AUDITORIA SARBANES-OXLEY APLICADA À IND-FORCE GROUP. IMPACTOS E BENEFÍCIOS NO TOCANTE AOS CONTROLES DE SEGURANÇA DA INFORMAÇÃO APLICADOS NO BRASIL

Felipe Caldeira Cota Melo Sanchez

RESUMO: Este artigo cientifico foi desenvolvido a fim de observar os impactos positivos e negativos ao se adequar uma organização multinacional do ramo automotivo às exigências da lei Sarbanes-Oxley (SOX), em especial ao se observar as exigências narradas em sua sessão 404 (quatrocentos e quatro), que faz menção à determinação de avaliação anual de controles e procedimentos internos para a emissão de relatórios financeiros. Tais impactos foram observados por meio do resultado obtido em pesquisa realizada junto aos usuários das áreas impactadas, conforme plano diretor de adequações processuais que abrangem os controles internos da organização, sua área de tecnologia da informação (TI) e área de segurança da informação (SI), assim como a partir dos resultados obtidos nas auditorias realizadas junto a área de TI e SI frente aos seus respetivos controles narrados na matriz de controles da TI e que foram consideradas instrumentos de suporte na obtenção dos resultados e informações necessárias para produção deste artigo, que se concentrou em demostrar o conjunto de esforços aplicados pela organização e seus resultados específicos nas áreas supracitadas.

Palavras-chave: Segurança da Informação. Sarbanes-Oxley. Auditoria

1 INTRODUÇÃO

Em setembro de 2013 com a fusão coorporativa entre empresas de um grupo multinacional do ramo automotivo, nasceu a Ind-Force Group.

O grupo de marcas anteriormente compostos pelas empresas Bulldozer e NH-Force (Grupo Force), se tratava de um grupo de capital aberto e participante da comercialização de títulos nas bolsas de valores Norte Americanas.

Com a nova fusão de empresas que originou o novo grupo Ind-Force, as empresas Long-Way, Hot-Gear e PT-Goals foram adicionadas às empresas Bulldozer e NH-Force, formando uma gigante do ramo automotivo industrial chamada Ind-Force Group.

Entretanto, as novas empresas então integradas não compartilhavam do mesmo rigor no tocante aos controles internos, já que estas não se encontravam até este momento, contempladas entre as empresas que publicam valores na bolsa de valores Norte Americana e consequentemente não passavam pelo rigor das regras e controles exigidos pela lei SOX.

O cenário apresentado neste artigo, irá se ater aos controles de SI considerados premissas para a certificação SOX no novo grupo que se formou da fusão supracitada, e que estão detalhados na seção ANEXO, através do **ANEXO A** – Descrição dos Controles SOX da orga-

---

[1] Artigo apresentado como trabalho de conclusão do curso de Especialização em Gestão da Segurança da Informação como requisito parcial para obtenção do título de Especialista. Orientador: Professor Luiz Otávio Botelho Lento. Belo Horizonte, 2018

nização Ind-Force, bem como o processo de auditoria aplicado para obtenção desta certificação, detalhada na subseção 2.6.1 Ordem de auditorias realizadas na Ind-Force Brasil Anualmente.

Como caminho natural para implantação dos controles de SI auditados pela SOX, torna-se obrigatória à confecção de uma matriz de controles da TI, com foco na segurança de informações e seus ativos. A matriz de controles confeccionada para suportar os controles de TI e SI da Ind-Force Brasil estão detalhados na seção ANEXO, através do item **ANEXO A** – Descrição dos Controles ITGC SOX. Esta matriz, por sua vez, se torna parte de um processo mais abrangente que contempla os controles internos de toda organização para itens que impactam direta ou indiretamente às finanças coorporativas.

Diante deste novo cenário, houve a necessidade da adequação das práticas de governança coorporativa, controles internos e controles da TI em suas ações que visão salvaguardar a SI para todas as empresas e marcas envolvidas nesta fusão a fim de atender às exigências da lei SOX.

Ao se considerar que o grupo Ind-Force não tem como um de seus produtos finais a TI e consequentemente a SI como *business*, mas considerando a participação vital da TI e da SI nos processos e sistemas que impactam direta ou indiretamente os resultados financeiros desta organização, auditorias internas e externas independentes passam a ser realizadas de forma recorrente, conforme detalhado na subseção 2.6 AUDITORIAS SOX ITGC IND-FORCE BRASIL deste artigo, trazendo consigo a necessidade da aplicação de novos controles de TI que visam garantir o nível aceitável de SI ou da adequação dos controles existentes, deixando em aberto quais seriam de fato os impactos e benefícios oriundos deste novo nível de exigências para adequação à lei SOX, especificamente no que tange à TI e sua segurança de informação.

As auditorias aplicadas sistematicamente aos controles de SI seriam benéficas para a organização? As auditorias em TI e SI trariam benéficos aos produtos e serviços oferecidos pela organização? Haveria um custo maior do que o benefício? A TI se favoreceria desta obrigatoriedade? Os controles trariam maior morosidade aos processos do negócio ou seria a oportunidade de melhorar o desempenho? Haveria de fato uma significativa melhora na governança de SI? Qual seria a percepção dos agentes envolvidos nos processos modificados e (ou) desenvolvidos para atender as exigências de controle?

Segundo José Mauricio Santos Pinheiro (2007), o cumprimento da Lei Sarbanes-Oxley pode ser uma tarefa difícil, mas com pesquisa e planejamento adequados ela pode ser usada para corrigir deficiências adicionais na estrutura de TI das empresas, adequando-as à nova realidade que se apresenta.

Por outro lado, Holmstrom e Kaplan (2003) argumentam que os custos privados de implementação da SOX podem superar os benefícios privados, uma vez que a eliminação completa de fraudes é muito dispendiosa. Um nível zero de fraude só pode ser obtido utilizando-se de instrumentos que gerem severas restrições no que se refere à flexibilidade com que a companhia é gerida. Nesse sentido, a falta de flexibilidade pode ser mais danosa para o conjunto de firmas do que alguns poucos escândalos decorrentes da maior liberdade corporativa.

2 DESENVOLVIMENTO

2.1 LEGISLAÇÃO APLICADA À EMPRESAS DE CAPITAL ABERTO

No Brasil a legislação societária que busca disciplinar a relação entre acionistas e empresas de capital aberto, se dá por meio da Lei de Sociedades Anônimas de 1976 e pelo novo Código Cível de março 2016.

Para empresas de capital aberto que publicam títulos nas bolsas de valores Norte Americanas, a lei SOX de julho 2002, foi uma consequência das fraudes e escândalos contábeis que, na época, atingiram grandes corporações nos Estados Unidos e teve como intuito tentar evitar a fuga dos investidores causada pela insegurança e perda de confiança em relação as escriturações contábeis e aos princípios de governança nas empresas. (PORTAL DE AUDITORIA, 2018, p. 1).

Para este estudo de caso iremos nos ater à lei Norte Americana SOX, cujas empresas envolvidas na pesquisa cientifica aqui realizada se aplicam.

2.2. A LEI SOX

Como resposta ao escândalo causado pela fraude contábil que atingiu as corporações Norte Americanas, protagonizada em especial pela empresa de energia Enron, uma das líderes mundiais de seu segmento na época, foi sancionada pelo então presidente George W. Bush em 30 de julho de 2002 a lei SOX, escritas pelo senador Paul Sarbanes e pelo deputado Michael Oxley.

> A Lei exigiu várias reformas para melhorar a responsabilidade corporativa, melhorar a divulgação financeira e combater a fraude corporativa e contábil, e criou o "Conselho de Supervisão de Contabilidade de Empresas Públicas", também conhecido como PCAOB, para supervisionar as atividades da profissão de auditoria. (SEC -U.S. SECURITIES AND EXCHANGE COMMISSION, tradução nossa)

2.3 IMPACTOS DA SOX SOBRE A SEGURANÇA DA TI

Entre as 69 (sessenta e nove) seções distribuídas pelos 11 (onze) capítulos da lei SOX, destaca-se a seção 404 (quatrocentos e quatro) da categoria aprimoramento das divulgações financeiras, como àquele que tem maior influência sobre os controles de SI, uma vez que nesta seção exige-se a avaliação anual dos controles e procedimentos internos por meio de auditorias externas e independentes para fins de emissão do relatório financeiro, incluindo os controles de TI que são voltados à Segurança das Informações.

É improvável que uma organização na presente era tecnológica, possa ser gerida e controlada sem a utilização da TI. Desta forma é fácil dizer que a TI está entre as áreas de maior impacto ao se adequar uma organização às exigências da lei SOX, em especial em seus controles que visão a Segurança das Informações.

