IMPLANTAÇÃO DA NORMATIVA SOX NUMA EMPRESA VAREJISTA: UM RELATO DE EXPERIÊNCIA

Bruno Souza Marinho da Cunha[1]

RESUMO

Toda e qualquer empresa ao colocar suas ações a venda na bolsa de valores de Nova York necessita garantir aos seus novos acionistas a veracidade das informações financeiras em seus sistemas e para isso existem normas de segurança a serem cumpridas.

Em julho de 2002 foi promulgada a lei de Sarbanes-Oxley nos Estados Unidos, estabelecendo uma das maiores reformas já ocorrida na regulamentação do mercado de capital norte americano. A lei foi uma resposta aos escândalos contábeis que envolveram grandes companhias consideradas umas das melhores para se trabalhar, do qual estabeleceu regras para a padronização e aperfeiçoamento dos controles financeiros das empresas que possuem capital negociado na Bolsa de Nova Iorque (NYSE). Com isso, seria necessário recuperar a confiança dos investidores ao mercado financeiro, e precaver os danos que ocorreram na decorrência das fraudes cometidas pelos executivos dessas empresas, como por exemplo, a Enron, Arthur Andersen e Worldcom.

Realizou-se uma pesquisa qualitativa do tipo bibliográfico e estudo de caso, e foi avaliado um sistema de âmbito financeiro de uma grande empresa multinacional com ramificações no estado de Sergipe, de forma adequá-lo a normativa SOX, garantindo assim informações condizentes com a realidade da organização, para desta forma tomar as melhores decisões e transparecer confiabilidade para o mercado financeiro em geral.

Palavras-chaves: Projeto, Informação, Segurança, SOx, Bolsa de valores

[1] Formado em Sistemas de Informação pelo Centro Universitário da Bahia (FIB), trabalha como líder de projetos de tecnologia na ITP Soluções corporativas. Email: brunosmarinho@gmail.com

1. INTRODUÇÃO

Esse projeto tem como finalidade relatar a implantação de normas de segurança em sistemas de informação de companhias varejistas de maneira que possa aumentar a confiabilidade dos dados ai armazenados, para atender a normativa SOx, a qual será melhor detalhada no decorrer do documento. Além disso, mostrar a experiência adquirida com essa implantação, mostrando as lições aprendidas de maneira que possa compartilhar com a sociedade esse conhecimento.

O primeiro passo é iniciar uma consultoria indicada pela Bolsa de Valores de Nova York (NYSE), avalia os sistemas da empresa e informam quais serão alcançados pela lei SOX. Pois alguns não são sistemas críticos, que envolvam dados financeiros ou sensíveis[2]. Além do mais, possa existir que em um determinado momento, algum ou alguns dos sistemas sejam substituídos por outros mais atualizados ou simplesmente por estratégica da empresa; daí então, serão avaliados, pois, estes a depender do prazo em que venham a ser substituídos, poderão ou não estar no escopo da auditoria. Definido o escopo, deve-se fazer o levantamento em cada sistema se atende ou não a cada item das regras, e em cada "lacuna" não cumprida, tem-se um GAP[3]. De posse dos gaps levantados (vide lista de gaps no anexo I), tem que se remediá-los (corrigi-los) antes da auditoria. O ideal é fazer uma auditoria interna anteriormente à auditoria oficial.

2. REFERENCIAL TEÓRICO

a. Lei Sarbanes-Oxley (SOx)

A Lei Sarbanes-Oxley (Sarbanes-Oxley Act, normalmente abreviada em SOx ou Sarbox) é uma lei dos Estados Unidos criada em 30 de julho de 2002 por iniciativa do senador Paul Sarbanes (Democrata) e do deputado Michael Oxley (Republicano). Segundo a maioria dos analistas esta lei representa a maior reforma do mercado de capitais americano desde a introdução de sua regulamentação, logo após a crise financeira de 1929.

[2] Informações de pessoa física, tais como: endereço, cpf, rg.

[3] s.m. (pal. ing.) Distanciamento; afastamento, hiato, separação, distanciamento (entre duas coisas); **lacuna**, vácuo. Divergência, diferença. Atraso (econômico, tecnológico etc.).

