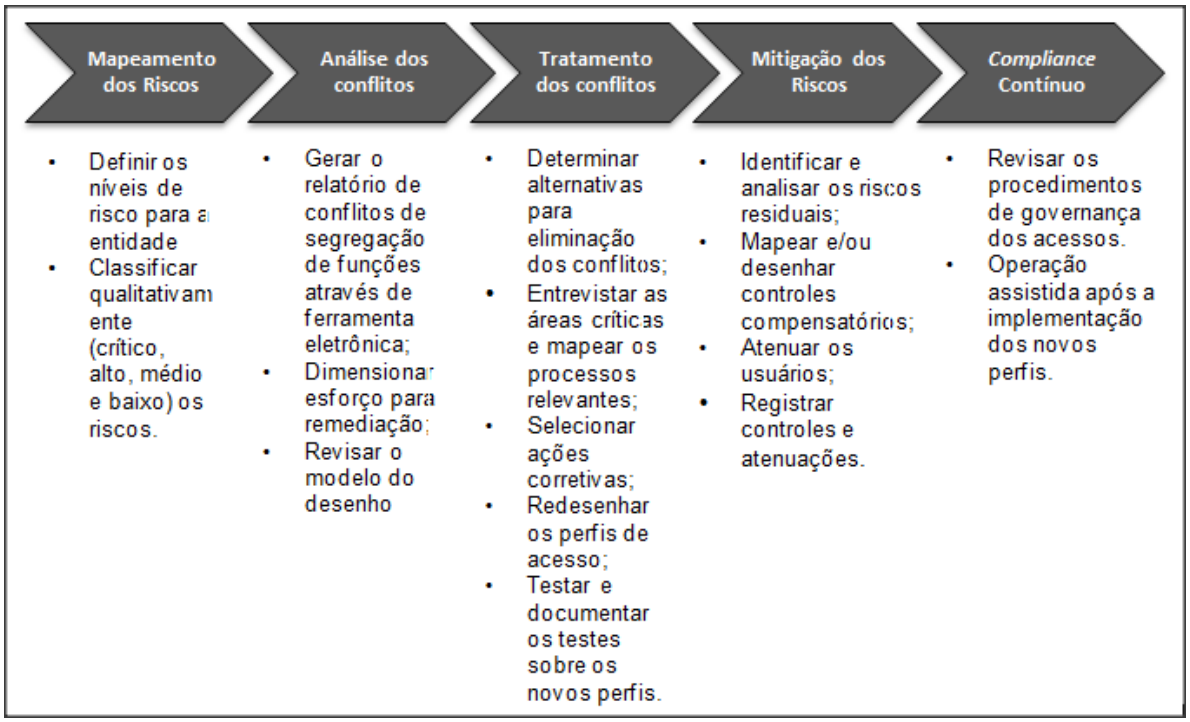

Figura 5 - Estabelecimento de controle de segregação de funções e restrição de acessos críticos.
Fonte: Elaborado pelo autor.

2.2.2.3 Política de Senhas

As políticas de senhas propendem prevenir o acesso indevido a programas e informações decorrentes da invasão através da utilização de senhas de terceiros e deve buscar garantir que as senhas dos sistemas de informação sejam controladas através de um processo de gerenciamento formal, cujo objetivo é garantir a individualidade, confidencialidade, segurança e complexidade das senhas.

É importante criar políticas e procedimentos que estabeleçam parâmetros de senhas e de bloqueio das contas para aumentar a segurança dos controles de acesso lógico aos sistemas de informação e a rede de computadores. Devem-se estabelecer parâmetros de senhas e de bloqueio das contas para aumentar a segurança dos controles de acesso lógico a sistemas e rede de computadores das organizações, como exemplificado no Quadro 2.

Quadro 2 – Boas práticas de mercado em relação à política de senhas.

#	**Descrição**	**Boas Práticas**
1	Comprimento mínimo de senhas	Entre 6 e 8 caracteres
2	Obrigatoriedade de alteração de senha no primeiro acesso	Sim
3	Composição de senhas (caracteres alfanuméricos, palavras proibidas)	Pelo menos uma letra, uma letra maiúscula, um caractere numérico, um caractere especial (#, @)
4	Frequência em que senhas devem ser alteradas	Entre 30 e 90 dias
5	Quantidade de tentativas inválidas de acesso para que contas sejam bloqueadas	Entre 3 e 5 tentativas
6	Possibilidade de usuários alterarem suas senhas	Sim
7	Quantidade de senhas utilizadas para que uma senha antiga possa ser reutilizada	4 a 12 senhas (a ser combinado com a frequência, para que a mesma senha não seja reutilizada em menos de um ano)
8	Tempo de inatividade para o bloqueio da sessão	15 a 30 minutos
9	Geração de logs de tentativas inválidas de acesso	Sim

Fonte: Elaborado pelo autor, baseado no COBIT e nas metodologias das principais empresas de auditoria.

2.2.2.4 Usuários genéricos e compartilhamento de licenças

Todos os usuários de sistemas de informação devem possuir um identificador único (ID de usuário) para uso pessoal e exclusivo. Este princípio deve ser aplicado para todos os tipos de usuários, incluindo administradores de rede, desenvolvedores de sistema e administradores de banco de dados.

O compartilhamento de usuários deve ser combatido com sanções administrativas e deve ser tema frequentemente abordado nas comunicações de segurança da informação, como prática inaceitável para a empresa. Destacamos que os usuários com acessos amplos (administradores e ‘super-usuários’) devem ser registrados, justificados e monitorados, de forma a garantir a segurança dos sistemas de informação.

Ressaltamos que a utilização de contas de usuário genéricas permite acesso irrestrito às transações do ambiente de *Enterprise Resource Planning* (ambiente de Planificação de Recursos Empresariais, tendo sua sigla por ERP), dificultando a identificação de uma pessoa que efetuou um evento indevido nesse sistema integrado de gestão empresarial. Por isso, a utilização de contas de super usuários

genéricos no ambiente de PRD deve ser restrita a situações específicas, com prazos e objetivos monitorados e aprovados pela Administração.

Neste domínio apresentamos os respectivos controles a serem implementados para sustentar uma auditoria de demonstrações financeiras.

2.2.3 Operações Computadorizadas

O objetivo dominante para as operações de informática é assegurar que os sistemas de produção e dados sejam completa e precisamente processados, de acordo com os objetivos de controle da administração, e que os problemas de processamento sejam identificados e resolvidos completa e precisamente para manter a integridade dos dados financeiros.

2.2.3.1 Rotinas automatizadas

As rotinas automatizadas são importante artifício no processamento de dados. O risco associado a estas rotinas se relaciona à possibilidade de falha das mesmas, derivando em corrompimento das bases de dados.

Assim, os controles de programas de execução e processamento em *batch* devem assegurar que as tarefas de produção autorizadas serão adequadamente programadas e monitoradas, e que as exceções serão resolvidas completa e precisamente em acordo com os objetivos de controle da administração. Em relação a rotinas automatizadas a administração de TI deve entender:

- Como a administração assegura que as adições, mudanças e eliminações na programação de tarefas serão autorizadas e concluídas oportunamente?
- Como a administração assegura que as dependências de tarefas e os procedimentos de reinício/recuperação serão documentados para todas as tarefas no programa de execução em batch?
- Como a administração monitora o processamento das tarefas para assegurar que elas serão executadas de acordo com o cronograma aprovado?
- Como a administração assegura que somente o pessoal autorizado terá acesso à ferramenta de execução de tarefas?

Nesta etapa, os controles relevantes a serem implementados tem como objetivo garantir que todas as rotinas automatizadas operem corretamente e que realizem operações aprovadas pela Administração.

Assim, a gerência de TI deve implementar controles que garantam que todas as rotinas computadorizadas sejam aplicadas apenas após testes de operação, formalizados e aprovados pelos gestores das aplicações. Adicionalmente, é importante que seja estudado em que momentos estas rotinas podem ser executadas, tendo em vista que podem influir diretamente no desempenho dos sistemas corporativos.

Os controles sobre rotinas automatizadas se estendem ao monitoramento. Conforme explanado anteriormente, as rotinas devem possuir indicadores de desempenho vinculados à sua execução para que os desvios sejam identificados e, caso sejam necessárias, intervenções corretivas possam ser executadas. Com base neste monitoramento regular será possível planejar futuras alterações do processo para que o mesmo seja cada vez mais eficiente, seguindo um ciclo de desenvolvimento e melhorias.

2.2.3.2 Backup e Planos de Contingência

Os controles de recuperação de desastres são controles operacionais importantes para assegurar que uma organização será capaz de continuar as suas operações em caso de desastre. Os controles de backup e "recuperação" devem assegurar que as exigências de backup sejam definidas para garantir que os dados estejam disponíveis quando necessário, que os problemas que precisam de solução sejam identificados oportunamente e que a "recuperação" desses problemas seja realizada completa e precisamente.

Nesta etapa, apresentaremos as diretrizes para a implementação de um plano de backup e continuidade adequado, apenas. A administração de TI deve-se preocupar em demonstrar ao auditor que possui um processo estruturado e controles sobre essas atividades, como por exemplo, possuir a documentação comprobatória dos testes de recuperação de backups e um plano de contingência divulgado.

O sucesso de um projeto de contingência pode ser representado pela estratégia de segurança efetiva da TI, conscientizando sobre a importância do planejamento e oferecendo serviços que estão diretamente alinhados e relacionados aos processos finalísticos do negócio e essenciais provendo o nível de serviço mínimo que permite executar aquelas aplicações e ou serviços que suportam processos de negócio considerados vitais para uma organização continuar a operar. Integrado por um plano de backup e replicação de dados, o mesmo deve ser acionado sempre que os serviços rotineiros estejam indisponíveis por consequência de algum desastre e ficará ativo até a recuperação da total capacidade de processamento. Definimos como desastre qualquer tipo de invasão, assim como roubo, vírus, ataque de hackers, falha de hardware e comunicação, ambiente, falhas de software, incêndio / enchentes / forças maiores entre outros.

Destacamos como principais objetivos a necessidade de assegurar a sobrevivência do negócio, reduzindo o impacto do desastre ou falha grave e produzindo planos de recuperação para TI que serão integrados ao ambiente de produção. Tudo isso com o menor impacto para o usuário.

O primeiro passo é a pesquisa: ela consiste em uma revisão da estrutura de planos existentes para a área, análise preliminar de risco, definição da base de dados a ser adotadas e caracterização dos aspectos da área que possam afetar as emergências. Definindo as necessidades do plano, tais como, as áreas e serviços cobertos irão conduzir o funcionamento do plano, no que diz respeito a equipamentos, pessoas e informações.

A palavra “*backup*” pode levar a sensação de segurança para a organização, afinal, se alguma coisa ocorrer existe uma cópia dos dados que é possível restaurar. Para que seja possível tratar adequadamente as informações e ter um mínimo de garantia das mesmas, é importante possuir os dispositivos adequados para realizar backup. Deve-se estabelecer uma rotina de backup na qual os dados são armazenados localmente, através de um planejamento dos dados que precisam ser resguardados.

Aplicando uma política de backup, relaciona-se um direcionamento do que será salvo, com qual periodicidade, qual o tempo de retenção dos dados, qual a expectativa de tempo de backup e de restauração. Sugerimos que estes sejam armazenados por um período de garantia, e que qualquer alteração de dados deve

também ser armazenada. Implantando uma política recomendável, deve-se uma cautela para que ao recuperar algum dado, a perda seja a menor possível, causando o mínimo impacto sem a necessidade de refazer o trabalho. Lembrando que toda documentação é necessária, para que seja acompanhado o processo.

Instruímos que seja catalogado como é feito o teste de restauração, realizando uma análise crítica, pois se torna necessário certificar se existem erros nos procedimentos operacionais, assim como as mídias e dispositivos. Garantimos assim a validação do backup. Paneje uma programação semanal, na qual é identificado todos os testes realizados, alternando o tipo de *backup* que é restaurado.

É essencial que seja checado, avaliado a necessidade de mudanças nos procedimentos de backup. Isso ocorre através da auditoria do backup, onde as evidências dos procedimentos e testes são constantemente avaliadas e criticadas, com a finalidade de assegurar que os controles de backup estão efetivos. É imprescindível analisar a janela que está sendo realizado o backup sem comprometer o desempenho e ambiente de produção. O controle deve ser realizado diariamente, e no caso de não ter sido concluído com sucesso, registrar o ocorrido. Muitos dos softwares de backup possuem ferramentas que alarmam um processo não concluído com sucesso, como o envio de e-mail e SMS.