Segundo PINHEIRO (2007), existem dois pontos de maior criticidade a serem observados no uso dos sistemas de informação no tocante à lei SOX, sendo:

> Segurança de sistemas de informação - A adequação do conteúdo da SOX deve ocorrer entre toda a cadeia de comunicação da empresa, principalmente nos recursos concernentes a informações financeiras. Sistemas de gestão - ERP (Enterprise Resource Planning), aplicativos contábeis, sistemas de relacionamento com clientes - CRM (Customer Relationship Management), Sistemas de gerenciamento de cadeia de suprimentos (Supply Chain Management), em conjunto com as demais aplicações de comunicação, banco de dados e armazenamento de informações precisam estar em sintonia com as regras adotadas na legislação. Consequentemente, a atenção do administrador deve se estender à utilização de todo e qualquer recurso tecnológico da empresa por parte dos funcionários e as políticas de segurança da informação adotadas devem ser adaptadas ao teor do Ato Sarbanes-Oxley. Uma atenção especial também deve ser conferida a terceirização (outsourcing) de serviços; Controle de registros - Um arquivo de registros de procedimentos é fundamental para a tranquilidade dos administradores. Estes registros devem ser tanto tangíveis (em papel) ou intangíveis (arquivos digitais e demais mídias) e a redundância em sistemas de backup é altamente recomendada. No bojo da lei encontram-se disposições que penalizam severamente a falsificação, destruição e perda de documentos e registros, bem como preveem a observação de prazos para seu armazenamento após o fechamento de cada exercício fiscal.

2.4 RESULTADOS ALCANÇADOS EM ORGANIZAÇÕES QUE SE ADEQUAM À SOX

Diante das informações esplanadas até aqui, conclui-se que a adequação dos controles internos das organizações que adentram as exigências da lei SOX abrangem de forma direta os controles da TI em seus requisitos de SI, e esta adequação é um fator *sine qua non* para as empresas de capital aberto que desejam publicar títulos na bolsa Norte Americana. Entretanto, uma vez que controles diversos passam a ser auditados sob risco de penalidades da lei, e os controles e processos alterados e aprimorados juntamente aos recursos de TI e seus ativos de SI para adequação à SOX passam a impactar em resultados financeiros, não obstante, os controles que outrora eram apenas uma visão da TI passam agora ser uma obrigação legal e de grande visibilidade à toda alta direção, podemos dizer que a TI se beneficiaria com a adequação organizacional para atender a SOX?

Segundo Oliveira e Linhares (2006, p.1) a lei SOX “sacode as grandes empresas americanas e estrangeiras e movimenta milhões de dólares para que elas possam se enquadrar às regras que visam à proteção dos acionistas minoritários do mercado de capitais”.

PENHA et alli (2006, p.1-2), destaca que a TI é o setor cujo grandes investimentos usualmente são despendidos e também que o processo de adequação à SOX exige adicionalmente aos montantes financeiros investidos, o apoio ostensivo dos gestores da organização.

> A adequação à Lei Sarbanes-Oxley apresenta algumas dificuldades. Este processo, por si só, requer investimentos iniciais para efetuar-se o diagnóstico dos controles internos existentes, e a identificação dos pontos falhos que precisam ser trabalhados. Como uma parte substantiva do sistema de controles internos está embasada nos sistemas de informação, os quais devem estar desenhados e construídos com o estabelecimento de pontos de controle interno, os recursos a serem empregados para a sua adaptação podem ser vultosos. Além disso, a empresa precisa estar consciente da necessidade de mudança. Os gestores devem assumir o seu papel de incentivadores deste processo, conscientizando a todos que a mudança é necessária e obrigatória, para que todos na empresa possam vislumbrar um futuro melhor.

2.5 AUDITORIAS SOX EM SEGURANÇA DA INFORMAÇÃO

As auditorias aplicadas às organizações de capital aberto que publicam valores na bolsa de Nova Iorque, têm como principal objetivo a transparência na gestão financeira das organizações e que impactam diretamente no valor monetário dos títulos ou papeis por elas negociados. Tais objetivos precisam ser medidos por meio de mecanismos de auditoria e segurança das informações financeiras, é neste sentido que a SI possui um papel fundamental em todo processo de implantação e manutenção de uma organização na SOX.

SILVA Claudiano, reforça a necessidade de adequação da SI à lei SOX.

> É necessário que haja adequação ao conteúdo da Sarbanes-Oxley em toda a cadeia de comunicação da empresa, principalmente nos recursos concernentes a informações financeiras. Como exemplo os Sistemas de ERP, aplicativos contábeis, sistemas de CRM, banco de dados e armazenamento de informações precisam estar em sintonia com as regras adotadas na legislação, buscar integração entre sistemas. Políticas de Segurança da Informação adotadas devem estar em conformidade com a Lei.

A auditoria então se divide em dois grandes grupos, com equipes distintas de trabalho, entretanto sinergicamente. Uma equipe realiza o processo de teste dos controles financeiros e a outra equipe fica responsável pelos testes denominados *Information Technology General Controls* (ITGC). Os testes ITGC tem foco na SI e são validados de acordo com a Matriz SOX ITGC de cada organização. Esta Matriz é confeccionada em um primeiro momento por um profissional com alto conhecimento da SOX em conjunto a um time de TI, além do time de SI e o time jurídico que validará as questões legais.

Posteriormente esta matriz deve ser mantida com base nas evoluções tecnológicas e organizativas, bem como com base nos resultados das auditorias apresentadas e melhorias ou correções indicadas por estas auditorias e seus agentes.

2.6 AUDITORIAS SOX ITGC IND-FORCE BRASIL

As auditorias SOX ITGC iniciaram efetivamente no ano de 2014 na Ind-Force Brasil, sendo que em 2013 foi realizada uma auditoria "pré SOX" para mapear o nível de maturidade dos controles e planos de ação a serem realizados na adequação e aprimoramento da SI.

A matriz de controles ITGC SOX Ind-Force Brasil é composta por 26 (vinte e seis) itens de controle, divididos em 08 (oito) blocos, conforme abaixo:

- Aquisição e Manutenção de Software
- Gestão de Mudanças
- Implementação e Validação de Soluções
- Garantir a Segurança dos Sistemas
- Gestão de Problemas e Incidentes
- Gestão de Configuração
- Gestão de Dados
- Gestão de Operações

Para uma visualização completa da matriz de controles ITGC, utilizar a seção ANEXO através do item **ANEXO A** – Descrição dos Controles ITGC SOX da organização Ind-Force, contendo todos os 26 (vinte e seis) controles, dividida em seus 08 (oito) blocos e suas respectivas descrições.

Entre os meses de fevereiro a abril de cada ano, um trabalho em conjunto com a organização independente que efetivará a auditoria é realizado em conjunto com a Ind-Force Brasil, a fim de definir as aplicações que serão escopo SOX no ano corrente. Este trabalho é realizado com base em um questionário, que poderá ser observado na sessão ANEXO, através do item **ANEXO B** – Questionário para definição das aplicações escopo da auditoria ITGC SOX, onde todos os processos que impactam direta ou indiretamente nos resultados financeiros são desmembrados e então indicadas às aplicações que suportam cada um destes micro processos.

Uma vez definido o escopo, os 08(oito) blocos de controle são auditados para cada uma das aplicações identificadas como escopo para o ano corrente.

2.6.1 Ordem de auditorias realizadas na Ind-Force Brasil Anualmente

2.6.1.1 *Internal audit*

Uma vez que o escopo SOX ITGC do ano corrente é definido, 01 (um) ou 02 (dois) dos sistemas são eleitos para a realização parcial, aproximadamente 10 (dez) entre os 26 (vinte e seis) itens de controle são eleitos, para execução da auditoria interna no primeiro semestre de cada ano.

Para eleição dos sistemas a serem auditados, são considerados aqueles que mais terão impacto na auditoria estatutária, ou seja, os sistemas que são mais amplamente utilizados para suportar os processos de negócio da organização, no tocante aos processos de impacto financeiro.

Esta auditoria visa atender tanto testes de TI, quando testes de processos de negócio contidos nos controles internos da organização, sob a ótica financeira.

2.6.1.2 *Audit of management*

Para um teste mais abrangente e profundo frente aos controles de TI e SI, no início do segundo semestre de cada ano uma empresa autorizada pelo *Public Company Accounting Oversight Board* (PCAOB) é contratada para realização de uma auditoria nos sistemas definidos previamente como escopo SOX ITGC, e que são geridos diretamente pela Ind-Force Brasil.