A criação desta lei foi uma consequência das fraudes e escândalos contábeis que, na época, atingiram grandes corporações nos Estados Unidos (Enron, Arthur Andersen, WorldCom, Xerox etc...), e teve como intuito tentar evitar a fuga dos investidores causada pela **insegurança** e perda de confiança em relação as escriturações contábeis (**segurança da informação**) e aos princípios de **governança** nas empresas.

A SOx se aplica a todas as empresas, sejam elas americanas ou estrangeiras, que tenham ações registradas na SEC (Securities and Exchange Comission, o equivalente americano da CVM brasileira). Isso inclui as empresas estrangeiras que possuem programas de ADRs (American Depositary Receipts), do nível 2 ou 3, nas bolsas de valores dos EUA.

A SOx prevê a criação, nas empresas, de mecanismos de auditoria e segurança confiáveis, definindo regras para a criação de comitês encarregados de supervisionar suas atividades e operações, formados em boa parte por membros independentes. Isso com o intuito explícito de evitar a ocorrência de fraudes e criar meios de identificá-las quando ocorrem, reduzindo os riscos nos negócios e garantindo a transparência na gestão.

Para supervisionar os processos de auditoria das empresas sujeitas a SOx, foi criado o Public Company Accounting Oversight Board (PCAOB ou seja Conselho de Auditores de Companhias Abertas) que tem a missão de estabelecer as normas de auditoria, controle de qualidade, ética e independência em relação aos processos de inspeção e a emissão dos relatórios de auditoria. São previstas inspeções às empresas de auditoria para obrigá-las a cumprir as regras estabelecidas e estar sempre em consonância com a SEC.

De forma ainda mais notável, a Lei Sarbanes-Oxley privilegia o papel crítico do “controle interno”.

O **controle interno** é um processo executado pela Diretoria, pelo Conselho de Administração ou por outras pessoas da companhia que impulsionam o sucesso dos negócios em três categorias:

- Eficácia e eficiência das operações.
- Confiabilidade dos relatórios financeiros.
- Cumprimento de leis e regulamentos aplicáveis.

b. Controle Interno

A palavra controle apareceu por volta de 1600, como significado de "cópia de uma relação de contas", um paralelo ao seu original. Deriva do latim *contrarotulus,* que significa "cópia do registro de dados". Taylor, o grande contribuinte da Administração Científica, doutrinava que existiam quatro princípios da administração, sendo um deles o princípio do controle, consistindo em: "controlar o trabalho para se certificar de que o mesmo está sendo executado de acordo com as normas estabelecidas e segundo o plano previsto. A gerência deve cooperar com os trabalhadores, para que a execução seja a melhor possível".

O controle interno pode ser definido como o planejamento organizacional e todos os métodos e procedimentos adotados dentro de uma empresa, a fim de salvaguardar seus ativos, verificar a adequação e o suporte dos dados contábeis, promover a eficiência operacional e encorajar a aderência às políticas definidas pela direção. É um processo executado pelo conselho de administração, gerência e outras pessoas de uma organização, desenhado para fornecer segurança razoável sobre o alcance do objetivo compreendendo:

- Eficácia e eficiência operacional;
- Mensuração de desempenho e divulgação financeira;
- Proteção do patrimônio;
- Cumprimento de leis e regulamentações;
- Fidedignidade da informação utilizada para o processo decisório e gerencial;
- Observação às políticas e diretrizes estabelecidas pela direção.

Tipos, objetivos, princípios, testes substantivos e de aderência

i) Tipos de Controle

Prévio ou preventivo	Aquele que antecede a conclusão ou operatividade do ato, como requisito para sua eficácia (Autorização para saída de veículo oficial).
Concomitante ou sucessivo	Aquele que acompanha a realização do ato para verificar a regularidade de sua formação. É o controle no decorrer do ato (conferência de mercadorias com a NF no ato do

	recebimento).
Subsequente ou corretivo	Aquele que se efetiva após a conclusão do ato controlado, visando corrigir-lhe de eventuais defeitos, declarar a sua nulidade ou dar-lhe eficácia (conciliação bancária).

ii) Objetivos do Controle Interno:

- Auxiliar a entidade a atingir seus objetivos;
- Proporcionar uma garantia razoável, nunca uma garantia absoluta;
- Auxiliar a entidade na consecução de seus objetivos.