Na avaliação dos riscos levantem os danos que podem ocorrer como resultado de um desastre, conforme citados anteriormente. Os riscos devem incluir os danos potenciais para usuários e negócios e quais devem ser priorizados, quais ações devem ser planejadas e que recursos provavelmente serão necessários.

Para ativarmos um plano, sugerimos que definam em que condições o plano deverá ser ativado. Uma das tecnologias mais comuns é a duplicação do site principal espelhando-o e, um site de backup que, em caso de falha, assume a continuidade da operação com a infraestrutura necessária para manter o ambiente disponível no menor tempo possível.

Neste planejamento, deve-se replicar arquivos, banco de dados e softwares, para que no momento de ativação, torna-se o mais transparente para o usuário.

Um plano de contingência jamais irá eliminar todas as fontes de risco e quantificar o impacto financeiro das crises. Este processo está relacionado com a sobrevivência do negócio e, portanto, é um incremento da confiança dos clientes e usuários, e

também da credibilidade da organização, pois afetam não apenas um sistema, mas todo um ambiente de trabalho. Sem a compreensão e o suporte dos diretores e altos executivos, torna-se impossível implantar uma gestão da Continuidade dos Serviços de TI de forma eficaz.

3 METODOLOGIA

3.1 Estratégia e Método de Pesquisa

Foi realizado um estudo qualitativo, avaliando o processo de auditoria de sistemas para validar os procedimentos utilizados dentro de uma empresa regulada pela SOX e outra que não sofre o mesmo tipo de regulamentação.

O processo de auditoria de sistemas foi realizado pela auditoria independente, como parte do trabalho de auditoria integrada, no caso de uma das empresas – regulamentada pela Lei SOX – já para a outra companhia, como parte do trabalho de auditoria contábil exigido pela CVM.

Para tanto, foi utilizado, como método, um estudo empírico comparando os achados de duas empresas de mineração presentes no interior do estado de Minas Gerais e que possuem o mesmo ERP. As empresas selecionadas possuem grande porte e atuação internacional. Também possuem áreas de TI segregadas em sub linhas de rede, sistemas e infraestrutura, de modo que seja possível manter equipes distintas quanto à especificidade de cada ambiente, evitando, ainda conflitos de segregações de funções relacionados a acesso lógico ou gestão de mudanças.

Para a análise comparativa, foram descritos os procedimentos e resultados de cada um dos trabalhos de auditoria, apresentando, ao final, a comparação entre cada um dos casos, com o intuito de identificar possíveis pontos divergentes.

Para realizar esta análise, foram coletadas, não apenas, informações referentes aos procedimentos de auditoria, mas também registros sobre a maturidade dos controles gerais de TI das duas empresas, uma vez que é ponto crucial da análise em questão.

Com o objetivo de reduzir o risco relacionado a diferenças entre a metodologia e o ambiente de negócio e de TI, selecionamos as empresas para o estudo empírico com base em dois critérios, sendo um, o mesmo sistema de gestão (ERP) e componentes tecnológicos e, o outro, a mesma empresa responsável pela auditoria externa.

O primeiro critério se deu com o objetivo de reduzir divergências relacionadas aos componentes tecnológicos envolvidos e ao sistema de gestão da empresa. Para tanto, foram escolhidas duas empresas cujo sistema fosse o SAP, o sistema operacional Linux e o banco de dados Oracle. Já o segundo critério foi adotado com

o objetivo de reduzir divergências relacionadas à metodologia de análise / auditoria. Para tanto, foram escolhidas empresas auditadas pela mesma empresa de auditoria externa, no caso em questão a EY.

Foram avaliados os procedimentos de auditoria utilizados no trabalho, além dos pontos de melhoria identificados em cada empresa, de modo que seja possível comparar o que foi analisado e identificado em cada uma das mineradoras. Objetivou-se verificar se existem diferenças significativas entre procedimentos de auditoria para as duas empresas.

3.2 Estratégia de Coleta de Dados

Todas as informações dispostas no estudo empíricos foram obtidas através de análise dos papéis de auditoria da EY, além de entrevista junto ao gerente Sr. João Carlos Ervilha, responsável pelos trabalhos de auditoria externa nas duas mineradoras, no que tange a análise de sistemas.

Para a análise em questão foram utilizados os seguintes métodos de coleta de dados: observação direta, análise documental e entrevista com o gerente responsável pela condução dos trabalhos de Auditoria Independente de Sistemas. A observação direta consistiu em avaliar *in loco* os procedimentos adotados pela auditoria independente, sua abordagem e o resultado dos mesmos, verificando se existe adoção de procedimentos distintos para uma empresa regulada pela Lei SOX e outra não regulada.

A análise documental auxiliou na identificação do método utilizado na avaliação de cada um dos procedimentos de auditoria, avaliando os resultados e a profundidade de análise de cada um dos itens verificados durante os trabalhos. Para tanto, foram analisados os papéis de trabalho de auditoria nas duas empresas, sendo vinte e sete diretamente referenciados neste documento. A lista consta no APÊNDICE A.

Por fim, a entrevista com o gerente responsável pelo trabalho de Auditoria de sistemas, visou levantar e avaliar os pontos críticos de cada passo da auditoria, além de verificar como são levados os pontos à equipe de auditoria financeira para composição do trabalho de auditoria independente.

Esses métodos utilizados de maneira conjunta trouxeram maior rigor à avaliação do estudo empírico, dando maior segurança quanto aos resultados

obtidos. Adicionalmente, foi possível cumprir com o objetivo do trabalho de avaliar os procedimentos de auditoria independente relativos a sistemas de informação e como os mesmos são tratados em empresas reguladas pela Lei Sarbanes-Oxley e empresas não reguladas pela SOX, através do COBIT. Isto se deu pelo atingimento de todos os três objetivos específicos apontados na introdução do trabalho.

3.3 Estratégia de Análise de Dados

Os dados foram analisados através de um estudo inter casos, sendo descrito todos os procedimentos para cada uma das empresas selecionadas e, ao final, será criado um comparativo entre o que foi analisado.

4 ESTUDO EMPÍRICO

Neste capítulo será apresentado um estudo empírico comparativo entre duas mineradoras presentes no estado de Minas Gerais, sendo uma regulada pela Lei SOX e outra que não precisa cumprir as determinações impostas pela lei.

Para tanto, o presente capítulo está subdividido em três partes, sendo a primeira uma caracterização do ambiente de TI da empresa A, enquanto a segunda, refere-se ao ambiente de TI da empresa B. Por fim, uma comparação entre os procedimentos de auditoria utilizados em cada companhia.

4.1 Caracterização do ambiente de TI da Empresa A

A empresa A é uma organização nacional, fundada na década de 70, com operação no Brasil e no continente africano. A mineração é o principal ramo de atuação, mas atua também no segmento de construção pesada. Essa companhia não é regulamentada pela Lei SOX, uma vez que não negocia ações em bolsas de valores americanas. No entanto, auditorias de demonstrações financeiras são realizadas anualmente, por se tratar de uma empresa de capital aberto e se submeter à regulamentação da Lei das S/A (Lei 6.404/76, alterada pela Lei 11.638/07). O processo de auditoria das demonstrações financeiras inclui a avaliação do ambiente de tecnologia da informação e de seus controles, de forma geral, que é a avaliação dos processos e dos controles de aplicações específicas.

No ano de 2013, o escopo da auditoria de sistemas incluiu controles relativos à Gerenciamento de Mudanças e Gestão do Acesso Lógico. Serão detalhados a seguir os controles utilizados pela Empresa A no âmbito desses processos.

No que diz respeito à Gerenciamento de Mudanças, a necessidade por qualquer tipo de desenvolvimento e melhoria é identificada pela área usuária, podendo ser classificadas como mudanças rotineiras, configuração de parâmetros, mudanças emergenciais, correções de erros ou aplicações de pacotes. Os desenvolvimentos e customizações são realizados de duas formas. Mudanças de baixa complexidade são analisadas e tratadas por equipe interna, enquanto alterações que demandem maiores recursos ou que possuam maior complexidade são destinadas a fornecedores contratados.

O processo de gerenciamento de mudanças que suporta o sistema SAP tem início com a abertura de chamado em uma ferramenta de *Service Desk*, no qual o profissional da área usuária informa a descrição da mudança necessária e o prazo desejado para ser disponibilizada em produção. Após o recebimento da solicitação, a equipe de TI gera um formulário com o objetivo de documentar as especificações funcionais e técnicas, além de registrar o resultado dos testes e autorizações realizadas pelo usuário chave para entrada em produção. Para tanto, é solicitada a assinatura do usuário chave ou gestor responsável pela área solicitante, com o objetivo de formalizar a autorização para o desenvolvimento da mudança (documento 1, APÊNDICE A).

Para validação das mudanças desenvolvidas, testes são realizados, em ambiente específico de homologação, pela área solicitante, sendo os mesmos validados e formalizados através de preenchimento e assinatura de campos específicos do formulário supracitado. Caso alguma alteração seja reprovada na fase de testes, o processo de homologação é reiniciado.

Com base na aprovação dos testes realizados pela área usuária, o gestor de TI corrobora a aprovação para entrada em produção da mudança por meio de assinatura de campo específico do formulário. Após finalizado o fluxo de aprovações dos testes e de entrada em produção, o analista *basis* da empresa verifica se a documentação e as aprovações estão adequadas e realiza o transporte da mudança para o ambiente produtivo do sistema SAP.

Para avaliação do processo detalhado, a auditoria, primeiramente, acompanhou a extração das tabelas E070 e TPLOG e as comparou de modo para verificar se todas as mudanças colocadas em produção constam na lista das mudanças desenvolvidas. Objetivou-se validar que nada foi colocado diretamente em produção. Tendo o conforto de que nenhuma mudança foi aplicada diretamente em produção, a auditoria independente, realizou uma avaliação do processo, através dos formulários descritos acima, de modo a ter razoável segurança de que todas as mudanças foram devidamente solicitadas, testadas e aprovadas para serem aplicadas em produção.

Adicionalmente, verificou-se um procedimento de monitoramento de mudanças realizado pela equipe de TI da empresa A, que possui a finalidade de validar se todos os passos do processo de gerenciamento de mudanças, como

autorizações, testes e aprovações foram corretamente documentados para as mudanças transportadas para o ambiente de produção. O procedimento é realizado semanalmente e todas as validações dos passos do processo são documentadas em formulário específico.

O monitoramento descrito acima foi avaliado pela auditoria independente através da verificação das atas de reunião do comitê criado para avaliar o processo, conforme descrito no papel de trabalho “Empresa A - Monitoramento de Mudanças” (documento 2, APÊNDICE A). Tal comitê é composto pelo gestor da TI, um analista de rede, um analista de infraestrutura e um analista de sistemas.

Validou-se, ainda, se as mudanças presentes no referido documento possuíam o formulário de criação da mudança e se constavam nas tabelas E070 e TPLOG.

Apesar da documentação referente ao processo de mudanças para a empresa A (documentos 1 e 2, APÊNDICE A), na qual foi verificado que os controles estão sendo operados de maneira adequada, além de um monitoramento eficiente, verificou-se que a empresa não possui equipes de desenvolvimento e produção adequadamente segregadas, visto que os analistas *basis* da empresa, responsáveis por transportar as mudanças para o ambiente de produção do sistema, também possuem a permissão para desenvolver mudanças relacionadas à alterações e criações de parametrizações de complexidade baixa no sistema (documento 3, APÊNDICE A).

A auditoria independente chegou a essa conclusão ao verificar as permissões de acesso ao diretório de produção da aplicação. A partir da execução de comandos no Linux, validados pela equipe de auditoria, extraiu-se a lista dos grupos e usuários com permissões de escrita e execução no diretório de produção e foram identificados grupos e usuários distintos com as mesmas permissões em ambos os diretórios.

Considerando o problema identificado acima, a auditoria independente optou por realizar procedimentos complementares, analisando e realizando testes de controles compensatórios existentes na empresa, que pudessem mitigar os riscos da inadequada segregação de função.