A auditoria de gestão (*Audit of Management*), é realizada usualmente entre os meses de junho e agosto do ano corrente e precedem a auditoria ITGC oficial SOX, sendo valida como uma auditoria também interna.

2.6.1.3 *Information Technology General Control*

Entre os meses de setembro e novembro do mês corrente, inicia-se enfim a auditoria oficial SOX ITGC, que audita todos os 26 (vinte e seis) itens de controle em seus 08 (oito) blocos para todas as aplicações do escopo SOX ITGC do ano corrente, independente da aplicação ser ou não gerida diretamente pela Ind-Force Brasil.

Os resultados obtidos pela auditoria de gestão, que é realizada preliminarmente, são utilizados como parte da auditoria, sendo que alguns dos controles testados e seus respectivos resultados são utilizados em uma estratégia de confiança, denominada *Reliance Strategy ITGC Tests*.

2.6.1.4 *Roll foward test*

A empresa responsável pela *Audit of Management*, retorna a campo, ou seja, localmente na Ind-Force Brasil no início do mês de dezembro do ano contábil para realizar seu último teste, denominado *Roll Foward Test*.

Nesta etapa, um teste com menor abrangência é refeito para cada um dos 26 (vinte e seis) itens de teste, contemplando uma nova massa de dados gerada após a data final da *Audit of Management*, ou seja, após sua conclusão que ocorre usualmente no mês de agosto.

Adicionalmente, itens que eventualmente receberam falha em seu resultado anterior, têm a implementação do plano de ação validada. Um novo resultado é disponibilizado junto à Ind-Force e compartilhado com a organização responsável pela auditoria ITGC oficial SOX.

2.6.1.5 *Final result*

No início de janeiro do ano sequente, a empresa responsável pela auditoria ITGC SOX, divulga o resultado final oficial observado e este é reportado diretamente ao PCAOB, que executa sua análise independente. Os resultados finais apresentados na auditoria ITGC SOX, rebem para cada um dos itens de controle, um dos valores descritos a seguir:

a) Avaliado sem falhas - Este valor no resultado final indica que o teste executado para o controle foi bem-sucedido e assim sendo, não foram observadas falhas de nenhuma natureza. Resultados que apresentam este valor, podem ainda receber uma observação que sugere uma melhoria evolutiva no controle, sem que, no entanto, se tenha identificado falhas no controle corrente;

b) Avaliado com falha imaterial - Este valor no resultado final indica que uma ou mais falhas foram observadas no controle sob avaliação, entretanto são falhas de processo, pessoas e (ou) sistêmicas e não contemplam ações dolosas que objetivam fraudar, obter ganho ilícito ou apropriar-se indevidamente de informações, títulos ou valores da organização;

c) Avaliado com falha material - Este valor no resultado final indica que uma ação dolosa e (ou) fraudulenta foi identificada durante os testes realizados e assim sendo, uma análise de cunho criminal deve ser estabelecida na organização de forma transparente junto ao PCAOB, no objetivo de identificar os agentes e responsabiliza-los, além de definir um amplo plano de adequação para garantir a governança coorporativa.

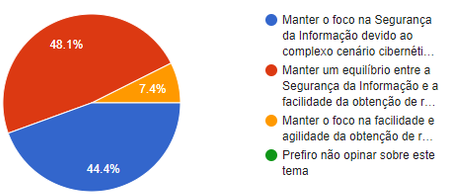
3. PESQUISA APLICADA À ORGANIZAÇÃO IND-FORCE BRASIL E RESULTADOS APRESENTADOS

A fim de aumentar a confiabilidade das informações aqui apresentadas, foi utilizada como instrumento de coleta de dados a aplicação de um questionário composto de questões fechadas e abertas. A pesquisa se ateve aos colaboradores da Ind-Force Brasil e ao público alvo composto de gerentes, coordenadores e analistas da área de TI e usuários chave das áreas de negócios. Adicionalmente, a pesquisa contou com a consulta à documentação visando apresentar os resultados de auditorias de SI dos últimos 04 (quatro) anos, ou seja, desde instituído o novo grupo de empresas Ind-Force, bem como as práticas evolucionarias de controles adotados como resultante das auditorias independentes e internas realizadas.

A pesquisa obteve respostas de 27 (vinte e sete) participantes com atuação em 18 (dezoito) diferentes áreas da organização, divididos por 05 (cinco) diferentes faixas etárias e 05 (cinco) faixas temporais de permanência na organização. Adicionalmente foram observados um total de 63 % de homens e 37 % de mulheres entre os participantes da pesquisa aqui realizada. Os dados completos coletados durante a pesquisa de campo, poderão ser observados na seção APÊNDICE, através do item APÊNDICE B – Questionário aplicado na pesquisa de campo realizada e respectivas respostas dos participantes

Na sequência deste artigo serão apresentados 09 (nove) gráficos resultantes da pesquisa aplicada aos colaboradores da Ind-Force Brasil, que representam os principais indicadores obtidos. Adicionalmente, imediatamente após a exibição gráfica dos indicadores, um resumo explicativo será descrito para um melhor entendimento:

Gráfico 1 - Percepção frente a implementação de processos de SI na organização

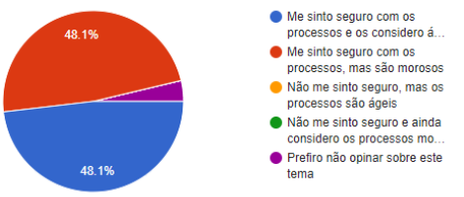


Fonte: Própria (2018)

Foi notado que 92,5 % dos participantes entendem a necessidade de se aplicar processos que garantam uma maior segurança na organização, sendo que deste montante 48,1 % possui uma visão mais moderada, ou seja, visualizam a necessidade de se manter um equilíbrio entre os processos de segurança e facilidade na obtenção dos recursos de TI, enquanto 44,4 %

consideram mais importante a segurança do que a facilidade na obtenção dos recursos TI, maximizando a segurança e reduzindo a materialização de riscos.

Gráfico 2 - Percepção geral da população pesquisada, quanto aos processos de TI

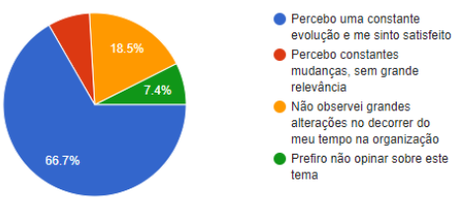


Fonte: Própria (2018)

Adicionalmente, foi notória a sensação dos usuários que se utilizam da TI quanto ao seu sentimento de segurança em relação à utilização de recursos informáticos devido aos processos, treinamentos, fluxos e ferramentas implementadas e constantemente sob evolução. Isto ficou claro pela expressiva representatividade de 96,2 % dos participantes na pesquisa.

No entanto houve uma divisão de opiniões no tocante a satisfação dos usuários quanto ao tempo de resposta frente aos processos existentes para TI.

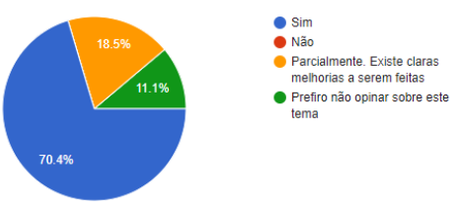
Gráfico 3 - Percepção sobre a evolução qualitativa dos processos de TI



Fonte: Própria (2018)

Ainda que não seja uma unanimidade, 66,7 % dos usuários pesquisados admitiram que a organização claramente está em constante evolução tecnológica e processual, com o objetivo de se obter maior segurança da informação em seus processos e sistemas.

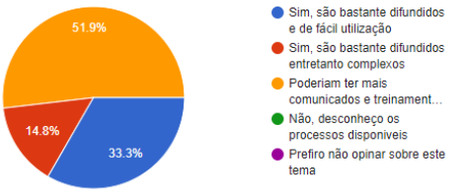
Gráfico 4 - Sensação de segurança para com as informações sensíveis da organização



Fonte: Própria (2018)

Foi demostrado por 70,4 % dos pesquisados, a sensação de segurança para com os dados sensíveis da organização, como protótipos, dados financeiros e dados pessoais. Por outro lado, uma fatia considerável da população pesquisada apontou a percepção de oportunidades de melhorias a serem exploradas pela TI na segurança dos dados sensíveis da organização.