Um adequado sistema de controle interno deve possuir:

- Relação custo-benefício;
- Qualificação adequada de funcionários;
- Descentralização de poderes e responsabilidades;
- Instruções devidamente formalizadas;
- Observação às normas legais, instruções normativas, estatutos e regimentos.

iii) Princípios de Controle Interno

Formas	Conceito
Segregação de funções	Ninguém deve ter sob sua responsabilidade todas as fases inerentes a uma operação; devem ser executadas por pessoas e setores independentes entre si.
Sistema de autorização e aprovação	Compreende o controle das operações através de métodos de aprovações; a pessoa que autoriza não deve ser a mesma que aprova para não expor ao risco os interesses da empresa.

Determinações de funções e responsabilidades	Determina a noção exata aos funcionários sobre suas funções, incluindo as responsabilidades do cargo com a definição através de organogramas.
Rodízio de funcionários	Corresponde ao rodízio dos funcionários para reduzir a possibilidade de fraudes.
Carta de fiança	Determina aos funcionários que em geral lidam com valores a responsabilidade pela custódia de bens e valores, resguardando a empresa e dissuadindo, psicologicamente os funcionários a tentações.
Manutenção de contas de controle	Indica a precisão dos saldos das contas detalhadas, geralmente controladas por outros funcionários.
Seguro	Compreende a manutenção de apólice de seguros, valores e riscos a que está sujeita a empresa.
Legislação	Atualização permanente sobre a legislação vigente, para diminuir riscos e não expor a empresa a contingências fiscais e legais.
Diminuição de erros e desperdícios	Indica a detecção de erros e desperdícios na fonte devido a controles mal definidos.
Contagens físicas independentes	Correspondem as contagens periódicas de bens e valores, visando aumentar o controle físico e proteger os interesses da empresa.
Alçadas progressivas	Compreende estabelecer de forma escalonada, dando aos altos escalões as principais decisões e responsabilidades.

c. Projeto

Segundo o Guia PMBOK em sua 4ª ed, projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. O temporário não quer dizer que seja curto, e sim o tempo de duração do projeto, onde o mesmo possui um inicio, meio e fim definidos.

Um projeto pode criar:

- ✓ Um produto;
- ✓ Uma capacidade de realizar um serviço;
- ✓ Um resultado (ex.: um projeto de pesquisa que beneficiará a sociedade).

d. Segurança da Informação

Informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe (SERRA, 2007, p.93).

"A Segurança da Informação pode ser usada como um diferencial na estratégia, especialmente em uma economia globalizada em que mais negócios são conduzidos eletronicamente." (EGAN, 2005, p.11).

Segurança da informação é a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. De acordo com a norma ABNT NBR ISO/IEC 17799:2005, o objetivo da política de segurança da informação é "Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes". Ela especifica que a Segurança da Informação é caracterizada pela preservação de:

- ✓ Confidencialidade: garantia de que a informação é acessível somente aos usuários autorizados;
- ✓ Integridade: garantia de que as informações não sejam alteradas indevidamente;
- ✓ Disponibilidade: garantia de que os usuários autorizados tenham acesso à informação sempre que preciso.
- ✓ Outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

e. Governança Corporativa

Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade (IBGC, 2015).

A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização.

Além disso, a governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócios. A governança de TI habilita a organização a obter todas as vantagens de sua informação, maximizando os benefícios, capitalizando as oportunidades e ganhando em poder competitivo. Esses resultados requerem um modelo para controle de TI que se adeque e dê suporte ao COSO ("Committe of Sponsoring Organisations of the Treadway Commission's Internal Control – Integrated Framework"), um modelo para controles interno amplamente aceito para governança e gerenciamento de riscos empresariais, e outros modelos similares.

Em resumo, para prover as informações de que a empresa necessita para atingir seus objetivos, os recursos de TI precisam ser gerenciados por uma série de processos naturalmente agrupados (COBIT 4.1, 2007, p.07).

Segundo o IBCG (Instituto Brasileiro de Governança Corporativa), a governança esta dividida em quatro princípios básicos: Transparência, Equidade, Prestação de Contas e Responsabilidade Corporativa.