Primeiramente, foi realizada uma verificação se o processo de mudanças, em si, apresenta adequada segregação de funções. Para tanto, as mudanças

analisadas anteriormente foram verificadas e a auditoria avaliou se os profissionais responsáveis por desenvolverem cada uma delas eram os mesmos que realizavam o transporte e aplicação em produção. Para esta análise, foi realizado novo batimento das tabelas E070 e TPLOG. A partir desta verificação, foi constatado que, mesmo que as equipes de desenvolvimento e produção não sejam segregadas, os profissionais responsáveis por desenvolver e transportar cada mudança para produção são distintos.

Adicionalmente, um segundo controle compensatório foi avaliado. Identificou-se a existência de um comitê que realiza acompanhamento e validação mensal das mudanças aplicadas em produção. o monitoramento inclui validação dos logs de migração ao ambiente de produção, e avaliação da adequação dos profissionais responsáveis pelo desenvolvimento e transporte. Tal comitê é composto pelo gestor de TI, analistas de sistemas e infraestrutura.

Para avaliar a efetividade do comitê, a auditoria independente realizou uma verificação de todas as atas geradas pelo comitê durante o período e da documentação suporte da avaliação realizada pelo comitê. Adicionalmente, verificou-se o log de transporte para produção das mudanças avaliadas anteriormente, de modo que fosse possível garantir que, efetivamente, o comitê realiza avaliação de tudo o que é migrado para produção. Todos os procedimentos descritos adicionais, descritos acima, foram verificados no documento “Empresa A - Comitê de Mudanças” (documento 4, APÊNDICE A).

Desta forma, mesmo que tenha sido identificada uma falha em segregação de funções, a auditoria independente, através dos procedimentos adicionais, descritos acima, possui razoável segurança quanto ao processo de gerenciamento de mudanças para a empresa A. Isso se deu, pois a auditoria conseguiu reduzir o risco relacionado à aplicação de uma mudança sem o devido registro e avaliação.

Com base nos procedimentos de auditoria descritos acima e no ambiente analisado, verificou-se que o resultado da auditoria, no que tange o processo de gestão de mudanças, necessita de melhorias relacionadas à Segregação de Funções, mas foi considerado eficaz devido aos fatores mitigantes existentes, também apresentados acima. Essa conclusão foi documentada na Carta de Recomendações entregue à empresa (documento 5, APÊNDICE A).

Quanto à análise da Gestão de Acesso Lógico, primeiramente foi solicitado que a empresa rodasse *scripts* em seu sistema operacional e banco de dados, de modo que os mesmos coletassem informações quanto ao ambiente. A partir do resultado, a equipe de auditoria realizou análises quanto aos acessos nesses componentes de infraestrutura, avaliando pontos técnicos que permeiam acessos via FTP (*File Transfer Protocol* ou Protocolo de Transferência de Arquivos), até configuração de senhas. Não foram identificados desvios quando comparado a melhores práticas de mercado[1] (documento 6, APÊNDICE A).

Adicionalmente, avaliou-se que o sistema possui parâmetros de senhas implementados, garantindo maior segurança e evitando acessos não autorizados. As configurações parametrizadas no sistema SAP foram verificadas através de análise da tabela RSPARAM, extraída diretamente do sistema. Avalia-se, nesse ponto a existência de complexidade de senhas, obrigatoriedade de alteração no primeiro acesso, *time out*, dias para alteração da senha, entre outros (documento 7, APÊNDICE A).

O acesso às funções de administração do sistema SAP é realizado através de transações críticas do sistema, restritas ao analista *basis*. Além disso, o acesso de administrador aos elementos de infraestrutura, como banco de dados e sistema operacional, que suportam o sistema SAP, é restrito aos profissionais apropriados da área de TI.

É importante ressaltar que o processo de concessão de acesso a este tipo de usuário segue o mesmo fluxo de autorizações existente para um usuário comum da aplicação. Por isso, não existe qualquer tipo de indicação que o usuário é privilegiado e também não são necessárias aprovações adicionais.

Para essa análise, foi solicitada a listagem dos profissionais que possuem perfil administrador (ou analista *basis*), de modo a validar o cargo ocupado por cada um desses profissionais e se, realmente, necessitavam deste tipo de permissão. Objetiva-se validar que apenas profissionais habilitados possuem perfil privilegiado.

Foi realizado, para tanto, uma comparação da listagem citada, com a lista de funcionários ativos da empresa, para identificar os analistas. Verificando que todos

[1] Melhores práticas de auditoria não são conceitos únicos formados no mercado, porém, são definidos com base nos resultados obtidos em outros trabalhos de auditoria, que apresentaram resultado satisfatório.

eram membros da equipe de TI da companhia, foi solicitada uma validação, por parte do gestor de TI da empresa, que tais profissionais necessitavam daquele tipo de acesso para exercício de suas funções na companhia.

Cabe ressaltar que, conforme documentado no papel de trabalho do controle em questão (documento 8, APÊNDICE A), tal avaliação não ficou restrita aos procedimentos acima, uma vez que, na análise dos controles de concessão de acessos, serão avaliados os usuários que efetuaram a inclusão do novo usuário, de modo a validar que apenas usuários *basis* realizaram tal ação.

Adicionalmente, junto com os perfis administradores, foram avaliados os usuários genéricos, aqueles cujos usuários não estão vinculados diretamente a nenhum funcionário. Para tanto, a auditoria independente, através de batimento com a lista de funcionários ativos da empresa, levantou quais usuários não possuíam esse vínculo e questionou a gestão da empresa sobre a necessidade de tais acessos. Após validação e verificação das permissões vinculadas a tais perfis, a auditoria independente concluiu que tais usuários eram necessários e suas permissões, condizentes. Tal conclusão foi documentada em papel de trabalho (documento 8, APÊNDICE A).

O processo de concessão de acesso para o sistema é realizado através da abertura de chamado na ferramenta de *Service Desk*, onde o profissional da área usuária informa a necessidade de criação de acesso ao sistema. Após o recebimento da solicitação, a equipe de TI gera um formulário referente ao chamado aberto na ferramenta e solicita o preenchimento do perfil a ser adicionado utilizando-se de um perfil espelho. Além disso, são colhidas as assinaturas de aprovação do gestor responsável pela área do usuário solicitante, do executor e do gerente de TI.

Por fim, após finalizar o fluxo de detalhamento e aprovação do acesso solicitado, o analista *basis* realiza a criação do novo usuário no sistema em conformidade com solicitação realizada.

A equipe de auditoria de sistemas realizou uma avaliação do processo, de modo a validar que os procedimentos descritos foram devidamente executados. Para tanto, realizou uma seleção aleatória, com base na metodologia de amostragem (ANEXO A), e para os itens selecionados, solicitou os formulários de criação, bem como verificou a existência de chamado na ferramenta de *Service Desk*. Como foi identificada que a criação dos usuários era baseada em usuários

espelho, para cada novo acesso, foram analisadas, ainda, as permissões do novo usuário e compararam às permissões do acesso existente, como forma de validar que o mesmo foi realizado corretamente e sem desvios. Caso fosse identificada alguma divergência no batimento realizado, era solicitado o chamado e formulário de concessão ou revogação das demais permissões divergentes. Todos procedimentos foram documentados em papel de trabalho (documento 9, APÊNDICE A), sem apontar qualquer desvio em relação ao que foi explicitado pela equipe de TI da empresa auditada.

Além do que foi exposto, avaliou-se a existência de Segregação de Funções, uma vez que as pessoas que solicitam a gestão dos acessos não são as mesmas pessoas que executaram as operações, conforme documentado no papel de trabalho “Empresa A - SoD em Gestão de Acessos” (documento 10, APÊNDICE A). Eventualmente, caso seja um acesso da TI, o gestor aprova a solicitação antes da execução e os analistas responsáveis pela gestão são distintos dos que solicitaram. Cabe ressaltar que não foi elaborada uma matriz de segregação de funções pela equipe de auditoria de sistemas, uma vez que a mesma foi criada pela equipe responsável pelo trabalho de controles internos.

Já o processo de revogação de acessos se dá a partir do momento em que ocorre o desligamento de um funcionário na empresa; a área de RH atualiza as informações referentes ao desligamento do funcionário no sistema de recursos humanos, o qual envia um e-mail automático para o analista *basis*, informando o nome, a matrícula e data de desligamento do profissional.

Posteriormente, com base nas informações do e-mail, o analista *basis* possui a responsabilidade de confirmar se o funcionário desligado possuía acesso ao sistema SAP com o objetivo de revogar o seu acesso do sistema.

Como forma de validar o processo, a equipe de auditoria procedeu com dois testes, sendo o primeiro, o batimento entre a lista de funcionários desligados, com a lista de usuários ativos no sistema; não foi identificado nenhum profissional desligado cujo acesso permanecia ativo no sistema, conforme disposto no documento “Empresa A - Revogação de Acessos” (documento 11, APÊNDICE A). Já o segundo teste consistia de uma avaliação de uma amostra de profissionais desligados no período auditado, com o objetivo de validar que o fluxo descrito para revogação de acessos existia e era efetivo. Conforme documentado (documento 11,

APÊNDICE A), nenhum dos itens selecionados na amostra apresentou desvios ao que foi narrado, portanto, o processo de revogação de acessos foi considerado efetivo.

Adicionalmente, a empresa possui 2 (dois) controles de monitoramento dos acessos: i) validação periódica de acessos; e ii) monitoramento de trilhas de auditoria. O primeiro ocorre semestralmente, onde a TI gera listas aos gestores, contendo o nome do profissional e todas as transações que o mesmo possui acesso, que validam se os acessos encontram-se pertinentes ou necessitam de ajustes. Para avaliação do controle, a equipe de auditoria de sistemas realizou uma amostragem (conforme descrita no ANEXO A), selecionando itens para compor o teste. Avaliou-se a validação dos acessos por parte do gestor e, caso o mesmo tenha solicitado alguma alteração, verificou-se se o perfil do profissional refletia o que havia sido solicitado pelo seu gestor, através do batimento com a lista de usuários / permissões do SAP (detalhes analisados a partir do documento 13, APÊNDICE A).

Já o segundo monitoramento ocorre apenas sob demanda, caso desejem avaliar quais os acessos e quais alterações foram realizadas no sistema. Cabe ressaltar que existe um controle semanal de verificação de tentativas inválidas de acesso e seu respectivo horário, com o objetivo de detectar alguma tentativa de penetração no sistema. Considerando que tal controle não é realizado de forma periódica e não possui escopo definido para monitoramento, não foram realizados procedimentos de teste e o mesmo foi considerado ineficaz, sendo reportado na Carta de Recomendações à Gestão (documento 5, APÊNDICE A).

Quando ocorre uma transferência entre cargo/área de algum profissional na empresa, o gestor da área que receberá o profissional, abre um pedido de transferência na ferramenta FAT que dispara um e-mail automático ao RH e à TI. Caso seja necessário alterar o perfil de acesso do usuário no sistema SAP, a TI realizará um procedimento de readequação dos acessos, ou seja, revogação de acessos inadequados e concessão de novos acessos, sendo documentado em formulário específico, com as devidas assinaturas.

Não obstante, conforme metodologia da EY (2013) caso o controle de monitoramento / validação de perfis de acesso seja realizado com periodicidade mínima semestral e o mesmo seja considerado eficaz, não é necessário realizar

procedimentos de teste e coleta de evidências para o controle de usuários transferidos, uma vez que o risco relacionado a transferência de acessos será coberto e mitigado pelo controle de validação periódica de perfis.

Tal justificativa foi documentada em papel de trabalho que contém todas as narrativas dos controles analisados (documento 12, APÊNDICE A).

Verificou-se, ainda, a existência de um controle de acessos físicos ao *data center* da companhia, que é realizada via biometria, cujo acesso só é liberado através de formulário físico preenchido. Mensalmente são feitas revisões dos acessos à sala de servidores, para verificar se apenas profissionais habilitados tiveram acesso ao local.

Para validação do acesso, a equipe de auditoria solicitou a listagem dos profissionais cadastrados a acessar o local e o log de acessos ao local, durante o período auditado. Para teste, a equipe de auditoria realizou batimento entre as listas a fim de identificar possíveis acessos indevidos. Verificou-se, porém, que, caso algum profissional acessasse o local, demais pessoas que o acompanhassem poderiam acessar o ambiente sem o devido registro. Considerando o ponto, foi levada a recomendação de melhoria à gestão de modo a reduzir o risco relacionado ao acesso físico, sendo, o mesmo, reportado na Carta de Recomendações à Gestão (documento 5, APÊNDICE A).