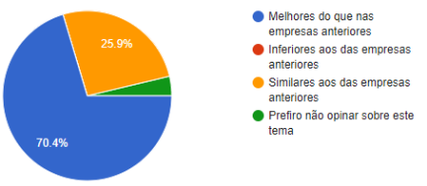
Gráfico 5 - Conhecimento dos usuários quanto aos meios disponibilizados pela organização por sua TI, para solicitar demandas e (ou) reportar falhas.



Fonte: Própria (2018)

Acerca dos meios disponibilizados pela TI para que os usuários registrem suas demandas e(ou) reportem falhas, foram considerados por 51,9 % dos pesquisados a possibilidade de melhorias, enquanto 48,1 % consideraram que os meios são bastante difundidos. Entretanto destes 48,1 %, 14,8 % consideram que mesmo com a divulgação adequada, os meios não são amigáveis o suficiente para o usuário final.

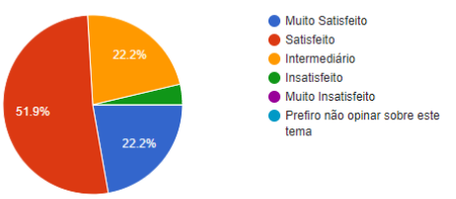
Gráfico 6 - Base comparativa dos usuários em relação a sua experiência de mercado



Fonte: Própria (2018)

Dos usuários pesquisados, 70,4 % consideraram os processos da organização objeto da pesquisa aqui realizada, superiores aos das organizações em que os mesmos atuaram anteriormente, quando observada a capacidade de promover a segurança das informações.

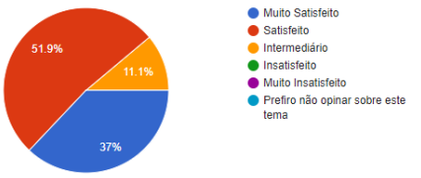
Gráfico 7 - Percepção em relação ao tempo de resposta para o atendimento na Gestão de Acessos.



Fonte: Própria (2018)

A maioria dos usuários pesquisados consideraram o tempo de resposta para os processos de gestão de acessos, adequado quando se expressaram através da pesquisa como Satisfeitos ou Muito Satisfeitos, totalizando 74,1 % do universo pesquisado.

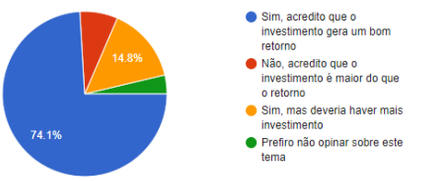
Gráfico 8 - Percepção em relação à qualidade do atendimento na Gestão de Acessos



Fonte: Própria (2018)

A maioria dos usuários pesquisados consideraram a qualidade na resposta para os processos de gestão de acessos adequado quando se expressaram através da pesquisa como Satisfeitos ou Muito Satisfeitos, totalizando 88,9 % do universo pesquisado.

Gráfico 9 - Conscientização quanto ao investimento na obtenção de maior segurança das informações



Fonte: Própria (2018)

Ficou notória através da pesquisa a conscientização dos usuários pesquisados quanto à necessidade da organização em investir recursos financeiros e humanos na obtenção de mecanismos que aumentem a segurança da informação, sendo que 74,1 % se posicionaram como satisfeitos com o alto investimento aplicado nos últimos anos para a finalidade de se obter segurança da informação e outros 14,8 % indicaram que concordam com o investimento e ainda sugerem que estes sejam maiores.

3.2 RELATORIOS DE AUDITORIAS ITGC SOX 2014, 2015, 2016 e 2017

Devido ao sigilo do detalhamento existente nos processos de auditoria e em seus resultados, a Ind-Force concordou em fornecer o resultado macro das auditorias SOX ITGC realizadas nos últimos 04 (quatro) anos em seu escopo América Latina.

O quadro 1 – Evolução SOX ITGC LATAM Ind-Force Group, detalha cronologicamente os sistemas auditados pela entidade de auditoria independente e seus respectivos resultados dos últimos 04 (quatro) anos:

Quadro 1 - Evolução SOX ITGC LATAM Ind-Force Group

EVOLUTIVAS SOX ITGC LATAM - INDFORCE GROUP

	2014	2015	2016	2017
Nº de Testes Realizados	260	312	390	416
Nº de Aplicações Testadas	10	12	15	16
Nº de Testes Falhos	142	31	4	0
Nº de Action Plans Realizados no Ano Contábil	137	27	4	0
Nº de Segestões de Melhorias	35	10	2	1

Fonte: Ind-Force Brasil (2018)

4 SOLUÇÃO DA PROBLEMATIZAÇÃO

Nesta etapa do artigo é possível obter uma solução com base nos resultados extraídos da pesquisa pura de caráter exploratório realizada e os resultados práticos obtidos nas auditorias ITGC SOX.

Através da pesquisa foi possível confirmar que as auditorias que certificam à organização para publicar títulos na bolsa de valores Norte Americana, ainda que por força maior em uma visão simplista, traz consigo melhorias latentes na segurança da informação, haja vista que por força de lei a alta direção se vê impelida a exigir tal evolução, se tornando patrocinadora na implantação e evolução da governança, tanto coorporativa quanto da TI e da SI.

Uma vez que o nível da segurança da informação é elevado, a organização ganha maior confiabilidade no mercado, bem como evita os custos diretos e indiretos da perda ou obtenção indevida de informações sensíveis ou de parada em serviços ou aplicações informáticas por um período comprovadamente prejudicial aos negócios da organização, gerando assim uma eficiência intangível no campo das finanças.

Os processos advindos de uma maior governança na TI e na SI, a princípio gera desconforto aos usuários da TI, entretanto com o aumento do seu nível de maturidade e divulgação apropriada, faz com que a TI funcione de forma mais ágil, eficaz e segura. Por outro lado, usuários de áreas não administrativas, demostram maior dificuldade na assimilação dos processos e fluxos, sendo que estas áreas requerem um maior investimento em treinamento e planejamento, também em aplicar processos mais simplificados sem que, no entanto, a segurança da informação seja prejudicada.

Identificamos assim que as exigências da lei SOX em uma organização multinacional do ramo automotivo, demanda um grande esforço financeiro e humano, envolvimento intensivo da alta direção, treinamentos e divulgação que promovam a conscientização e aceitação das mudanças inerentes às adequações que serão necessárias, além de pessoal qualificado dedicado na implementação de processos de governança que promovam controle e segurança das informações. Por outro lado, uma vez que tais requisitos sejam cumpridos, a organização tende a se beneficiar substancialmente com maior controle, uniformidade, eliminação de perdas, processos bem definidos, aumento de valor intangível da organização frente ao mercado e maior segurança do bem de alto valor organizacional em todas as suas esferas, a saber suas informações.

5 CONCLUSÃO

Ao se considerar os percentuais avaliados na pesquisa fica explicita no escopo deste artigo, que há uma percepção da grande maioria dos usuários da organização, objeto deste estudo, quanto a necessidade de investimento em SI bem como da necessidade eminente de se obter e aplicar esforços na TI em implementação e evolução continua dos processos que visam salvaguardar os ativos de informação organizacionais, em especial àquelas que possuem maior sensibilidade, e assim são classificados.

Também é notória a percepção de evolução dos processos de TI que visam à SI nos últimos anos e que a qualidade e tempo de resposta da TI para as demandas e incidentes registrados tem evoluído exponencialmente a medida que o processo ganha maturidade. Por outro lado, foi identificado pela pesquisa que apesar dos esforços em se divulgar a consciência segura, ainda existe uma lacuna a ser preenchida no campo da capacitação geral dos usuários e na obtenção de processos mais simplificados no tocante à interface com o usuário final, aumentando assim a experiência qualitativa dos usuários e fazendo com que estes evoluam de usuários finais da TI para parceiros da TI.

Ao se observar com ótica especifica sobre a lei SOX, foi demostrado através das respostas obtidas na pesquisa, um nível intermediário de conhecimento dos usuários pesquisados sobre o conceito básico da lei e consequentemente da importância de se aplicar esforços contínuos para manter controles robustos na manutenção da segurança da informação a fim de estar em conformidade com as exigências da lei.

Constata-se então que no ano de 2014 quando a fusão das empresas Bulldozer, NH-Force, Long-Way, Hot-Gear e PT-Goals haviam formado recentemente o grupo Ind-Force, os resultados finais da auditoria SOX ITGC apresentaram um número consideravelmente alto de testes falhos, sendo necessário um esforço muito alto de investimento financeiro e de recursos humanos na aplicação de planos de ação para correção e evolução dos processos de gestão da TI. É notório também, que nos anos posteriores, apesar do número de sistemas e consequentemente de testes terem aumentado, o número de falhas observadas no resultado final das auditorias SOX ITGC foram inversamente proporcionais, demonstrando aumento do grau de maturidade da governança da TI, SI nos processos aplicados.