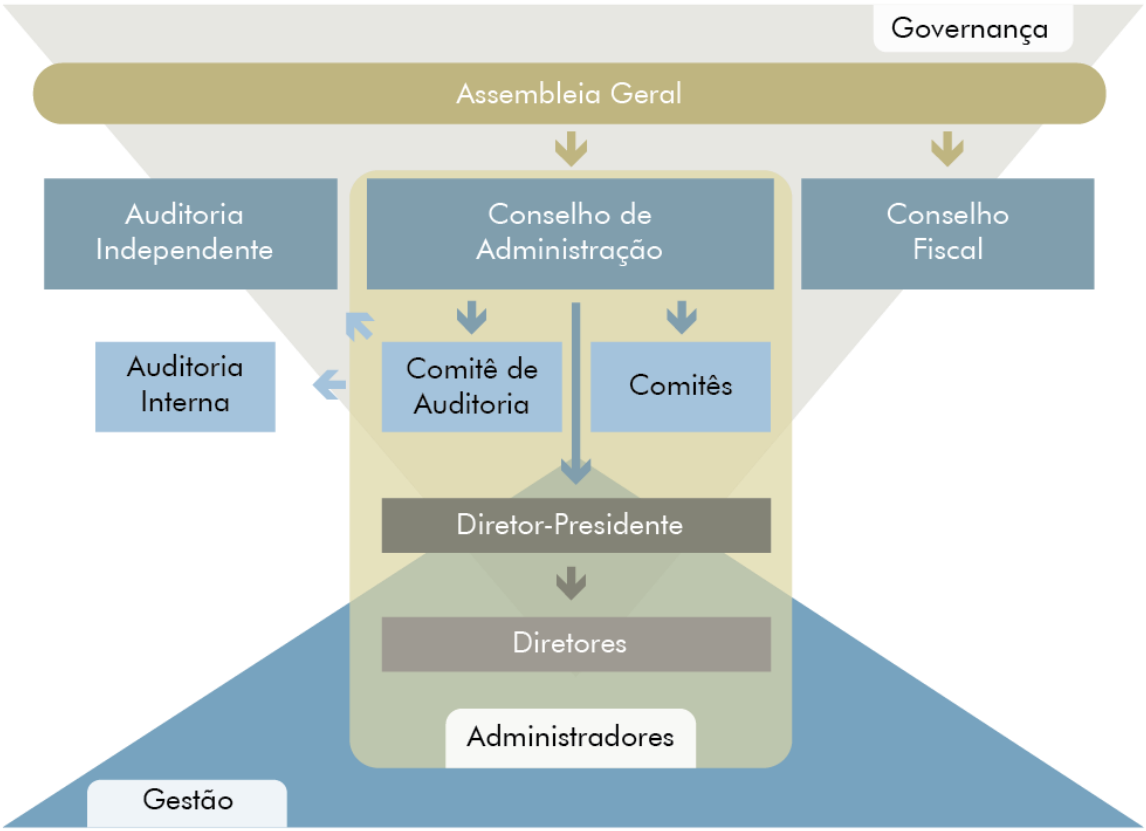

Figura 01 - Sistema de Governança (fonte: IBGC)

3. DESENVOLVIMENTO

A principal ideia de uma empresa varejista de grande porte ao entrar na Bolsa de Valores de Nova York é de angariar recursos, aumentando seu poder de investimento e para ampliar sua abrangência territorial. Com isso ganhará novos mercados e clientela para o seu crescimento.

O projeto para implantação da norma SOX é iniciado a partir de uma visão estratégica da empresa em poder disponibilizar a suas ações na bolsa de valores de Nova York. Partindo deste principio, devem-se coletar os requisitos iniciais, definir limites, premissas e restrições, Identificar as Partes Interessadas, os riscos preliminares e fatores de sucesso do projeto definir quais as etapas e escopo dos sistemas alcançados para fazer o levantamento dos GAPs.

Etapas realizadas durante o projeto:

- Termo de abertura do projeto (TAP)
- Definição dos sistemas alcançados
- Definição dos entregáveis
- Elaboração de cronograma e definição de prazos
- Auditoria interna
- Auditoria externa

Ao iniciar o projeto são definidas por uma consultaria externa, os sistemas incluídos no escopo e é passada uma lista de premissas as quais todos esses sistemas devem estar em conformidade. Essas premissas foram divididas em quatro distintos domínios para um melhor entendimento e organização:

A. Segurança da Informação e acesso a dados
    a. Acesso de pessoal de TI ao ambiente de produção por fora das aplicações
    b. Administração dos acessos por segurança da informação
    c. Restrição de acessos a transações críticas de negócios para usuários finais
    d. Restrição de acessos a transações criticas para usuários de sistemas

B. Desenvolvimento de manutenção de aplicações
    a. Acesso restrito e independente da área de desenvolvimento (Incluindo separação de ambientes). Excluir acessos para modificar qualquer componente de um programa.
    b. Registro histórico de alterações em aplicações.
    c. Aprovação formal das alterações por parte de desenvolvimento e por parte do usuário final.