Por fim, avaliou-se a existência de normas e procedimentos envolvendo toda a Gestão de TI, sua periodicidade de atualização e adequabilidade em relação à governança em tecnologia da informação. Verificou-se que existe um procedimento de revisão periódica das políticas que fazem parte do processo de Gerenciamento de Acesso Lógico, a fim de avaliar se os mesmos são seguidos e/ou encontram-se atualizados em relação ao ambiente de TI. Foi avaliado se existiam revisões internas de aderência dos procedimentos executados às políticas de segurança, revisões periódicas de políticas e procedimentos operacionais de TI, revisões de patamares mínimos de segurança, revisões da avaliação de riscos de TI e gerenciamento de patches e atualizações de segurança. Adicionalmente, avaliou se os mesmos estavam sendo devidamente utilizados pelos profissionais da companhia.

A equipe de auditoria avaliou as políticas e verificou que todos os documentos encontravam atuais, com as indicações da última revisão, além de estarem aderentes à prática da empresa.

Com base nos procedimentos de auditoria descritos acima e no ambiente analisado, verificou-se que o resultado da auditoria, no que tange o processo de gestão de acessos, necessita de melhorias relacionadas ao monitoramento de trilhas de auditoria, bem como melhorias no acesso físico ao *Data Center.* Independente dos pontos levantados, o ambiente foi considerado eficaz devido aos demais controles existentes e do risco relacionado a cada um dos controles; os riscos de cada análise são determinados pela auditoria com base em uma avaliação de impacto e probabilidade de ocorrência de cada ponto e apresentado à companhia na Carta de Recomendações (documento 5, APÊNDICE A).

Os controles relacionados a Operações de TI não foram avaliados para essa empresa, pois, de acordo com o Gerente responsável pela Auditoria de Sistemas, Sr. João Carlos Ervilha, isso seu deu pelo fato de não se tratar de uma auditoria integrada, ou seja, não trata-se de um trabalho cujos auditores necessitam emitir sua opinião sobre Demonstrações Financeiras e Controles Internos, da mesma forma como é determinado pela Lei SOX, sendo necessário que o auditor opine, apenas, quanto ao primeiro ponto citado (DFs). Dessa forma, diferente de empresas cuja auditoria é integrada, o risco de auditoria é menor, uma vez que o auditor não precisa opinar sobre os controles internos da companhia. Adicionalmente, a avaliação de risco das contas da companhia, não apontou nenhum controle que fosse atrelado a interfaces sistêmicas que fossem relevantes ou materiais. Não existem rotinas automatizadas executadas que gerem e/ou tragam informações relevantes ao processo de fechamento contábil. Ademais, caso haja interrupções ou problemas nos procedimentos de *backup* e *restore*, o risco relacionado a essas falhas são mitigados através de testes manuais substantivos de auditoria, sem qualquer tipo de prejuízo à análise das contas da companhia.

4.2 Caracterização do ambiente de TI Empresa B

A empresa B é uma multinacional, que após algumas fusões, aquisições e incorporações, têm sua participação no Brasil, através de sua razão social atual, desde o início dos anos 2000. Esta empresa possui atuação global, sendo atuante em países das Américas, África e Oceania; possui ações sendo negociadas em bolsas norte americanas e, portanto, sofre regulação em relação à Lei SOX.

Em seu processo de auditoria de sistemas foram analisados os controles relativos à Gerenciamento de Mudanças, Gestão do Acesso Lógico e Operações em TI.

Quanto ao processo de gerenciamento de mudanças (documento 14, APÊNDICE A), as alterações no sistema são solicitadas via ferramenta de controle de chamados, porém a mesma é um pacote de mercado e não possui fluxo de aprovações. Desta forma, todas as aprovações são feitas através de e-mail e anexadas ao chamado.

As solicitações são encaminhadas para os analistas de desenvolvimento que analisam o problema e encaminham um e-mail para o fornecedor, informando os detalhes da alteração solicitada. Tal procedimento é realizado quando se trata de mudanças complexas (novos projetos), como a implantação de um novo módulo ou novas funcionalidades. Para solicitações de customizações simples, como alterações de relatórios, alterações de taxas de juros, entre outras, que seguem o mesmo fluxo descrito anteriormente, porém, não são encaminhadas ao fornecedor, sendo realizadas diretamente pelos analistas de desenvolvimento da empresa.

Finalizado o desenvolvimento das mudanças solicitadas são realizados testes em ambiente específico de homologação, com a participação da área usuária e dos analistas de desenvolvimento. Além disso, também são realizados testes em caso de nova versão ou *release* disponibilizados pelo fornecedor.

O aceite do usuário evidenciando a realização dos testes é feito através de e-mail, anexado ao chamado e, posteriormente, as mudanças são direcionadas aos analistas de produção do sistema, de forma que as atualizações possam ser migradas para produção.

Cabe ressaltar que não existem testes para alterações de registros de banco de dados. Quando necessária esse tipo de alteração o analista responsável pela mudança envia e-mail ao gerente solicitando aprovação para alterar direto em produção, não sendo evidenciados testes para este procedimento em ambiente de homologação de forma prévia.

Para que as mudanças sejam transportadas para o ambiente de produção, é necessário que os analistas de desenvolvimento finalizem a atividade na ferramenta de chamados e, em seguida, registrem uma atividade de transporte para produção que é direcionada aos analistas de produção.

Após o transporte, os analistas de produção registram na própria ferramenta as atividades realizadas e encerram o chamado, através da qual é possível monitorar e controlar as solicitações de transporte das mudanças para o ambiente de produção.

Para avaliação do processo, a auditoria, primeiramente, acompanhou a extração das tabelas E070 e TPLOG e as comparou de modo para verificar se todas as mudanças colocadas em produção constam na lista das mudanças desenvolvidas. Objetivou-se validar que nada foi colocado diretamente em produção. Tal procedimento foi idêntico ao realizado para a empresa A.

Tendo o conforto de que nenhuma mudança foi aplicada diretamente em produção, a auditoria independente, realizou uma avaliação do processo, através dos chamados descritos acima, de modo a ter razoável segurança de que todas as mudanças foram devidamente solicitadas, testadas e aprovadas para serem aplicadas em produção.

Mesmo identificando uma fragilidade no processo de mudanças, uma vez que as aprovações são realizadas via e-mail e anexadas aos chamados, através de amostragem (vide ANEXO A), selecionou-se itens para compor a base de testes e verificou-se que em todos os chamados, solicitação, teste e aprovação estavam anexados.

Adicionalmente, os analistas de desenvolvimento também preenchem um formulário de controle de atualizações, contendo o resultado da implantação, ou seja, o número do chamado na ferramenta, o impacto da mudança, planejamento, plano de implantação, plano de teste, plano de migração, plano de falha na instalação e plano de comunicação. Posteriormente, estes formulários são assinados pelo analista de desenvolvimento responsável e pelo gerente de TI e armazenados em pastas dentro da sala de TI.

A equipe de auditoria de sistemas buscou, para cada mudança selecionada anteriormente, os formulários citados, a fim de incrementar a análise do controle de teste / homologação das mudanças e compor o teste de monitoramento de mudanças.

O processo de mudanças emergenciais ocorre da mesma forma que o processo de mudanças nos sistemas descrito acima, contendo, inclusive, os mesmos níveis de autorização. A única diferença é que, caso seja confirmada a

urgência em um desenvolvimento, este é priorizado pelos analistas de negócio em relação às outras mudanças, conforme documentado em papel de trabalho (documento 14, APÊNDICE A)

Para a gestão e controle das mudanças, ocorre mensalmente uma conferência das alterações / manutenções realizadas, a qual é documentada através do relatório de Gerenciamento de Mudança (Implantação e Atualização de Programas, Sistemas, Infraestrutura) – documento 15, APÊNDICE A – listando as ocorrências do mês em questão, contemplando: segmento, categoria, número do registro na ferramenta de chamados, descrição da mudança e a data de implantação. Esse relatório é assinado pelo gerente de TI, e anexado junto às demais evidências do processo de gestão de mudanças, caso seja necessário, e armazenado no armário da área de TI.

A equipe de auditoria verificou a totalidade dos relatórios, validando se os mesmos possuíam todas as informações das mudanças, bem como os anexos. Verificou-se, ainda, se existia a assinatura do gestor para cada relatório. Objetivou-se validar que o controle de monitoramento das mudanças é devidamente realizado e documentado.

Adicionalmente, verificou-se que a empresa possui adequada segregação de funções no processo de gestão de mudanças, de forma que, quando existe a necessidade de mudança de versão, o desenvolvimento é feito por fornecedores externos, sendo a equipe interna responsável por atualizar o ambiente de produção com as respectivas atualizações. Além de validar se existe adequada segregação de funções no processo, a equipe de auditoria realizou conferência quanto às permissões de escrita e execução nos diretórios de produção. Através do acompanhamento da execução de comandos no Linux, foi possível validar que nenhum usuário ou grupo com acesso ao diretório de produção, possui, também, acesso ao diretório de desenvolvimento. Todo o processo de avaliação de segregação de funções em Gestão de Mudanças foi documentado em papel de trabalho, consultado para execução deste estudo (documento 17, APÊNDICE A).

O procedimento executado acima foi igual ao adotado junto a empresa A, portanto sem divergências quanto a metodologia empregada na análise do controle de segregação de funções.

Com base nos procedimentos de auditoria descritos acima e no ambiente analisado, verificou-se que o resultado da auditoria, no que tange o processo de gestão de mudanças, necessita de melhorias relacionadas à formalização das autorizações e aprovações, uma vez que são realizadas via e-mail. Independente do ponto levantado, o ambiente foi considerado eficaz devido aos demais controles existentes e do risco relacionado a cada um deles; os riscos de cada análise são determinados pela auditoria com base em uma avaliação de impacto e probabilidade de ocorrência de cada ponto e apresentado à companhia na Carta de Recomendações (documento 16, APÊNDICE A).

Quanto ao processo de Gestão de Acesso Lógico verificamos que os ambientes de sistema operacional e banco de dados possuem critérios e controles parametrizados com base em utilização de senha individuais e controles. Os parâmetros de segurança do banco de dados e sistema operacional são configurados adequadamente com restrição de acessos e necessidade de atualização.

Para chegar à conclusão acima, a auditoria de sistemas solicitou a execução de *scripts* diretamente no banco de dados e sistema operacional para retornar informações quanto à segurança geral do ambiente. Considerando que o resultado dos mesmos não apresentou nenhuma divergência ao que é considerado boa prática de mercado, entendeu-se que o controle é eficaz.

O procedimento acima é igual ao que foi adotado para avaliação na empresa A, não apresentando qualquer tipo de divergência quanto a análise metodológica.

Para as atividades direcionadas ao controle de senhas e controle de parametrização de senhas foram analisados se os sistemas possuem padrões mínimos, necessitando de número mínimo de caracteres, dentre estes é necessário a utilização de composição alfanumérica e caractere especial, sendo mantido um histórico das ultimas cinco senhas, onde fica impossibilitada sua utilização antes da sexta.

Na oportunidade, foi solicitada a extração da tabela RSPARAM do SAP, de modo que a mesma retornasse com as informações de parametrização de senhas. Foi verificado que sistema necessita de uma adequação e atualização em seus parâmetros de senha, tornando este controle mais efetivo e os critérios de senha mais robustos. Tal necessidade foi apontada no documento de parametrização de

senhas (documento 18, APÊNDICE A) e na Carta de Recomendações à Gestão (documento 16, APÊNDICE A).

Quanto ao acesso de contas de usuários privilegiados, foi informado que apenas os profissionais da área de Sistema de Informações, cuja permissão seja *basis*, possuem permissão para incluir, alterar e excluir perfis de outros usuários, ou seja, possuem perfil privilegiado.

Para verificação do que foi apontado pela equipe de TI da empresa B, a equipe de auditoria de sistemas realizou uma verificação das listas de usuários e seus perfis de acesso, identificando usuários com perfil *basis*. A partir dessa verificação, foi realizado um batimento com a lista de profissionais ativos da companhia, para validar que os mesmos encontravam-se alocados na área de Sistemas de Informações. Adicionalmente, foi solicitado ao gestor da TI que validasse que todos os profissionais, cujo perfil de acesso era *basis*, necessitavam deste tipo de permissão para exercício de suas funções.