Como resultante, o investimento financeiro foi reduzindo gradativamente e o resultado final obtendo melhoras significativas, evento este claramente percebidas pelos autores envolvidos desde à alta direção, até os usuários finais da TI.

SARBANES-OXLEY AUDIT APPLIED AT THE IND-FORCE GROUP. IMPACTS AND BENEFITS AROUND THE INFORMATION SECURITY CONTROLS IN BRAZIL

Abstract: This scientific article was developed in order to observe the positive and negative impacts to adapting of a multinational organization of the automotive industry to the requirements of the Sarbanes-Oxley Act, especially in complying with the requirements of its 404 (four hundred four) session, which refers to the assessment determination of internal controls and procedures for the issuance of financial reports. These impacts were observed through the results of a survey carried out with the users of the impacted areas, according to the master plan of procedural adaptations that cover the organization's internal controls, the information technology (IT) and information security area (IS), as well as from the results obtained in the audits carried out in the area of IT and IS against their respective controls narrated in the matrix of IT controls and which were considered support instruments in obtaining the results and information necessary for production of this article, which focused on demonstrating the set of efforts applied by the organization and its specific results of the areas mentioned above.

Keywords: Information Security. Sarbanes-Oxley. Audit

REFERÊNCIAS

BRESSAN, Flavio. O MÉTODO DO ESTUDO DE CASO. Artigo < http://www.fe-cap.br/adm_online/art11/flavio.htm>. Acesso realizado em: 06 Nov.2016

ESTATOS UNIDOS**. Sarbanes-Oxley Act of 2002**. Disponível em <https://www.sec.gov/about/laws.shtml#sox2002>. Acesso realizado em 06 Nov.2016, tradução nossa.

ESTATOS UNIDOS**. Holmstrom, B. and Kaplan**, S.N. The State of US corporate governance: whatís right and whatís wrong? Journal of Applied Corporate Finance, 15 Mar, 2003.

ESTATOS UNIDOS**. U.S. SECURITY AND EXCHANGE COMMISSION.** Disponível em < https://www.sec.gov/>. Acesso realizado em: 16 Out.2016.

LEI SARBANES-OXLEY. Em: WIKIPÉDIA, a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Lei_Sarbanes-xley&oldid=47044990>. Acesso realizado em: 25 Out.2016

OLIVEIRA, Marcelle; LINHARES, Juliana. A Implantação de Controle Interno Adequado às Exigências da Lei Sarbanes-Oxley em Empresas Brasileiras – Um Estudo de Caso. In: Congresso USP Controladoria e Contabilidade, Jun, 2006. Disponível em: < http://www.geocities.ws/wolneyunb/arquivos/textoresenha22007.pdf>. Acesso em: 12 Nov.2016

PINHEIRO, José Maurício Santos. Sarbanes-Oxley e o Impacto Sobre a Governança de TI. Artigo <http://www.projetoderedes.com.br/artigos/artigo_sarbanes_oxley.php>. Acesso realizado em: 22 Out. 2016.

PORTAL DE AUDITORIA. Introdução à lei Sarbanes-Oxley. Disponível em :http://www.portaldeauditoria.com.br/auditoria-interna/Introducao-a-lei-Sarbanes-Oxley-SOx.asp>. Acessado em 04 Nov.2016

TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO. SOX, Lei Sarbanes Oxley, Disponivel em <https://claudianojs.wordpress.com/2011/09/21/sox-lei-sarbanes-oxley/>. Acessado em 03 Mar.2017

VENTURA, Luciano. GOVERNANÇA CORPORATIVA – A EXPERIÊNCIA BRASILEIRA, 2016

APÊNDICE A - Perguntas aplicadas à pesquisa de campo junto à 27 (vinte e sete) usuários da TI na organização Ind-Force.

Questionário TCC - Controles SOX

Prezado (a),
O questionário abaixo faz parte de um estudo de caso referente ao TCC (Trabalho de Conclusão de Curso) de Pós-Graduação em Gerenciamento da Segurança da Informação da Universidade UNISUL.
Conto com o seu apoio para responder as perguntas elencadas que serão base para uma análise sobre a percepção dos atores envolvidos de forma direta ou indireta, no processo de certificação e manutenção da lei SOX (Sarbanes Oxley) na organização, no que tange os controles de ICT (Information and Communication Technology) com foco em Segurança da Informação.
O questionário é formado de 10 questões fechadas de múltipla escolha e outras 5 questões abertas, para livre descrição de sua resposta.
O objetivo da pesquisa desenvolvida neste TCC é apresentar as vantagens e desvantagens, dificuldades e facilidades percebidas no dia a dia pelos participantes das áreas que se utilizam dos processos de ICT, assim como pelo próprio ICT, frente a implantação de controles aplicados para adequar à organização às exigências da lei Norte Americana SOX, em uma organização multinacional do ramo automotivo, com escopo delimitado nas filiais do Brasil.

Desde já gostaria de agradecer por sua colaboração ao responder o questionário proposto:

* Required

Dados Pessoais

1. **FAIXA ETÁRIA** *
Mark only one oval.

- ◯ Entre 18 e 25 anos
- ◯ Entre 26 e 35 anos
- ◯ Entre 36 e 50 anos
- ◯ Acima de 50 anos

3. **Qual sua área de atuação na organização** *

_____

4. **Qual a sua função na organização** *

_____

5. **Quanto tempo você trabalha nesta organização** *
Mark only one oval.

- ◯ Menos de 1 ano
- ◯ Entre 1 e 3 anos
- ◯ Entre 4 e 7 anos
- ◯ Entre 8 e 12 anos
- ◯ Acima de 12 anos

QUESTÕES DE MÚLTIPLA ESCOLHA

Assinale a alternativa que mais se aproxima de sua percepção aos pontos levantados.
Lembre-se de que se trata de sua visão pessoal, logo não há respostas certas ou erradas.

6. **Qual a sua percepção sobre a necessidade de se manter processos que focam na Segurança das Informações em relação ao cenário corporativo de forma geral?** *
Mark only one oval.

- ◯ Manter o foco na Segurança da Informação devido ao complexo cenário cibernético e o tráfego de dados da organização na Web
- ◯ Manter um equilíbrio entre a Segurança da Informação e a facilidade da obtenção de recursos ICT
- ◯ Manter o foco na facilidade e agilidade da obtenção de recursos ICT, mesmo que exista um risco na eliminação de passos atualmente exigidos
- ◯ Prefiro não opinar sobre este tema

7. **Qual a sua percepção geral sobre os processos de ICT da organização, no tocante à segurança da informação?** *
Mark only one oval.

- ◯ Me sinto seguro com os processos e os considero ágeis
- ◯ Me sinto seguro com os processos, mas são morosos
- ◯ Não me sinto seguro, mas os processos são ágeis
- ◯ Não me sinto seguro e ainda considero os processos morosos
- ◯ Prefiro não opinar sobre este tema

8. **Qual a sua percepção em relação à evolução dos processos de ICT e os controle da segurança da informação?** *
Mark only one oval.

- ◯ Percebo uma constante evolução e me sinto satisfeito
- ◯ Percebo constantes mudanças, sem grande relevância
- ◯ Não observei grandes alterações no decorrer do meu tempo na organização
- ◯ Prefiro não opinar sobre este tema

9. **Você considera que as informações sensíveis da organização estão seguras?** *
Mark only one oval.

- ◯ Sim
- ◯ Não
- ◯ Parcialmente. Existe claras melhorias a serem feitas
- ◯ Prefiro não opinar sobre este tema

10. **Você conhece bem os meios disponibilizados pela organização para se solicitar recursos de ICT como acessos ou mudanças em sistemas?** *
Mark only one oval.

- ◯ Sim, são bastante difundidos e de fácil utilização
- ◯ Sim, são bastante difundidos entretanto complexos
- ◯ Poderiam ter mais comunicados e treinamentos para utilização
- ◯ Não, desconheço os processos disponíveis
- ◯ Prefiro não opinar sobre este tema

11. **Em relação às suas experiências profissionais anteriores, você considera os processos de segurança da informação da atual organização:** *
Mark only one oval.

- ◯ Melhores do que nas empresas anteriores
- ◯ Inferiores aos das empresas anteriores
- ◯ Similares aos das empresas anteriores
- ◯ Prefiro não opinar sobre este tema

12. **Qual a sua percepção em relação ao TEMPO de atendimento para criação\alteração de uma conta de usuário em aplicativos gerenciados pelo time de Segurança da Informação:** *
Mark only one oval.