C. Operações computadorizadas
    a. Administrar e monitorar a “malha” de processos.
    b. Realizar backups

A. Logs de acesso
    a. Registro e consolidação de eventos de Segurança (logs) nos aplicativos.

b. Registro y consolidação dos eventos de segurança (logs) da infraestrutura (serviços de diretórios, servidores, base de dados, dispositivos de segurança, ACS, Acessos remotos, acessos wireless, firewalls, antivírus e IPS).

Os sistemas que devem estar no escopo para as remediações são os que trabalham com dados financeiros e/ou sensíveis, tais como dados de informações pessoais de clientes e funcionários, pois a norma foi criada principalmente para conter falhas financeiras.
Cada sistema deve seguir os controles listados abaixo (fig. 02) com o máximo de rigor possível, pois todos os domínios serão analisados pela empresa auditora da bolsa de Nova York.

ÍTEM	DOMÍNIO	COMTROLE
1.1.1	Segurança de Base de dados	Existem pessoas de sistema e/ou negocio com acesso de forma direta à base de dados?
1.1.2	Segurança de pastas compartilhadas e diretórios de instalação	Existem pessoas de sistema e/ou negocio com acesso de forma direta a qualquer pasta onde se encontram instalados componentes da aplicação?
1.1.3	Segurança - Contas de serviço	Existem contas de serviço, especial ou com capacidades administrativas em conhecimento de alguma pessoa de sistemas ou negocio?
1.1.4	Segurança Interfaces	Existem pessoas de sistema e/ou negocio com acesso em forma direta a qualquer pasta onde se armazenam qualquer tipo de arquivos de interface o temporais?
1.1.5	Segurança - contas administrativas - acessos de emergência a ambientes produtivos.	Existem pessoas de sistemas e/ou negocio com qualquer tipo de acesso administrativo (root, admin, cofer, sa, administrator, etc)aos servidores (APP, Base de dados, etc)
1.1.6	Segurança APP Servers	Existem pessoas de sistemas e/ou negocio com qualquer tipo de acesso aos servidores (APP, Base de dados, etc).

ÍTEM	DOMÍNIO	COMTROLE
1.1.7	Segurança controle de operações	Existem pessoas de sistemas e/ou negocio com qualquer tipo de acesso que lhes permita administrar os serviços (stop, start, reiniciar jobs, etc) ?
1.1.8	Segurança gestão de Jobs Batch Imputs	Existem pessoas de sistemas e/ou negocio com qualquer tipo de acesso que lhes permita executar um Batch Imput sobre qualquer tabela, motor, base de dados?
1.1.9	Segurança Parametrização de aplicações	Existem pessoas de sistemas e/ou negocio com qualquer tipo de acesso que lhes permita realizar una modificação a qualquer arquivo o parâmetro de configuração ou parametrização da aplicação?
1.2.1	Administração da Segurança centralizada em SI.	A Segurança de sua aplicação é administrada por Segurança TI?
1.2.2	Administração da Segurança modulo de Segurança implementado em APP.	A Aplicação tem modulo para administração de Segurança?
1.2.3	Definição e configuração de perfis de acesso.	Encontram-se definidos e configurados os perfis de usuários sobre a aplicação.
1.2.4	Segurança Accounting, Usuários genéricos a nível de aplicação em usuários finais.	A aplicação conta com usuários genéricos utilizados por usuários finais?
1.2.5	Segurança Accounting, usuários genéricos em nível de aplicação em usuários de sistemas.	A aplicação conta com usuários genéricos utilizados por usuários de sistemas?
1.2.6	Segurança Accounting, Usuários genéricos de interface.	A aplicação conta com usuários genéricos utilizados por usuários de interfaces ou serviços?
1.2.7	Reportes de Acessos	A aplicação conta com a possibilidade de emitir relatórios do tipo: Últimos acessos ao sistema, tentativas falhas de acesso, ABM de Perfis e de Usuários, etc.