Além do que foi exposto, no papel de trabalho “Empresa B - Super Usuários e Usuários Genéricos” (documento 19, APÊNDICE A), foi analisada a utilização e gestão de contas de usuários genéricos. Para tanto, analisou-se a listagem de usuários do sistema e banco de dados, a fim de identificar algum usuário que não estivesse vinculado a nenhum profissional. Após verificação, não foram identificados usuários genéricos, com exceção de contas padrão.

As contas de sistema observadas foram enviadas para validação pelos profissionais da TI, havendo a indicação de que as mesmas foram geradas mediante a instalação dos sistemas e ambientes.

Quanto à Revisão Periódica de Usuários (documento 20, APÊNDICE A), foi identificada uma validação que é realizada, trimestralmente, para grupos de usuários, na qual um relatório é emitido e disponibilizado na rede, de modo que o coordenador de cada área analise e valide se os acessos às transações que os usuários possuem estão de acordo com as funções dos profissionais.

Esse procedimento é realizado através de e-mails, onde os coordenadores são comunicados sobre a ação e, local pela qual, também são enviadas as respostas de validação ou solicitação de ajuste.

Não foi observada a validação em um dos trimestres e tal fato é um ponto de atenção, devendo ser observado e avaliado pelas áreas a manutenção e realização deste controle.

Novamente, foi verificada a utilização de e-mails para validações e aprovações, o que, por sua vez, demonstra fragilidade no processo, pois, devido a isso, não foi identificada uma das validações trimestrais. Tal não conformidade foi levada à Carta de Recomendações à Gestão (documento 16, APÊNDICE A).

Adicionalmente, identificaram-se outros pontos de melhoria ao controle, para que exista maior rigor quanto à cobrança das validações por parte dos coordenadores das áreas, de modo que a equipe de TI possa avaliar a implementação da validação mediante a utilização de sites internos, possibilitando uma interação mais rápida.

Como forma de validar o processo de revogação de acessos, a equipe de auditoria procedeu com dois testes, sendo o primeiro, o batimento entre a lista de funcionários desligados, com a lista de usuários ativos no sistema; não foi identificado nenhum profissional desligado cujo acesso permanecia ativo no sistema, conforme disposto no documento “Empresa B - Revogação de Acessos” (documento 21, APÊNDICE A). Já o segundo teste consistia de uma avaliação de uma amostra de profissionais desligados no período auditado, com o objetivo de validar que o fluxo descrito para revogação de acessos existia e era efetivo. Conforme documentado (documento 21, APÊNDICE A), nenhum dos itens selecionados na amostra apresentou desvios ao que foi narrado, portanto, o processo de revogação de acessos foi considerado efetivo.

O processo, em si, de revogação dos acessos se dá mediante solicitação do setor de RH, onde, por e-mail, ocorre a comunicação com o setor de TI, indicando a necessidade de revogação dos acessos dos profissionais desligados.

Considerando que o controle de validação periódica de acessos foi falho, a metodologia de trabalho da EY (2013), determina que um controle de transferência de profissionais deva ser analisado. Neste âmbito, foi verificado que é responsabilidade de cada coordenador solicitar a inclusão ou remoção dos acessos dos usuários que eventualmente sejam transferidos, através de formulários enviados, por e-mail, contendo a solicitação. Desta forma, o controle de acessos ocorre de forma passiva pelo setor de TI, onde a demanda e possíveis mudanças

ocorrem apenas com a comunicação das áreas, havendo o risco de manutenção dos acessos de profissionais cujas responsabilidades se alteraram com o tempo.

Tendo em vista que o processo narrado acima é falho em seu desenho, a auditoria optou por realizar procedimentos adicionais, como forma de mitigar o risco relacionado à falha de dois controles. Para tanto, através de uma seleção aleatória, conforme documentado em papel de trabalho – “Empresa B - Fatores Mitigantes para Gestão de Identidades” (documento 22, APÊNDICE A) – selecionou 25 usuários e solicitou que o gestor responsável por aquele profissional validasse os perfis de acesso vinculados a ele. A partir de uma resposta positiva para todos os casos, a auditoria de sistemas possui razoável segurança que nenhum risco relacionado à gestão de identidades foi materializado, mesmo que os controles tenham sido falhos. Os pontos descritos acima foram devidamente documentados e apresentados à gestão na carta de recomendações (documento 16, APÊNDICE A).

Quando trata-se de concessão de acesso, identificou-se que o acesso ocorre com o pedido por e-mail do gestor dos profissionais. Tendo o profissional sido contratado, o responsável pelo mesmo solicita o acesso e a equipe da TI concede o acesso ao sistema em acordo com o perfil solicitado.

Para todos os casos de gestão de acessos, a equipe de auditoria avaliou os registros de solicitações e efetivou comparações com as transações liberadas no sistema com os pedidos enviados a TI, de modo a validar que todos os acessos foram devidamente solicitados e registrados. Além do que foi exposto, avaliou-se a existência de Segregação de Funções, uma vez que as pessoas que solicitam a gestão dos acessos não são as mesmas pessoas que executaram as operações (documento 23, APÊNDICE A). Eventualmente, caso seja um acesso da TI, o gestor aprova a solicitação antes da execução e os analistas responsáveis pela gestão são distintos dos que solicitaram. Cabe ressaltar que não foi elaborada uma matriz de segregação de funções pela equipe de auditoria de sistemas, uma vez que a mesma foi criada pela equipe responsável pelo trabalho de controles internos.

A equipe de auditoria de sistemas ainda buscou por controles relacionados ao monitoramento de trilhas de auditoria de usuários, com o objetivo de verificar se a empresa monitora possíveis atividades suspeitas, porém verificou que nenhum controle desta natureza é realizado de maneira periódica, conforme detalhado no

documento de Walkthrough dos Controles Gerais de TI da empresa B (documento 24, APÊNDICE A).

Da mesma forma do que foi apontado para a empresa A, também foram analisados os controles de acesso ao *Data Center.* Identificou-se que é necessário autenticar, através de um leitor de crachá eletrônico ou biometria localizada na porta, o acesso, sendo profissionais não habilitados, impedidos de acesso.

Para tanto, a equipe de auditoria de sistemas analisou a lista de profissionais com permissão a acessar o interior da sala do *Data Center*, que continha a assinatura do Gerente da área, atestando que essas pessoas, efetivamente, possuem permissão para acessar o local. Adicionalmente foi realizado um batimento da listagem supracitada com os logs de acesso ao local, com o objetivo de validar que apenas os devidos profissionais tiveram acesso à sala de servidores da empresa. Além do que foi descrito, ainda foi verificada a validação mensal realizada pelo gestor de TI – procedimento similar ao teste realizado pela auditoria (documento 25, APÊNDICE A).

Por fim, avaliou-se a existência de normas e procedimentos envolvendo toda a Gestão de TI, sua periodicidade de atualização e adequabilidade em relação à governança em tecnologia da informação. Verificou-se que existe um procedimento de revisão periódica das políticas que fazem parte do processo de Gerenciamento de Acesso Lógico, a fim de avaliar se os mesmos são seguidos e/ou encontram-se atualizados em relação ao ambiente de TI. Foi avaliado se existiam revisões internas de aderência dos procedimentos executados às políticas de segurança, revisões periódicas de políticas e procedimentos operacionais de TI, revisões de patamares mínimos de segurança, revisões da avaliação de riscos de TI e gerenciamento de patches e atualizações de segurança. Adicionalmente, avaliou se os mesmos estavam sendo devidamente utilizados pelos profissionais da companhia.

A equipe de auditoria avaliou as políticas e verificou que todos os documentos encontravam atuais, com as indicações da última revisão, além de estarem aderentes à prática da empresa.

Com base nos procedimentos de auditoria descritos acima e no ambiente analisado, verificou-se que o resultado da auditoria, no que tange o processo de gestão de acessos, necessita de melhorias relacionadas ao monitoramento de trilhas de auditoria, bem como melhorias no que tange formalização de controles, uma vez

que existe quantidade demasiada de aprovações e validações realizadas via e-mail. Independente dos pontos levantados, o ambiente foi considerado eficaz devido aos demais controles existentes e do risco relacionado a cada um dos controles; os riscos de cada análise são determinados pela auditoria com base em uma avaliação de impacto e probabilidade de ocorrência de cada ponto e apresentado à companhia na Carta de Recomendações (documento 16, APÊNDICE A).

Diferente da empresa A, por se tratar de uma auditoria integrada, foi realizada a avaliação de controles relativos a Operações em TI, que contemplam *Backups* e *Restore*, Execução de Rotinas Automatizadas e Gestão de Incidentes. De acordo com o Sr. João Carlos Ervilha, considerando que em uma auditoria integrada necessita-se avaliar os controles internos da empresa de forma mais extensa e efetiva, essas atividades são avaliadas para dar maior conforto quanto à segurança do ambiente de TI, mesmo que a complexidade do ambiente e a operação da empresa não requeiram tantos controles.

Primeiramente, verificou-se que as execuções dos procedimentos de *backup* ocorrem automaticamente, por meio da ferramenta automatizada, monitorada de forma diária pela equipe interna de TI, com registro e controle por meio de *Check list.* São realizados procedimentos de backups diários, semanais e mensais nos servidores dos bancos de dados que suportam o sistema, sendo que, para os procedimentos de backups diários e semanais (*backups full*), a retenção da fita é de 7 e 30 dias, respectivamente, já para o procedimento mensal (*backup full*), a retenção da fita é permanente.

Para avaliar a adequação do que foi informado, a equipe de auditoria ainda realizou uma verificação se os *backups* são utilizáveis, ou seja, se em caso de *restore*, os mesmos poderiam ser utilizados sem nenhum tipo de restrição e nada foi constatado fora da normalidade.

O procedimento adotado pela auditoria foi verificar, na ferramenta, o *scheduler* do *backup,* a fim de validar a veracidade dos prazos indicados. Ademais, foi solicitado o log de execução da rotina, de modo a verificar se nenhum item apresentou problemas durante o processo. Para os casos que tiveram inconsistências, verificou-se que a rotina foi reexecutada sem apresentação de problemas. Considerando que nenhum *backup* apresentou mais de uma falha seguida, não foi necessária a abertura de chamados para tratativa dos incidentes.

Para avaliação da recuperação dos dados, a equipe de TI da empresa B foi questionada sobre a existência de testes de *restore*, cuja resposta foi positiva. Para tanto, a auditoria solicitou as evidências dos testes executados para análise e verificou que nenhum apresentou problemas. Adicionalmente, solicitou que um *restore* fosse simulado, de modo que fosse possível avaliar a efetividade dos procedimentos executados (documento 26, APÊNDICE A).

Adicionalmente, os *jobs* e rotinas automáticas da empresa são programados e monitorados através da ferramenta de controle em ambiente do sistema operacional.

A programação e o monitoramento de *jobs* “batch” são realizados apenas por profissionais da equipe de produção, cujos acessos são restritos (por meio de perfis de acesso) na própria ferramenta (já avaliados nos controles de Gestão de identidades e acessos). Caso ocorra algum problema durante a execução de qualquer *job*, os analistas são responsáveis por verificar o erro e tomar ações de forma que o problema seja resolvido. Além disso, diariamente, os analistas de produção registram, em uma planilha (*check list*), o resultado dos “*jobs*” executados, como também assinam o documento e o armazena em pasta localizada dentro do departamento de TI.

A equipe de auditoria avaliou a planilha e verificou a existência de formalização da revisão e monitoramento das rotinas. Foi identificado que semanalmente, o gestor avalia os *jobs* executados, e demanda justificativa em caso de falhas, bem como tratativa e tempo de indisponibilidade da funcionalidade. De posse da documentação do monitoramento, a equipe de auditoria de sistemas avaliou os formulários e as justificativas / tratativas e não identificou divergências. Adicionalmente, foi realizada uma simulação de execução de *job* aleatório para avaliar a funcionalidade do mesmo (documento 27, APÊNDICE A).