- ◯ Muito Satisfeito
- ◯ Satisfeito
- ◯ Intermediário
- ◯ Insatisfeito
- ◯ Muito Insatisfeito
- ◯ Prefiro não opinar sobre este tema

13. **Qual a sua percepção em relação à QUALIDADE do atendimento para criação\modificação de uma conta de usuários em aplicativos gerenciados pelo time de Segurança da Informação:** *
Mark only one oval.

- ◯ Muito Satisfeito
- ◯ Satisfeito
- ◯ Intermediário
- ◯ Insatisfeito
- ◯ Muito Insatisfeito
- ◯ Prefiro não opinar sobre este tema

14. **Você considera uma boa estratégia da organização investir em controles de ICT e Segurança da Informação para atender exigências SOX?** *
Mark only one oval.

- ◯ Sim, acredito que o investimento gera um bom retorno
- ◯ Não, acredito que o investimento é maior do que o retorno
- ◯ Sim, mas deveria haver mais investimento
- ◯ Prefiro não opinar sobre este tema

15. **Você já sofreu algum ataque cibernético com alguma consequência?** *
Check all that apply.

- ☐ Nunca
- ☐ Sim, utilizando um computador pessoal
- ☐ Sim, utilizando um dispositivo móvel pessoal
- ☐ Sim, utilizando um dispositivo corporativo
- ☐ Não sei responder

Questões Abertas

Descreva com suas palavras, sua visão sobre os temas propostos.
Lembre-se de que se trata de sua visão pessoal, logo não há respostas certas ou erradas.

16. **Você concorda com a afirmativa: "A implementação de governança e metodologias para os processos de Segurança da Informação, apesar de causar certos transtornos ao usuário durando o período de adaptação, se mostra mais ágil, seguro e simples quando alcança seu grau intermediário de maturidade". Justifique sua resposta.** *

17. **O que você sabe sobre a lei SOX (Sarbanes Oxley) e qual a relação você sugere entre a SOX e a Segurança da Informação de uma organização?** *

18. **Em sua percepção em seu período como funcionário desta organização, os processos de ICT ficaram mais ou menos seguros? Qual a relação você visualiza entre os processos exigidos para utilização e suporte de ICT e sua resposta quanto ao nível de segurança da informação?** *

19. **Você está satisfeito com os processos atualmente aplicados para solicitação de serviços de ICT (Acessos em Aplicações, Alteração em Sistemas, Acesso à Internet, Restauração de dados perdidos, entre outros)? Justifique sua resposta.** *

20. **Se você tivesse a oportunidade de alterar um processo atualmente existente para ICT, qual seria a alteração realizada?** *

Fonte: Própria (2018)

APÊNDICE B – Questionário aplicado na pesquisa de campo realizada e respectivas respostas dos participantes

Dados Pessoais

FAIXA ETÁRIA	SEXO	Qual sua área de atuação na organização	Qual a sua função na organização	Quanto tempo você trabalha nesta organização
Entre 36 e 50 anos	Masculino	ICT	Analista de Segurança da Informação	Entre 4 e 7 anos
Entre 26 e 35 anos	Masculino	Information and Comunication Technology	Coordenador de Infraestrutura	Entre 4 e 7 anos
Entre 26 e 35 anos	Masculino	ICT COMM & PS	Analista Sistemas Sr	Entre 4 e 7 anos
Entre 18 e 25 anos	Feminino	ICT	Estagiário	Entre 1 e 3 anos
Entre 36 e 50 anos	Feminino	PMO	Coordenador de Projetos	Entre 1 e 3 anos
Entre 26 e 35 anos	Masculino	Controles Internos	Coordenador	Entre 1 e 3 anos
Entre 36 e 50 anos	Feminino	Processos e sistemas logisticos	Analista	Acima de 12 anos
Entre 26 e 35 anos	Masculino	ICT - Information and Communication Technologies	Analista de Sistemas Senior	Entre 8 e 12 anos
Entre 18 e 25 anos	Feminino	Supply Chain	Estagiária	Menos de 1 ano
Entre 26 e 35 anos	Masculino	Compras	Especialista de Sistemas & Métodos de Compras	Entre 4 e 7 anos
Entre 18 e 25 anos	Feminino	Compras	Comprador de materiais indiretos	Entre 1 e 3 anos
Acima de 50 anos	Masculino	Global Logistics	Coordenador de Logistica	Acima de 12 anos
Entre 26 e 35 anos	Feminino	WCM - World Class Manufacturing	Coordenador de Processos	Entre 4 e 7 anos
Entre 18 e 25 anos	Masculino	Compras	Comprador Jr.	Entre 1 e 3 anos
Entre 36 e 50 anos	Masculino	Comercial	Coordenador de Vendas	Entre 4 e 7 anos
Acima de 50 anos	Feminino	Desenvolvimento do Produto	Engenheira Sênior	Entre 8 e 12 anos
Entre 26 e 35 anos	Masculino	Recursos Humanos	Analista de RH Pleno	Entre 1 e 3 anos
Entre 18 e 25 anos	Feminino	Controladoria	Estagiaria	Entre 1 e 3 anos
Entre 36 e 50 anos	Masculino	Expedição	Coordenador	Acima de 12 anos
Entre 36 e 50 anos	Masculino	Fiscal	Analista Fiscal	Entre 8 e 12 anos
Entre 26 e 35 anos	Masculino	Finance	Analista financeiro pleno.	Entre 1 e 3 anos
Entre 36 e 50 anos	Masculino	Recebimento	Analista Sênior	Entre 8 e 12 anos
Entre 18 e 25 anos	Masculino	Product Development	Trainee	Menos de 1 ano
Entre 26 e 35 anos	Feminino	RH	Analista de Comunicação Pleno	Entre 1 e 3 anos
Entre 26 e 35 anos	Masculino	Marketing	Analista de Marketing Pleno	Entre 1 e 3 anos
Entre 36 e 50 anos	Feminino	Controladoria Industrial	Controller	Entre 8 e 12 anos
Entre 26 e 35 anos	Masculino	Manutenção	Coordenador de Manutenção	Entre 4 e 7 anos

Questões de Múltipla Escolha

RESULTADO DA PESQUISA - QUESTÕES DE MULTIPLA ESCOLHA			
Você conhece bem os meios disponibilizados pela organização para se solicitar recursos de ICT como acessos ou mudanças em sistemas?	**Nº de Respostas**	**Em relação às suas experiências profissionais anteriores, você considera os processos de segurança da informação da atual organização:**	**Nº de Respostas**
Poderiam ter mais comunicados e treinamentos para utilização	14	Melhores do que nas empresas anteriores	19
Sim, são bastante difundidos e de fácil utilização	9	Prefiro não opinar sobre este tema	1
Sim, são bastante difundidos entretanto complexos	4	Similares aos das empresas anteriores	7
Qual a sua percepção geral sobre os processos de ICT da organização, no tocante à segurança da informação?	**Nº de Respostas**	**Qual a sua percepção em relação ao TEMPO de atendimento para criação\alteração de uma conta de usuário em aplicativos gerenciados pelo time de Segurança da Informação:**	**Nº de Respostas**
Me sinto seguro com os processos e os considero ágeis	13	Insatisfeito	1
Me sinto seguro com os processos, mas são morosos	13	Intermediário	6
Prefiro não opinar sobre este tema	1	Muito Satisfeito	6
		Satisfeito	14
Qual a sua percepção em relação à evolução dos processos de ICT e os controle da segurança da informação?	**Nº de Respostas**	**Qual a sua percepção em relação à QUALIDADE do atendimento para criação\modificação de uma conta de usuários em aplicativos gerenciados pelo time de Segurança da Informação:**	**Nº de Respostas**
Não observei grandes alterações no decorrer do meu tempo na organização	5	Intermediário	3
Percebo constantes mudanças, sem grande relevância	2	Muito Satisfeito	10
Percebo uma constante evolução e me sinto satisfeito	18	Satisfeito	14
Prefiro não opinar sobre este tema	2		
Você considera que as informações sensíveis da organização estão seguras?	**Nº de marcações para a opção**	**Você considera uma boa estratégia da organização investir em controles de ICT e Segurança da Informação para atender exigências SOX?**	**Nº de marcações para a opção**
Parcialmente. Existe claras melhorias a serem feitas	5	Não, acredito que o investimento é maior do que o retorno	2
Prefiro não opinar sobre este tema	3	Prefiro não opinar sobre este tema	1
Sim	19	Sim, acredito que o investimento gera um bom retorno	20
		Sim, mas deveria haver mais investimento	4
Você já sofreu algum ataque cibernético com alguma consequência?	**Nº de Respostas**	**Qual a sua percepção sobre a necessidade de se manter processos que focam na Segurança das Informações em relação ao cenário corporativo de forma geral?**	**Nº de Respostas**
Sim, utilizando um computador pessoal, Sim, utilizando um dispositivo corporativo	3	Manter o foco na facilidade e agilidade da obtenção de recursos ICT, mesmo que exista um risco na eliminação de passos atualmente exigidos	2
Sim, utilizando um computador pessoal, Sim, utilizando um dispositivo móvel pessoal	1	Manter o foco na Segurança da Informação devido ao complexo cenário cibernético e o tráfego de dados da organização na Web	12
Sim, utilizando um dispositivo corporativo	1	Manter um equilíbrio entre a Segurança da Informação e a facilidade da obtenção de recursos ICT	13
Sim, utilizando um dispositivo móvel pessoal	1		
Sim, utilizando um dispositivo pessoal, Sim, utilizando um dispositivo pessoal	1		
Não sei responder	3		
Nunca	11		
Sim, utilizando meu comutador coorporativo	1		
Sim, utilizando um computador pessoal	5		