ÍTEM	DOMÍNIO	COMTROLE
1.3.1	Definição de transações critica.	Encontram-se definidas as transações criticas na aplicação e a necessidade de segregação especifica por temas de controle?
1.3.2	Transações criticas validação gerência de risco.	As “transações criticas” e suas necessidades de segregação devem ser validadas com a gerência de risco.
1.3.3	Implementação de mudanças em sistemas	A segregação definida e as “transações criticas” devem ser implementadas por Segurança TI nos sistemas.
1.3.4	Aceitação de provas de permissão por parte do usuário final.	As mudanças implementadas devem ser provadas e validadas pelo usuário final "champion user".
1.4.1	Acesso a ambiente produtivo para usuários de sistemas.	Exceto os responsáveis de Operações TI, nenhum usuário de Sistemas deve contar com acesso aos ambientes produtivos das aplicações.
2.1.1	Existência de ambientes separados	A aplicação conta com ao menos 2 ambientes separados ? (produção e teste).
2.1.2	Separação de acessos em ambientes não produtivos ou baixos (desenv e homolog) e de produção.	Os acessos devem estar estritamente separados, aos ambientes produtivos das aplicações. Somente podem acessar em situação normal a área responsável de operar as aplicações instanciadas em Operações TI. Em situações normais somente um grupo de usuários reduzido (máximo 03 por aplicação), poderá ter permissão de visualização em tabelas ou mediante transações especificas do sistema. No caso que se requeira modificar para corrigir algum tipo de problema em produção, isto devera realizar-se mediante o uso de um usuário de emergência controlado e custodiado em SAT.
2.1.3	Modificações em programas e/ou qualquer componente de software em ambientes	Todas as modificações a qualquer componente de software incluindo qualquer aspecto de configuração das aplicações, deve realizar-se exclusivamente

ÍTEM	DOMÍNIO	COMTROLE
	produtivos via SPP.	mediante o processo formal de SPP.
2.1.4	Modificações em programas e/ou qualquer componente de software em ambientes produtivo só Operações TI	Todas as modificações a qualquer componente de software incluindo qualquer aspecto de configuração das aplicações devem ser realizado exclusivamente por integrantes da área de OPERAÇÃOES IT.
2.2.1	Gestão de versões e documentação de mudanças	Todas as mudanças de versões devem estar associadas a um ticket formal e contar com a documentação que respalde o mesmo.
2.2.2	Documentação de mudanças a nível técnico.	Todas as aplicações devem contar com um repositório de versões em forma eletrônica, onde deve ficar evidência de todas as modificações realizadas e um link à informação gerada no ticket da mudança (ponto anterior desta planilha 2.2.1).
2.3.1	Documentação formal de aceitação por parte de usuário final e equipe funcional.	Todas as modificações a programas devem ser aprovadas pelo usuário final e a equipe funcional. Ficando guardadas como evidenciados requerimentos originais, a aceitação das provas e a aceitação final de funcionamento por parte do usuário final.
3.1.1	Documentação de todos os processos da aplicação.	Todos os processos da aplicação se encontram formalmente documentados (Responsável do processo, detalhe funcional do processo, escalação).
3.1.2	Execução de todos os processos por parte de Operações TI	Todos os processos da aplicação são executados pela área de Operações TI.
3.1.3	Monitoramento de todos os processos por parte de Operações TI	Todos os processos da aplicação são monitorados pela área de Operações TI.
3.2.1	Backup de ambientes e de configuração	Toda aplicação deve contar com o backup da configuração do ambiente produtivo.

ÍTEM	DOMÍNIO	COMTROLE
3.2.2	Backup de Dados	Toda aplicação deve contar com o backup de dados do ambiente produtivo.
4.1.1	Registro de Logs	Toda aplicação deve registrar eventos de Segurança segundo a norma vigente.
4.1.2	Centralização e Correlação de Eventos	Todos os registros de Segurança devem ser guardados em forma centralizada.
4.2.1	Registro de Logs	Todos os servidores de aplicativos e de base de dados devem registrar eventos de Segurança segundo a norma vigente.
4.2.2	Centralização e Correlação de Eventos	Todos os registros de Segurança devem ser guardados em forma centralizada.