Por fim, no caso de incidentes na Rede, como por exemplo, a interrupção de processamento de algum servidor, as equipes de Infraestrutura e de Help Desk recebem dois alarmes automáticos: uma notificação enviada por e-mail pelo próprio aplicativo para o grupo de e-mail ‘WhatsUp’, onde estão cadastrados os analistas das equipes de Help Desk e de Infraestrutura e um alarme sonoro em suas estações de trabalho.

De acordo com a metodologia de trabalho da EY (2013), caso os dois primeiros controles (*Backup* e *restore* e *Job Scheduling*) sejam eficazes, não é

necessário realizar procedimentos de teste para o controle de gestão de incidentes, uma vez que possíveis falhas e tratativas já foram analisadas e documentadas nos demais controles.

Após a análise feita pelas equipes responsáveis, as devidas providências são tomadas em conjunto com a equipe de Help Desk para a resolução do problema. Já para os incidentes nos sistemas operacionais e banco de dados, são gerados alarmes na própria ferramenta, onde as analistas de Banco de Dados são notificadas, de forma que possam solucionar o problema.

Através dos procedimentos executados, verificamos que não houve nenhum ponto identificado a ser reportado.

4.3 Comparação entre os Procedimentos de Auditoria

A partir da descrição do ambiente de TI das empresas, foi possível compreender a metodologia utilizada pela auditoria. Através dos procedimentos detalhados, verificou-se que os métodos de auditoria utilizados para avaliação dos controles gerais de TI são similares no que tange Gestão de Acesso Lógico e Gerenciamento de Mudanças, porém diferente na análise de Operações em TI, analisados apenas na empresa B, cujo escopo era uma auditoria integrada.

Conforme descrito na caracterização do ambiente de TI das duas empresas, para o processo de Gerenciamento de Mudanças, verificou-se que a EY acompanhou a extração das tabelas E070 e TPLOG, comparando-as de modo a verificar que todas as mudanças colocadas em ambiente de produção constavam na lista das mudanças desenvolvidas. Objetivou-se validar, com esse procedimento, que nada foi colocado diretamente em produção. Para ambas as empresas, o procedimento foi similar.

Tendo o conforto de que nenhuma mudança foi aplicada diretamente em produção, a auditoria independente realizou uma avaliação do processo, através dos chamados abertos nas ferramentas de Service Desk, de modo a ter razoável segurança de que todas as mudanças foram devidamente solicitadas, testadas e aprovadas para serem aplicadas em produção. Mesmo verificando que o processo continha diferenças entre as empresas, o procedimento adotado foi o mesmo, uma vez que foi feita uma análise de como as mudanças eram solicitadas, testadas e aprovadas para os dois casos.

Para avaliar a segregação de funções dentro do processo de mudança das duas empresas, a equipe de auditoria realizou conferência das permissões de escrita e execução nos diretórios de produção. Através do acompanhamento da execução de comandos no Linux, foi possível validar que nenhum usuário ou grupo com acesso ao diretório de produção, possui, também, acesso ao diretório de desenvolvimento. Adicionalmente, durante avaliação do processo de mudanças, avaliou-se se nos chamados de mudanças continham informações dos desenvolvedores e executores, de modo que se verificasse se o processo também apresenta adequada segregação. Para tanto, em ambas as empresas, verificou-se novamente as tabelas E070 e TPLOG para verificar que os usuários responsáveis por desenvolver mudanças eram distintos dos responsáveis por aplica-las em produção.

No que tange a avaliação do monitoramento do ambiente de mudanças, identificamos que o procedimento executado se baseia na avaliação de como as empresas realizam e mantem este controle. Dito isso, verificou-se o processo de avaliação das mudanças; mesmo que os ambientes sejam diferentes, a forma utilizada para analisar o controle é similar em ambas as empresas.

Para a empresa A, identificou-se ainda a execução de um controle compensatório, uma vez que o controle de segregação de funções demonstrou-se falho em tal ambiente. Não obstante, de acordo com o gerente da auditoria, Sr. João Carlos Ervilha, caso o ambiente da empresa B apresentasse o mesmo ponto, o procedimento de análise seria igual ao realizado para a empresa A.

Partindo para a análise do processo de Gestão do Acesso Lógico, verificam-se mais controles, mas, novamente, procedimentos de auditoria similares para todos eles.

Primeiramente foi solicitada a execução de *scripts* diretamente no banco de dados e sistema operacional do sistema de ambas as empresas, para retornar informações quanto à segurança geral do ambiente. A equipe de auditoria de sistemas realizou a avaliação das informações obtidas para compor um papel de trabalho similar.

Adicionalmente, com o intuito de avaliar as parametrizações de senha, foi solicitada a extração da tabela RSPARAM, para análise de critérios mínimos como complexidade de senhas, histórico de senhas, *timeout*, entre outros. Para ambas as

empresas, a auditoria realizou avaliação da tabela para verificar a confiabilidade das senhas do SAP.

O terceiro controle dentro do processo de Gestão de Acesso Lógico é relacionado à avaliação de usuários privilegiados, com perfil para incluir, alterar e excluir outros usuários, e usuários genéricos, não vinculados diretamente a nenhum profissional das empresas. Para análise do controle em questão, a equipe de auditoria de sistemas realizou uma verificação das listas de usuários e seus perfis de acesso, identificando usuários com perfil *basis,* uma vez que foi a permissão indicada como sendo a que possui o tipo de autorização descrita anteriormente. A partir dessa verificação, foi realizado um batimento com a lista de profissionais ativos em cada companhia, para validar que os mesmos encontravam-se alocados no departamento de TI de ambas. Adicionalmente, foi solicitado aos gestores de TI que validassem que todos os profissionais, cujo perfil de acesso era *basis*, necessitavam deste tipo de permissão para exercício de suas funções. Conforme descrito, e considerando que o ERP de ambas as empresas é o mesmo, a equipe de auditoria de sistemas executou o mesmo procedimento de análise em ambas.

Para as duas empresas, a avaliação dos usuários com permissões privilegiadas se estendeu ao controle de concessão de acessos; a auditoria verificou se os usuários criados no período foram concedidos apenas por profissionais com perfil *basis*.

Além do que foi exposto, foi analisada a utilização e gestão de contas de usuários genéricos. Para tanto, avaliou-se a listagem de usuários do sistema e banco de dados, a fim de identificar algum usuário que não estivesse vinculado a nenhum profissional. Após verificação, não foram identificados usuários genéricos, com exceção de contas padrão, em ambos os ambientes.

Em outro momento, foi analisado o controle de validação periódica de usuários para as duas empresas. Conforme descrito nas sessões anteriores, foi levantado o processo na empresa A e na empresa B, analisando se o controle foi executado da forma descrita. Para tanto, foram avaliados todos os meses e conferido se os gestores das áreas realizaram a verificação dos perfis de cada usuário, além da validação formal. Para os casos de usuários que não tenham sido validados, a equipe ainda realizou o batimento dos acessos para verificar se o mesmo teve seu perfil adequado ao que foi apontado pelo gestor. Mesmo que o

controle possua suas particularidades, em cada uma das empresas analisadas neste trabalho, verificou-se que o procedimento adotado é o mesmo.

Analisou-se ainda o controle de revogação de acessos nas duas empresas. Novamente, através do que foi documentado anteriormente, verificou-se a utilização dos mesmos procedimentos de auditoria para ambas. Foi realizado um batimento entre as listas de desligados e listas de usuários ativos no sistema, a fim de identificar profissionais, que não mais pertencem ao quadro de funcionários das empresas, cujo acesso permanecia ativo. Adicionalmente, através de seleção aleatória, itens foram colhidos para a realização de uma avaliação do processo de revogação, para identificar se o mesmo era efetivo.

Também foi analisado o controle de concessão de acessos, no qual a equipe de auditoria avaliou os registros de solicitações e efetivou comparações com as transações liberadas no sistema com os pedidos enviados a TI, de modo a validar que todos os acessos foram devidamente solicitados e registrados. Além do que foi exposto, avaliou-se a existência de Segregação de Funções, uma vez que as pessoas que solicitam a gestão dos acessos não são as mesmas pessoas que executaram as operações.

Ambos os controles, Concessão de Acessos e Segregação de Funções, foram analisados através dos mesmos procedimentos tanto na empresa A quanto na B, conforme descrito na caracterização dos ambientes acima.

Houve a tentativa de se analisar o monitoramento de trilhas de auditoria, para ambas as empresas, porém não foi identificado um controle similar em nenhum dos casos.

Já para a avaliação de usuários transferidos, não foram executados procedimentos de auditoria, uma vez que o controle de validação periódica de acessos existia em ambas as empresas; de acordo com a metodologia de trabalho da EY, caso o primeiro controles exista e seja eficaz, não há necessidade de se avaliar usuários transferidos, pois o risco relacionado aos dois controles é o mesmo.

Adicionalmente, avaliou-se o controle de acesso físico ao *Data Center*, para tanto, a equipe de auditoria interna solicitou a lista dos profissionais que possuíam acesso ao local e realizou um batimento com os logs de acesso ao ambiente. Adicionalmente, solicitou validação dos gestores de TI quanto à necessidade de tais acessos ao *Data Center*, como forma de ter maior conforto quanto aos profissionais

que possuem permissão para adentrar ao local. Esse procedimento foi executado em ambas as empresas, sem qualquer tipo de distinção entre elas.

Por fim, avaliou-se a existência de normas e procedimentos envolvendo toda a Gestão de TI, sua periodicidade de atualização e adequabilidade em relação à governança em tecnologia da informação. Foi avaliado se existiam revisões internas de aderência dos procedimentos executados às políticas de segurança, revisões periódicas de políticas e procedimentos operacionais de TI, revisões de patamares mínimos de segurança, revisões da avaliação de riscos de TI e gerenciamento de patches e atualizações de segurança. Adicionalmente, avaliou se os mesmos estavam sendo devidamente utilizados pelos profissionais da companhia.

O procedimento acima foi o mesmo nas duas empresas avaliadas, diferindo apenas o tipo de documento analisado.

Até o presente momento, verificou-se que para os processos de Gestão de Mudanças e Gestão de Acesso Lógico, os procedimentos de auditoria não se diferem. Porém, para a empresa B, que é regulada pela Lei SOX, verificou-se a avaliação de um processo a mais, o de Outros ITGCs ou Operações de TI. O intuito dessa avaliação adicional é aumentar o conforto, e reduzir o risco, em relação à auditoria, uma vez que para empresas reguladas pela lei americana, a EY necessitou emitir um parecer, não apenas sobre as Demonstrações Financeiras, mas também sobre o ambiente de Controles Internos da empresa.

Para essa análise, foram avaliados controles de *Backup*, *Restore* e *Job Scheduling.* O procedimento adotado pela auditoria foi averiguar, na ferramenta, o *scheduler* do *backup* a fim de validar a veracidade dos prazos indicados. Ademais, foi solicitado o log de execução da rotina, de modo a conferir se nenhum item apresentou problemas durante o processo. Para os casos que tiveram inconsistências, verificou-se que a rotina foi reexecutada sem apresentação de problemas.

Em relação aos *jobs*, a equipe de auditoria de sistemas realizou uma simulação de modo a validar a forma como as rotinas são criadas e executadas no sistema. Adicionalmente, verificou o log de execução das rotinas e avaliou a tratativa dos *jobs* que apresentaram falhas em sua execução.

Considerando o que foi descrito acima, foi elaborado um quadro comparativo com os procedimentos de auditoria e os resultados encontrados no trabalho.

Quadro 3 – Comparativo entre empresas (Gestão de Mudanças).