Questões Abertas

Você concorda com a afirmativa: “A implementação de governança e metodologias para os processos de Segurança da Informação, apesar de causar certos transtornos ao usuário durando o período de adaptação, se mostra mais ágil, seguro e simples quando alcança seu grau intermediário de maturidade”. Justifique sua resposta.
Certamente! Assim como podemos observar no ciclo PDCA, todo processo é planejado, executado, validado e melhorado!
Certamente. Está foi a percepção quanto aos novos processos ICT implementados nos últimos anos.
Concordo com a afirmativa, quando os usuarios tem mais tempo de adaptação mais "simples" fica.
Concordo parcialmente. A agilidade deve levar em conta outros quesitos não mencionados.
Concordo pois é natural que a metodologia se torne ágil e simples a medida que se torna cotidiana.
Concordo pois todo processo no inicio parece ser mais complexo do que realmente é!
Concordo que se torna mais fácil e ágil, porem ainda sim o time ICT pode trabalhar em tornar os processos mais simples.
Concordo!
Concordo! Dentro do padrão evolutivo processual, é natural que um processo novo gere desconforto devido as mudanças aplicadas e gradativamente vá se tornando natural e cultural, facilitando sua utilização e visualizando seus benefícios.
Concordo, mas acredito que menos é mais e que a simplicidade as vezes traz mais qualidade do que a complexibilidade.
Concordo, mas nem sempre se tornam mais ágeis.
Concordo.
Concordo. No inicio tudo parece mais complicado do que realmente é. Depois do periodo de adaptação quando o usuário já conhece mais a ferramenta, fica mais claro e fácil.
Concordo. Usualmente precisamos criar a cultura da importância da Segurança da Informação junto aos usuários.
Parcialmente, alguns processos se mantem complexos em todo seu ciclo.
Sim concordo com a afirmação uma vez que a medida que se alcança maior maturidade aos processos, estes naturalmente se tornam mais simples aos seus utilizadores.
Sim, assim como todo novo processo, tanto a qualidade quanto a utilização evolui com o tempo.
Sim, desde que a comunicação destas implementações sejam efetivas e transparentes.
SIM, é natural que toda mudança no início gere uma certa resistência pelos usuários, mas quando a implementação ocorre com qualidade a mesma resulta em diversos benefícios para a organização e para os seus usuários.
Sim, os processos de segurança garantem que pessoas tenham acesso a informações de acordo com o nivel de confidencialidade das mesmas definidas pela empresa. O processo estruturado garante agilidade no atendimento as demandas.
Sim, quanto mais se utiliza mais simples se tornam os fluxos e processos.
Sim, realmente gera uma mudança de cultura, sendo necessário uma fase de adaptação. Mas ao passar por esta etapa, existe sim uma nítida evolução no processo e consequentemente aos usuários da TI e incremento de Segurança.
Sim, todo processo se torna simples a medida que seus participantes mantem maior contato com os mesmos.
Sim. Concordo
Sim. De forma geral as alterações de processos, também em TI, geram um desconforto inicial mas a medida que se utiliza o processo vai se tornando uma rotina e consequentemente mais fácil de se entender e utilizar.
Sim. O usuário irá ter um pouco de dificuldade para se adaptar as regras novas, mas com o passar do tempo, fará tudo de forma automática trazendo benefícios para si próprio e para a empresa.
O que você sabe sobre a lei SOX (Sarbanes Oxley) e qual a relação você sugere entre a SOX e a Segurança da Informação de uma organização?
A segurança da informação está contida dentro dos controles internos da organização que por sua vez é exigido e testado em auditorias pela lei norte americana Sarbanes Oxley (SOX).
A SOX e Segurança da Informação estão diretamente relacionados. Para atender os requisitos de controle de processo definidos pela SOX é extremamente necessário o alinhamento com a segurança da informação.
A SOX é um lei norte americana, criada para minimizar os riscos de fraudes nas organizações que publicam valores na bolsa de Nova Iorque, minimizando possíveis perdas dos investidores em casos de fraudes e ações que desvalorizem a organização. Uma vez implementada a SOX, controle internos serão incluídos e consequentemente uma maior seguranças das informações serão observadas.
A SOX é uma lei Norte Americana, inerente à bolsa de valores de NY e está intrinsecamente ligada à segurança da informação e controles internos, já que tem por objetivo dar razoável confiabilidade aos investidores em relação à organização pela qual se está investindo.
A SOX foi implementada com o objetivo de auditar as empresas cotadas em bolsas americanas quanto aos controles financeiros das mesmas com o objetivo de evitar fraudes e garantir maior segurança aos investidores. A Segurança da Informação precisa garantir que o uso e os acessos aos sistemas financeiros ou os pares estejam bem segmentados e de acordo com a real função dos usuários e de modo que não haja nenhum acesso indevido ou que tenha algum conflito de interesse.
Certificação que traz um conforto razoável à Administração, terceiros, investidores, etc., de que a Organização possui um ambiente de gerenciamento de riscos adequado, com controles eficientes e eficazes. Sobre a relação com Segurança da Informação, entendo que é um pilar primordial e que necessita de ser gerenciado e testado para concluirmos a respeito do ambiente geral de controles internos da Organização.
É uma lei criada para a criação de mecanismos de auditoria e segurança confiaveis nas empresas, com o intuito de evitar fraudes. Todas as informações de uma organização devem ser asseguradas e que haja meios de identificar irregularidades quando houver.
Entendo que é uma lei voltada para empresas nos EUA e que possuem atuação global para proteger a própria companhia no vazamento de informações e também evitar fraudes.
Lei dos Estados Unidos para quem atua na bolsa de valores de Nova Iorque.
Lei dos EUS que atinge empresas americanas ou não que atuam na bolsa de valores americana.
Lei Norte Americana foi escrita pelo Deputado Oxley e o Senador Sarbanes que deram nome à lei protecionista aos acionistas da bolsa de valores dos EUA e sancionada pelo então presidente George Bush em 2002.
Meu conhecimento é superficial, entretanto sei que é de grande relevância para a organização e tem impacto na bolsa de valores. A Segurança está entre os itens necessários exigidos pela agência certificadora.
Não conheço bem, mas sei que temos auditorias e que existem processos controlados para se obter as certificações.
Não conheço detalhes sobre a lei ainda.
Não conheço muito bem, só sei que é uma exigência legal.
Não possuo conhecimentos amplos sobre o assunto.
Não sei nada sobre a lei SOX
Não tenho conhecimento.
Não tenho muito conhecimento a respeito da SOX para comentar.
Que se trata de uma lei de origem americana (EUA) por empresas cotadas na bolsa, onde a mesma mecanismos de auditoria e segurança confiáveis com o intuito 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.
São regras aplicadas às organizações para manter segurança em seus Controles Internos.
São regras para bolsa de valores dos EUA que exigem segurança das empresas para participarem da bolsa.
Sei que a lei visa proteger, identificar e combater fraudes que impactam no desempenho financeiro da empresa. Creio que a relação entre a SOX e a Segurança da Informação esteja nas atividades desenvolvidas dentro dos sistemas utilizados na empresa, uma vez que são desenvolvidas atividades que movimentam ou contribuem no financeiro da companhia.
Sei que é obrigatório para empresas que estão na bolsa e que visa aumentar os controles, segurança e que visa dar mais confiabilidade aos dados financeiros, contábeis, etc se implementada em conjunto com normais de Segurança da Informação.
Sei que se trata de regras referente a bolsa de valores e que nossa organização encontra-se inserida neste cenário, sendo necessário o cumprimento das diversas regras inerentes à SOX.
Tenho apenas um conhecimento básico e sei que são regras da organização.
Tenho um conhecimento parcial! Se trata de uma lei dos EUA que regula as empresas participantes da bolsa de valores, garantindo segurança aos investidores.