Fig. 02 – Lista de controles (GAPS)

De posse da lista dos gaps acima, deve-se fazer uma validação para cada sistema. Cada ítem deve ser analisado junto à equipe de aplicações para um melhor entendimento e validação se há um Gap neste quesito ou não. Após esta etapa, partimos então para definir qual o prazo para a remediação para cada Gap levantado na etapa anterior. Para ter como encerrado o Gap, deve-se fazer um documento de encerramento de Gap, o qual deve conter:

- Informação do Gap encerrado;
- Como foi realizada a correção;
- Estado anterior;
- Estado atual;
- Evidência[4] de que já esta aplicada a alteração para encerramento do Gap.

[4] s.f. Caráter do que é evidente, manifesto: a evidência de uma prova. Evidência de fato, a que se obtém por meio da observação. Recusar-se à evidência, não querer convencer-se. Estar em evidência, em destaque, em bom conceito ou situação.

4. CONCLUSÃO

De acordo com o conhecimento adquirido nesse estudo e a experiência vivenciada no projeto SOx, é importante poder afirmar que um projeto para disponibilizar as informações seguras e disponíveis no momento de que a empresa necessita para atingir seus objetivos, é necessário um controle interno bem elaborado, atendendo aos elementos-chave : valor, risco e controle, além de gerenciar os processos internos para atingir uma excelência na utilização dos recursos de TI , contribuindo assim para a eficácia da governança de TI.

Com o fim da implantação da norma SOx na companhia, podemos concluir que o sucesso obtido, foi devido ao grande esforço e empenho dos colaboradores da área de segurança de TI; a qual, foi designada para esta tarefa. SOx não acaba. Segue pelo tempo em que a empresa tiver suas ações na bolsa de NY, ou seja, uma vez na bolsa, a possibilidade de seguir, é praticamente total durante seu ciclo de vida.

Como lições aprendidas, é possível citar várias, tais como:

- Em um grande projeto, onde a sua conclusão é fundamental para a sobrevivência da companhia, a necessidade de ter uma postura mais dura em relação aos seus colaboradores envolvidos, é de fato muito importante, pois sem isso o andamento do mesmo pode ser prejudicado devido a morosidade e falta de comprometimento doso mesmos, ocasionando um atraso ou ate mesmo tendo um resultado não satisfatório.
- A segurança corporativa é de fato algo em aumenta a insatisfação de alguns colaboradores mais desinformados, pois isso resulta em procedimentos mais bem elaborados, detalhados e mais trabalhosos, podendo inclusive aumentar a burocracia interna. Entretanto, garantirá a sua alta gerencia, um ganho de fidelidade de seus dados e garantia de um processo mais seguro.
- A frase popular conhecida “Não coloque os carros na frente dos bois – Autor desconhecido” é muito bem empregada nesse estudo de caso, pois a ideia de ter incluído a empresa na bolsa de NY sem ter iniciado as devidas correções em seus sistemas informáticos ou não; foi uma grande antecipação o que de fato ocasionou uma corrida interna para as devidas adequações. Entretanto foi o grande motivador para que as atividades acontecessem.

5. REFERÊNCIAS

- http://www.fraudes.org/showpage1.asp?pg=312 **Monitor da Fraudes** Acesso em 11 jan. 2013
- http://controladoriageral.mg.gov.br/ **Controladoria-Geral do Estado de Minas Gerais** Acesso em 11 jan. 13
- http://www.ibgc.org.br/inter.php?id=18161 **Instituto Brasileiro de Governança Corporativa**. Acesso em: 10 jan 2015.
- PROJECT MANEGEMENT INSTITUTE INC, **Um guia do Conhecimento em Gerenciamento de Projetos** (Guia PMBOK), 4ª Ed. Pensilvânia – EUA, 2008.
- IT GOVERNANCE INSTITUTE™. **CobiT 4.1**. Illinois – EUA, 2007
- EGAN, M. E. **Seis Desafios Significativos para a Segurança da Informação**. 2005. Disponível em: https://www-secure.symantec.com/region/br/enterprisesecurity/content/expert/BR_4779.html .Acesso em: 10 jan. 2015
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma ISO/IEC 17799**. Tecnologia da informação – Técnicas de segurança - Código de pratica para a gestão da segurança da informação. Rio de Janeiro, 2005.
- SERRA, J. PAULO. **Manual de Teoria da Comunicação**. Covilhã: Livros Labcom, 2007. 203 pp. p. 93-101. ISBN 978-972-8790-87-5

APÊNDICE I

Com a intenção de coletar dados subjetivos, foi realizada uma entrevistas estruturada[5] com um dos líderes do projeto para a implantação do SOx na empresa. As perguntas foram previamente elaboradas de maneira a obter o máximo de informação do projeto como todo.