Controles	Empresa A (Não SOX)		Empresa B (SOX)	
	Procedimento Adotado	**Resultado da Auditoria**	**Procedimento Adotado**	**Resultado da Auditoria**
Solicitação / Autorização	Batimento e análise das tabelas E070 X TPLOG / Avaliação do processo de solicitação e autorização para desenvolvimento de Mudanças	Solicitação / Autorização para desenvolvimento de mudanças formal e devidamente documentados.	Batimento e análise das tabelas E070 X TPLOG / Avaliação do processo de solicitação e autorização para desenvolvimento de Mudanças	Solicitação / Autorização para desenvolvimento de mudanças formal e devidamente documentados.
Testes / Homologação	Avaliação do processo e evidenciação de testes / homologação das mudanças solicitadas	Testes / Homologação das mudanças são devidamente executados em ambiente segregado e documentados.	Avaliação do processo e evidenciação de testes / homologação das mudanças solicitadas	Testes / Homologação das mudanças são devidamente executados em ambiente segregado e documentados.
Aprovação para a Produção	Avaliação do processo e evidenciação das aprovações para transporte para a produção	Aprovação para envio ao ambiente produtivo é devidamente documentado.	Avaliação do processo e evidenciação das aprovações para transporte para a produção	Aprovação para envio ao ambiente produtivo é devidamente documentado.
Monitoramento de Mudanças	Avaliação dos procedimentos de monitoramento das mudanças implementadas em produção	Monitoramento executado semanalmente por comitê de mudanças.	Avaliação dos procedimentos de monitoramento das mudanças implementadas em produção	Monitoramento executado mensalmente por comitê de mudanças.
Segregação de Funções	Avaliação das permissões de acesso ao ambiente de desenvolvimento e produção / Comparação dos acessos	Não segrega funções de desenvolvimento.	Avaliação das permissões de acesso ao ambiente de desenvolvimento e produção / Comparação dos acessos / Verificação dos profissionais que transportaram mudanças para ambiente produtivo	Segrega funções de desenvolvimento.
Controles Compensatórios	Verificação dos profissionais que transportaram mudanças para ambiente produtivo	Mudanças são desenvolvidas por profissionais diferentes dos responsáveis pelo transporte em produção.	Não avaliado pela auditoria	-

Fonte: Elaborado pelo autor.

Quadro 4 – Comparativo entre empresas (Gestão de Acessos).

Controles	Empresa A (Não SOX)		Empresa B (SOX)	
	Procedimento Adotado	**Resultado da Auditoria**	**Procedimento Adotado**	**Resultado da Auditoria**
Segurança Geral	Análise a partir dos resultados obtidos através da execução de scripts	Nenhuma falha significativa identificada	Análise a partir dos resultados obtidos através da execução de scripts	Nenhuma falha significativa identificada
Parametrização de Senhas	Avaliação da tabela RSPARAM do SAP	Parametrização conforme melhores práticas de mercado.	Avaliação da tabela RSPARAM do SAP	Parametrização conforme melhores práticas de mercado.
Usuários Administradores / Genéricos	Avaliação dos profissionais com posse de permissões basis / Validação de contas genéricas	Apenas profissionais habilitados, que necessitam deste tipo de acesso, possuem perfil basis / Usuários de sistema são os únicos genéricos identificados.	Avaliação dos profissionais com posse de permissões basis / Validação de contas genéricas	Apenas profissionais habilitados, que necessitam deste tipo de acesso, possuem perfil basis / Usuários de sistema são os únicos genéricos identificados.
Validação Periódica de Usuários	Avaliação do processo de validação de usuários e análise do período de execução	Validação periódica executada semestralmente.	Avaliação do processo de validação de usuários e análise do período de execução	Validação periódica executada trimestralmente.
Concessão de Acessos	Avaliação do processo de concessão	Concessão de acessos realizada de maneira formal, contendo solicitação e aprovação.	Avaliação do processo de concessão	Concessão de acessos realizada de maneira formal, contendo solicitação e aprovação.
Revogação de Acessos	Avaliação do processo de revogação / Batimento e análise das listas de desligados X usuários ativos	Revogação realizada através de procedimento formal / Não existem profissionais desligados com perfil ativo no sistema.	Avaliação do processo de revogação / Batimento e análise das listas de desligados X usuários ativos	Revogação realizada através de procedimento formal / Não existem profissionais desligados com perfil ativo no sistema.
Monitoramento de Trilhas de Auditoria	Avaliação dos procedimentos de monitoramento das trilhas de auditoria dos perfis	Não são executados procedimentos de monitoramento de perfis de auditoria.	Avaliação dos procedimentos de monitoramento das trilhas de auditoria dos perfis	Não são executados procedimentos de monitoramento de perfis de auditoria.
Acesso Físico ao Data Center	Batimento e análise das listas de permissões ao Data Center X logs de acesso	Apenas profissionais habilitados, que necessitam deste tipo de acesso acessaram o local, porém para acompanhantes não eram requeridos registros.	Batimento e análise das listas de permissões ao Data Center X logs de acesso	Apenas profissionais habilitados, que necessitam deste tipo de acesso acessaram o local.
Monitoramento do Processo (Políticas)	Avaliação da existência e adequabilidade de políticas e procedimentos	Políticas e procedimentos são revisadas periodicamente e são adequadas à realidade da empresa.	Avaliação da existência e adequabilidade de políticas e procedimentos	Políticas e procedimentos são revisadas periodicamente e são adequadas à realidade da empresa.
Segregação de Funções	Avaliação dos profissionais que concederam acessos, analisando distinção para os aprovadores	Gestão de identidades realizada de forma segregada.	Avaliação dos profissionais que concederam acessos, analisando distinção para os aprovadores	Gestão de identidades realizada de forma segregada.

Fonte: Elaborado pelo autor.

Quadro 5 – Comparativo entre empresas (Operações em TI).

Controles	Empresa A (Não SOX)		Empresa B (SOX)	
	Procedimento Adotado	**Resultado da Auditoria**	**Procedimento Adotado**	**Resultado da Auditoria**
Backup e Restore	Não avaliado pela auditoria	-	Avaliação dos schedulers e execução dos backups / Avaliação das tratativas de erros / Avaliação e simulação dos testes de Restore	Backups são executados devidamente, sendo qualquer problema tradado / Testes de Restore são devidamente executados e tratados.
Job Scheduling	Não avaliado pela auditoria	-	Avaliação das rotinas existentes / Avaliação das trativas de erros	Rotinas são devidamente cadastradas e executadas / Possíveis erros são devidamente registrados e tratados.

Fonte: Elaborado pelo autor.

Com a definição da metodologia de análise e dos controles, conforme descrito acima, foi possível avaliar o ambiente de TI para cada uma das empresas, indicando se o ambiente analisado encontra-se em aderência com as melhores práticas de mercado ou não. A partir do que foi relatado, apesar de alguns pontos de melhoria identificados em ambos os casos, verificou-se que, a empresa A, mesmo não sendo regulada pela Lei SOX, apresenta ambiente mais maduro quando comparado à empresa B, uma vez que seus controles são mais robustos e menos susceptíveis a falhas. Tal conclusão se fez com base nos procedimentos práticos executados pela equipe de auditoria de sistemas, que chegaram a conclusões específicas dos controles avaliados.

Por fim, com base na comparação entre os procedimentos adotados pela equipe de auditoria de sistemas e pelos resultados identificados, foi possível verificar as diferenças entre os controles e a metodologia empregada. Considerando os procedimentos adotados, não foram identificadas diferenças entre a auditoria da empresa A e da empresa B, no que tange Gestão de Mudanças e Gestão do Acesso Lógico, porém, para a segunda companhia que é regulada pela Lei SOX, foram realizados procedimentos adicionais. Dito isso, verifica-se que os procedimentos adotados são similares, com exceção dos controles de operações em TI, uma vez que o risco relacionado a uma auditoria vinculada à Lei SOX é maior do que o trabalho relacionado à empresa A, o que fez com que não se analisassem todos os pontos nessa empresa.

5 CONCLUSÃO

Considerando que os trabalhos e recomendações da auditoria possuem papel relevante na construção e aprimoramento da governança corporativa e consequentemente na estrutura de controles internos de uma organização, investigou-se o nível de maturidade dos controles e do ambiente de TI das empresas auditadas, sejam elas reguladas ou não pela Lei SOX por meio da ótica do trabalho de auditoria independente. Adicionalmente, foi avaliado se o fato de uma empresa ser regulada pela SOX implica na construção de controles mais robustos e eficazes.

Para tanto, foram traçados os objetivos específicos de (i) analisar os procedimentos de auditoria utilizados para a avaliação dos controles gerais de tecnologia da informação; (ii) comparar os controles gerais e o ambiente de TI relacionado de empresas reguladas pela SOX e empresas não reguladas pela Lei e (iii) avaliar o impacto de uma empresa regulada pela Lei SOX no nível de maturidade de seus controles de TI.

Para analisar os procedimentos de auditoria utilizados na avaliação dos controles gerais de tecnologia da informação, analisou-se o COBIT e verificou-se que, além de ser utilizado como referência para desenho dos controles de Tecnologia da Informação, o documento é utilizado como principal guia para os trabalhos de auditoria de sistemas, independentemente se as empresas são regulamentadas ou não pela Lei SOX. Verificou-se que os procedimentos gerais de auditoria também são utilizados, como adoção de amostragem estatística aleatória e representativa, uma vez que as análises são realizadas por meio de testes de parte representativa da população de mudanças e acessos. Os procedimentos para coleta de dados, documentação de testes e reporte dos problemas identificados também foram analisados. Adicionalmente são utilizados, pela EY, *frameworks* relacionados à infraestrutura de TI como o ITIL - sigla em inglês para Biblioteca de Infraestrutura em Tecnologia da Informação.

Este estudo constatou que os controles gerais relacionados a Gerenciamento de Mudanças e Gestão do Acesso Lógico tiveram seus desenhos testes realizados com base no COBIT e em normas e padrões gerais de auditoria. A avaliação realizada mostrou que os procedimentos adotados para análise dos controles dos processos acima referenciados foram similares em ambas as empresas, com pequenas divergências devido à particularidade de cada ambiente. Contudo, os

controles relacionados às Operações de TI, mesmo que tenham sido avaliados com base no COBIT e em outros guias, só foram analisados para a empresa regulada pela Lei SOX. Isso decorre da determinação da lei americana para que seja realizada uma avaliação mais bem estruturada e aprofundada dos controles internos das empresas, levando ao teste de mais controles por parte das equipes de auditoria. Dessa forma, a EY optou por ampliar o escopo e utilizar mais procedimentos de análise, com o intuito de ter maior segurança em relação aos controles gerais de TI.

Para comparar os controles gerais de TI e o ambiente de empresas reguladas pela SOX e empresas não reguladas pela Lei, foram documentados os controles analisados pela auditoria independente e os procedimentos adotados para essa análise nas duas empresas. Após a comparação, foi possível verificar que a empresa regulada pela Lei SOX, mesmo tendo sido objeto de maior análise de auditoria, apresentou um ambiente de TI mais frágil, com controles menos eficazes e mais suscetíveis a erros e falhas. Na prática, mesmo que a Lei SOX demande um ambiente de controles mais robusto e eficaz, o ambiente de TI da empresa regulamentada apresentou a característica oposta. Por outro lado, os controles referentes à companhia que não precisa se submeter à legislação americana são mais robustos e mais eficazes. O processo de TI é mais informatizado, com ferramentas e controles automáticos, apresentando um melhor controle sobre as aprovações e etapas do processo, enquanto a empresa regulada pela Lei SOX apresenta muitos controles manuais, mais passíveis de falhas, como por exemplo, aprovações por e-mail e formulários físicos. Adicionalmente, para os controles analisados de Gestão de Mudanças e Gestão de Acessos, verificamos que as empresas, de modo geral, apresentam quantidade similar de controles eficazes.

Com base nos dados analisados e nos procedimentos de auditoria adotados, verifica-se que, mesmo que a seção 404 da Lei SOX oriente aos administradores estabelecer e manter uma estrutura de controles internos adequados, de modo a suportar as informações publicadas em relatórios financeiros, no período analisado a empresa regulada pela lei americana não priorizou a adequação dos controles internos de TI, se atendo ao mínimo necessário para que seu ambiente de TI fosse considerado eficaz pela auditoria independente. E a empresa não regulamentada pela Lei SOX apresentou um ambiente de controles de TI mais robusto e eficaz.

Desse modo, nas duas empresas analisadas, verificou-se que o fato de uma empresa ser regulada pela Lei SOX não é suficiente para assegurar elevada maturidade de seus controles de TI.

6 REFERÊNCIAS

AMORIN, E. Y. S. A Lei Sarbanes Oxley: O impacto da lei na estrutura de governança corporativa. 2005. 209 p. Dissertação (Mestrado em Administração de Empresas) – Escola de Administração de Empresas de São Paulo – Fundação Getúlio Vargas, São Paulo, 2005. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/5480>. Acesso em: 31 jan 2014.

AMORIN, L. Para que servem as auditorias? Revista Exame, São Paulo, Ed. 0984, p. 80, 2011.

BARROS, A. J. N. O processo de gestão de risco nas organizações. 2012. 115 p. Dissertação (Mestrado em Auditoria) – Instituto Superior de Contabilidade e Administração do Porto, Porto, 2012. Disponível em: < http://recipp.ipp.pt/bitstream/10400.22/1147/1/DM_Ana_Barros_2012.pdf>. Acesso em: 04 fev 2014.

BOYNTON, W.; JOHNSON, R. N., KELL, W. G. Auditoria: tradução autorizada. São Paulo: Atlas, 2002.

BRYAN, L. D. Corporate Managers' Experiences Related To Implementing Section 404 Of The Sarbanes-Oxley Act: A Focus On Information Systems Issues. The Journal of Applied Business Research, Vol. 25, n. 3, 2009. Disponível em: < http://journals.cluteonline.com/index.php/JABR/article/viewFile/1024/1008> Acesso em: 05 abr. 2014.

CARDOSO, A. P.; RODANTE, A. Auditoria: Registros de uma profissão, Ed. IBRACON, 2007.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. Internal Control – Integrated Framework. 2012.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. Fraudulent Financial Reporting: 1987-1997. 1999. Disponível em: <http://www.coso.org/publications/FFR_1987_1997.PDF> Acesso em: 01 abr. 14.

CONTROLADORIA GERAL DA UNIÃO (CGU), 2009. A responsabilidade social das empresas no combate à corrupção. Disponível em: < http://www.cgu.gov.br/publicacoes/ManualRespSocial/Arquivos/ManualRespsocialEmpresas_alta.pdf>. Acesso em: 01 mar. 2014.

COSTA, A. M. C. A Auditoria Interna nos Municípios Portugueses. 2008. 151 p. Dissertação (Mestrado em Contabilidade e Finanças) – Faculdade de Economia – Universidade de Coimbra, Coimbra, 2008. Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/17846/1/Disserta%c3%a7aoAnabela_Final.pdf> Acesso em: 03 abr. 2014.

DANTA, W. R. H. Importância dos controles internos nas empresas antes e depois do advento da Sarbanes-Oxley Act. 2006. 232 p. Dissertação (Mestrado em Economia) – Faculdade de Ciências Econômicas – Universidade Federal do Rio

Grande do Sul, Porto Alegre, 2006. Disponível em: < http://www.lume.ufrgs.br/bitstream/handle/10183/11496/000615887.pdf?sequence=1 >. Acesso em: 22 jan. 2014.

DELLOITE TOUCHE TOHMATSU. Lei Sarbanes-Oxley: Guia para melhorar a governança corporativa através de eficazes controles internos, 2003. Disponível em: < http://www.deloitte.com/assets/Dcom-brazil/Local%20Assets/Documents/guia_sarbanes_oxley(1).pdf>. Acesso em: 07 mar. 2014.

EY. ITGC: IT General Controls/Application Controls. 2013. s.l.

FRANCO, H.; MARRA, E.. Auditoria contábil. 4 ed. São Paulo: Atlas, 2001. 607 p.

GHERMAN, M. COBIT: Integrando TI aos negócios. 2005. Disponível em <www.modulo.com.br> Acesso em: 14 abr. 2014.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. Livro COBIT, s.d., s.l. <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Downloads.aspx> Acesso em: 22 jan. 2014.

INSTITUTO PORTUGUÊS DE AUDITORES INDEPENDENTES (IPAI), A Lei Sarbanes Oxley de 2002: Resumo das principais cláusulas de interesse para os auditores internos, s.d., Disponível em <https://www.google.com/#q=IPAI+A+LEI+DE+SARBANES-OXLEY+DE+2002> Acesso em: 15 abr. 2014.

IT GOVERNANCE INSTITUTE. IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting. 2 ed. Illinois (EUA): ITGI, 2006.

GHERMAN, M. Controles Internos - Buscando a solução adequada - Parte V. Disponível em <http://www.modulo.com.br/checkuptool/artigo_10.htm> Acesso em: 15 abr. 2014

GOETZ, J.P.; LECOMPTE, M.D. Etnogría y diseño cualitativo en investigación educativa. 1984. Madrid: Morata.

KPMG. A lei Sarbanes Oxley. (s.n.t.). Disponível em: < http://www.kpmg.com.br/images/Sarbanes_Oxley.pdf>. Acesso em: 07 mar. 2014.

MENDONÇA, M. M.; COSTA, F. M.; GALDI, F. C.; FUNCHAL, B. O impacto da lei Sarbanes-Oxley (SOX) na qualidade do lucro das empresas brasileiras que emitiram ADRs. In: Congresso USP de Controladoria e Contabilidade, 8., 2008, São Paulo. Disponível em: < http://www.scielo.br/scielo.php?pid=S1519-70772010000100004&script=sci_arttext>. Acesso em: 14 fev. 2014.

OLIVEIRA, L. M.; DINIZ FILHO, A. Curso básico de auditoria. São Paulo: Atlas, 2001

PACHECO, M. S.; OLIVEIRA, D. R.; LA GAMBA, F. A História da Auditoria e suas Novas Tendências: Um enfoque sobre Governança Corporativa, Seminários em Administração, Ed. FEA-USP, 2007.

PRADAS, L. T., SALVADOR, I. C. Auditoria de entidades locales, Instituto de Auditores – Censores Jurados de Cuentas de España, Madrid, 2005 In: COSTA, A. M. C. A Auditoria Interna nos Municípios Portugueses. 2008. 151 p. Dissertação (Mestrado em Contabilidade e Finanças) – Faculdade de Economia – Universidade de Coimbra, Coimbra, 2008. Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/17846/1/Disserta%c3%a7aoAnabela_Final.pdf> Acesso em: 03 abr. 2014.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). Auditing Standard No. 5. 2007. Disponível em < http://pcaobus.org/standards/auditing/pages/auditing_standard_5.aspx#introduction> Acesso em: 29 abr. 2014.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). Auditing Standard No. 2. 2004. Disponível em < http://pcaobus.org/standards/auditing/pages/auditing_standard_2.aspx#introduction> Acesso em: 29 abr. 2014.

RAIBORN, C.; SCHORG, C.. The Sarbanes-Oxley Act of 2002: An Analysis of and Comments on the Accounting Related Provisions, Journal of Business and Management, Vol. 10, n. 1, p. 1-13, 2004. Disponível em: <http://search.epnet.com/login.aspx?direct=true&db=buh&an=13335454>. Acesso em: 05 abr. 2014.

RIBEIRO, E. Sarbanes-Oxley e TI. 2011 Disponível em: <http://www.tiespecialistas.com.br/2011/08/sarbanes-oxley-e-ti/> Acesso em: 30 mar 2014.

RODRIGUES, L. C.; MACCARI, E. A.; SIMÓES, S. A. O desenho da gestão da tecnologia da informação nas 100 maiores empresas na visão dos executivos de TI. Journal of Information Systems and Technology Management, São Paulo, Vol. 6, No. 3, p. 483-506, 2009.

SILVA, L. M.; MACHADO, S. B. Z. Um estudo sobre os impactos da Lei Sarbanes-Oxley na área de auditoria interna de uma empresa brasileira com ações negociadas nos Estados Unidos, 2008. Disponível em: <http://www.congressocfc.org.br/hotsite/trabalhos_1/555.pdf>. Acesso em: 02 mar. 2014.

SOARES, F. E. G., Lei Sarbanes-Oxley: Os principais impactos de sua aplicação nas organizações. 2006, 76 p. Monografia (Pós Graduação – MBA em Administração e Sistemas de Informações) – Faculdade de Administração, Ciências e Turismo – Universidade Federal Fluminense, Niterói, 2006.

SOUZA, L. A. A.; DYNIEWICZ, A. M., KALINOWSKI, L. C. (s.n.t.). Auditoria: Uma abordagem histórica e atual.

TIBÚRCIO, C. PCAOB. 2008. Disponível em <http://www.contabilidade-financeira.com/2008/05/pcaob.html.> Acesso em: 03 mai. 2014.

APÊNDICE A

Relação de Documentos Consultados da EY

N°	Título	Tipo de Documento	Ano do Documento
1	Empresa A - Gestão de Mudanças	Papel de Trabalho da Auditoria	2013
2	Empresa A - Monitoramento de Mudanças	Papel de Trabalho da Auditoria	2013
3	Empresa A - SoD em Gestão de Mudanças	Papel de Trabalho da Auditoria	2013
4	Empresa A - Comitê de Mudanças	Papel de Trabalho da Auditoria	2013
5	Empresa A - Carta de Recomendações à Gestão	Relatório de Auditoria	2013
6	Empresa A - Scripts de Segurança	Papel de Trabalho da Auditoria	2013
7	Empresa A - Parametrização de Senhas	Papel de Trabalho da Auditoria	2013
8	Empresa A - Super Usuários e Usuários Genéricos	Papel de Trabalho da Auditoria	2013
9	Empresa A - Concessão de Acessos	Papel de Trabalho da Auditoria	2013
10	Empresa A - SoD em Gestão de Acessos	Papel de Trabalho da Auditoria	2013
11	Empresa A - Revogação de Acessos	Papel de Trabalho da Auditoria	2013
12	Empresa A - Walkthrough dos Controles Gerais de TI	Papel de Trabalho da Auditoria	2013
13	Empresa A - Validação Periódica de Acessos	Papel de Trabalho da Auditoria	2013
14	Empresa B - Gestão de Mudanças	Papel de Trabalho da Auditoria	2013
15	Empresa B - Gerenciamento de Mudança (Implantação e Atualização de Programas, Sistemas, Infraestrutura)	Evidência de cliente	2013
16	Empresa B - Carta de Recomendações à Gestão	Relatório de Auditoria	2013
17	Empresa B - SoD em Gestão de Mudanças	Papel de Trabalho da Auditoria	2013
18	Empresa B - Parametrização de Senhas	Papel de Trabalho da Auditoria	2013

N°	Título	Tipo de Documento	Ano do Documento
19	Empresa B - Super Usuários e Usuários Genéricos	Papel de Trabalho da Auditoria	2013
20	Empresa B - Revisão Periódica de Usuários	Papel de Trabalho da Auditoria	2013
21	Empresa B - Revogação de Acessos	Papel de Trabalho da Auditoria	2013
22	Empresa B - Fatores Mitigantes para Gestão de Identidades	Papel de Trabalho da Auditoria	2013
23	Empresa B - SoD em Gestão de Acessos	Papel de Trabalho da Auditoria	2013
24	Empresa B - Walkthrough dos Controles Gerais de TI	Papel de Trabalho da Auditoria	2013
25	Empresa B - Acesso Físico	Papel de Trabalho da Auditoria	2013
26	Empresa B - Backup e Restore	Papel de Trabalho da Auditoria	2013
27	Empresa B - Job Scheduling	Papel de Trabalho da Auditoria	2013

ANEXO A

Definição da população e amostra

Para determinar a amostra a ser testada, deve ser considerada a frequência com que o controle é executado, como pode ser observado no Quadro 3.

Quadro 6 – Frequência do controle.

Frequência do controle	Tamanho da população	Amostra
Controle Sob demanda	-	-
Controle Diário	252 dias úteis ou 365 dias corridos	25
Controle Semanal	52	10
Controle Quinzenal	26	10
Controle Mensal	12	3
Controle Trimestral	4	2
Controle Semestral	2	1
Controle Anual	1	1

Fonte: EY, 2013.

Para controles efetuados sob demanda ou cuja execução seja realizada várias vezes ao dia, será utilizada 10% da população, como amostra. Salvo seguintes exceções mostradas no Quadro 7.

Quadro 7 – Exceções.

Tamanho da população de amostra	Número de itens para teste
Para populações maiores que 250 itens	Serão testados 25 itens como amostra
Para populações menores que 50 itens	Serão testados 5 (cinco) itens como amostra
Para populações menores que 5 itens	Será utilizada toda população como amostra
Para controles automatizados	Será testado apenas 1 (um) item como amostra

Fonte: EY, 2013.

Para controles cuja periodicidade seja perene ou não definida, deverá ser realizada uma análise individual como forma de determinar a melhor amostra de testes.

Para toda e qualquer amostra, caso sejam identificados problemas com pelo menos 1 (um) item, durante a fase de testes, o controle será considerado como não conforme.