1. Entrevista com participante do projeto

Entrevistador: Houve um estudo da empresa antes da decisão de implantar o SOX?

Entrevistado: *Como a BVNY da uma opção de escolha na qual a empresa põe as ações a venda, recebe o dinheiro e se adequa em 2 anos ou se adequa em dois anos, passa pela auditoria e põe as ações a venda para receber o dinheiro, Não houve nenhum estudo para a implantação da normativa. A empresa optou por colocar as opções a venda antes de adequar os sistemas internos no período de dois anos.*

Entrevistador: A empresa teve alguma orientação externa na ajuda da implantação?

Entrevistado: *Sim. Tivemos a ajuda de duas consultorias externas. Uma para adequar os sistemas e o entorno de acesso aos sistemas e outra para normalizar a parte de processos internos de forma a manter segurança, realizando a segregação de função, utilizando a seguinte estratégia: Quem aprova o pedido, não pode solicitar, quem compra não vende, etc. Onde a premissa é de que a mesma pessoa não pode ter a permissão de interferir de forma ativa em prol do seu favorecimento. Sempre haverá uma pessoa que aprovará sua solicitação.*

[5] Entrevista Estruturada: são elaboradas mediante questionário totalmente estruturado, ou seja, é aquela onde as perguntas são previamente formuladas e tem-se o cuidado de não fugir a elas (LODI, 1974 apud LAKATOS, 1996).

Entrevistador: Como você via a empresa antes do SOX?

Entrevistado: *Via como uma empresa onde as coisas funcionavam de forma insegura, informal e desorientada, porem funcionava. A questão toda se dá porque um dia haverá um problema (e certamente haverá) que não se saberá como agir, pois não havia sido pensado ou não se saberá quem fez e como fez para ajudar na sua solução. E hoje não temos o melhor dos mundos, mas já se tem um modelo definido que ajuda bastante na confiabilidade dos acessos como na fidelidade dos dados lançados nos sistemas.*

Entrevistador: Qual a importância do projeto Sox para a área de segurança da empresa?

Entrevistado: *O projeto veio nortear a empresa no âmbito da segurança tanto nos acessos aos entornos dos sistemas financeiros, quanto nos próprios sistemas, garantindo assim um dado fidedigno e uma informação real, sem ações não autorizadas e devidamente documentadas nos sistemas da empresa. Com isso a empresa passará a dar garantias tanto a seus acionistas como a sua diretoria das informações extraídas de seus sistemas. Também ganhamos segurança nos processos operacionais, nas lojas, pois quem faz o pedido não é quem compra, quem recebe não é quem valida e assim por diante. Antes não tínhamos essa segregação, o que poderia causar fraudes difíceis de serem descobertas.*

Entrevistador: Qual foi sua maior dificuldade para a implantação? Você sentiu resistência por parte da área de TI por ter retirado acessos que facilitavam o trabalho deles?

Entrevistado: *A maior dificuldade foi colocar na cabeça das pessoas que o projeto era importante para a companhia e que os prazos para as devidas correções nos sistemas deveriam ser cumpridos pois uma falha ou uma falta, poderia causar-lhe danos financeiros enormes. O uso da persuasão ou do convencimento não foi suficiente para lograr os resultados desejados. Foi necessário intervir na perda financeira e no medo da demissão de funcionários para que o andamento das atividades seguisse o fluxo adequado.*

Entrevistador: Ao final de tudo isso, você faria a implantação da mesma forma ou mudaria algo?

Entrevistado: *Mudaria sim. Duas coisas: A começar pela opção de implantação. Primeiro eu iria realizar as alterações nos sistemas e processos internos para daí então colocar as ações na BVNY. Pois desta maneira seria menos doloroso e diminuiria o impacto na operacionalização do dia a dia. E em segundo que o apoio da alta gerencia fosse mais incisivo com maior divulgação para os participantes do projeto, pois o envolvimento e conhecimento da causa por todos os participantes, gerando um maior comprometimento e em consequência contribui para o sucesso do mesmo.*