Em sua percepção em seu período como funcionário desta organização, os processos de ICT ficaram mais ou menos seguros? Qual a relação você visualiza entre os processos exigidos para utilização e suporte de ICT e sua resposta quanto ao nível de segurança da informação?
Tem melhorado constantemente devido a criação de políticas e normas junto ao respectivo acompanhamento da área de Security e aos processos de comunicação corporativos e com os gestores das áreas.
Sim, é notório uma evolução gradativa ao longo dos últimos anos tanto processualmente, quanto a nível de ferramentas ICT.
Com certeza ficaram mais seguros, inclusive podemos ver nitidamente este ponto no que tange a Gestão de acessos dos nossos sistemas.
Mais seguros. Vejo uma relação sólida entre os processos e o suporte de ICT. Vários processos foram criados buscando a excelência no que se fiz a respeito a segurança da informação e divulgado ao usuários diretos da empresa.
Os processos ficaram mais seguros. Os processos estabelecidos pelo ICT garantem o correto mapeamento de perfis e por consequencia melhora a segurança da informação.
Mais seguros.
Um pouco mais seguros. Ainda temos pontos como o uso notes e celulares que para mim ainda não são totalmente seguros.
Sim. Documentações de acessos de usuáriso. Geração de matrizes RACI.
Não percebi grandes mudanças durante o meu período como funcionário. A relação citada é de grande importância e deve ser sempre melhorada.
Mais seguros, a cada dia temos mais controles para gestão e mapeamento de usuarios, assim como autorizações por pessoas especializadas e gestores.
Do tempo que trabalho na organização vejo que os processos ficaram mais seguros porém cada vez mais burocráticos.Vejo que em relação ao suporte e resposta o atendimento está mais rapido.
O cenário organizacional fica diferente a cada ano com o avanço das tecnologias e com a internet. A resposta natural de uma grande empresa multi-nacional é aumentar no mesmo nível a segurança dos sistemas e das informações trafegadas.
Mais seguros e sempre em evolução
Os processos de uma forma geral demostram ser controlados e ter segurança adequada.
Acredito que estão sempre em evolução, pois sempre recebemos novidades e comunicados internos sobre o tema.
Sim. Os processos anteriormente à SOX eram desorganizados e inseguros (apesar de mais ágeis, gerava muitas vezes retrabalho) e agora posso enfim dizer que estou satisfeita com os processos ICT.
Vejo uma evolução constante dos processos, que os tornam mais seguros, mas em contrapartida mais complexos ou demorados.
Para os processos que eu utilizo e(ou) faço parte, tiveram pequenas alterações por já estarem em um grau bastante elevado de segurança e certamente outras ações devem ser alvo atual de prioridade em ações evolutivas.
Os processos ficam cada vez mais complexos, mas acredito que seja devido a exigências vindas de cima para baixo, logo são estratégicas da organização.
Houve uma evolução notória em relação à segurança da informação após o processo de fusão entre as empresas do grupo e fica explicito o papel da TI neste processo.
O ICT da organização se preocupa bastante com a Segurança, e isto pode ser percebido nas campanhas de compliance e processos bem estabelecidos.
Sim, ficaram mais seguros e os processos ICT garantem boa parte desta segurança, juntamente com as atitudes das pessoas da organização de um modo geral.
Como estou a pouco tempo na organização, ainda não pude perceber grandes alterações, Entretanto os processos em que precisei de utilizar me pareceram de simples utilização e bastante seguros.
Os processos de ICT são seguros e evoluem claramente ao longo de cada ano. Estou satisfeita com o empenho de nosso ICT.
Acredito que sim, mas minha utilização dos processos foram minimas até aqui.
Os processos ficaram mais seguros até porquê o cenário global exige cada vez mais segurança dentro das organizações para que elas se mantenham competitivas e confiáveis na percepção de valor dos seus clientes.
Foram criados muitos processos burocráticos que no fim atrapalham a atividade das áreas que não são de TI.
Você está satisfeito com os processos atualmente aplicados para solicitação de serviços de ICT (Acessos em Aplicações, Alteração em Sistemas, Acesso à Internet, Restauração de dados perdidos, entre outros)? Justifique sua resposta.
Sim. Temos uma ferramenta amigável, com SLA's bem definidas e com todos os serviços devidamente agrupados por área responsável de atendimento.
Sim. Apesar de demandarem todo um fluxo, uma vez que se compreende o processo, ele se torna simples e garante que serei atendido.
Parcialmente, pois temos vários sistemas de controle de chamados e poderíamos ter todas as solicitações controladas por um único sistema.
Sim. Nunca tive problemas com os itens informados.
Sim, na minha área de atuação, os processos são satisfatórios.
Razoavelmente satisfeito. Já possúimos ferramentas robustas em uso e que suportam o usuário no processo junto ao ICT.
Sim, mas sempre se pode melhorar.
Em partes sim, pois os usuários ainda detem de caminhos diversos para solicitação de serviços do tipo, o que se torna moroso, desgastante e gera a sensação de falta de organização. O ideal seria uma unificação.
Não. O processo de abertura de chamados dificulta o atendimento.
Sim, não tive problemas junto ao ICT nas minhas demandas.
Estou satisfeito, sempre que precisei mesmo que com algumas burocracias as solicitações foram atendidas em tempo consideravél.
Poderia ser mais veloz, mas de forma geral estou satisfeito pois sempre tenho minhas solicitações atendidas.
Sim, mas nem sempre consigo realizá-los sem suporte do próprio ICT.
Sim, nunca tive problemas com os processos.
Sim, mas acredito que podem melhorar e serem mais simplificados.
Sim, vide resposta anterior.
Sim, mas podem e devem ser sempre melhorados sob a visão de maior comodidade aos usuários sem que perca qualidade ou segurança.
Sim, tudo que precisei até então fui atendido a contento e dentro de processos corretos.
Não, acredito que poderiam ser menas regras e mais agilidade no atendimento.
Sim, satisfeito por existir processos bem estabelecidos e com um time apto para suporta-lo.
Satisfeito.
Parcialmente. Os processos atendem bem seu objetivo e garantem maior segurança e organização, porem muitas vezes são demorados.
Sim, Não tive nenhum problemas para obter meus acessos e credenciais na rede, e-mail, internet e sistemas de uso diário.
Sim, satisfeita conforme dito na resposta anterior.
Sim, sem maiores problemas.
Sim satisfeita, pois se mostram dinâmicos e adaptáveis à realidade proposta pelo mundo corporativo.
Parcialmente, considero muito burocrático (aprovações, chamado para abrir chamado, etc)

Se você tivesse a oportunidade de alterar um processo atualmente existente para ICT, qual seria a alteração realizada?
Por sermos uma empresa global, diversos serviços da nossa região na América Latina (como Proxy e Firewall) são geridos pelo time Europa e não diretamente por nós, gerando um tempo de atendimento muito grande e a falta de entendimento da real necessidade e urgência dos nossos usuários.
Gerar uma maior sinergia entre as áreas internas de ICT para com a área de negócios minimizando entendimentos falhos e garantindo que o business entende o porquê de cada mudança, se tornado parte da mudança.
Implementação de um único sistema de abertura de tickets, seja ele para infra, controle de acessos, change em sistemas, etc
Automatização do processo de controle de transferidos.
Seria na ferramenta de abertura de chamados, que considero complexa para o ponto de vista de usuário.
Maior monitoramento (mais no detalhe) em conceder perfis de acesso.
No momento não tenho um processo para ser alterado.
Unificação de solicitação de acessos em uma unica ferramenta, ou ainda que ela contivesse o link e manuais com orientações para cada necessidade de sistema na organização. Um unica base contendo todos o conteúdo.
Alteraria a abertura de chamados para uma forma mais eficiente de analisar os serviços prestados pelo ICT.
Apenas ter mais visibilidade do que cada usuario poderia ter acesso ou não, ser algo mais aberto ao funcionário.
Alterar o processo de solicitação de Notebook/desktop pois sempre que entra um novo funcionario ou estagiario perde se alguns dias aguardando o equipamento. No momento da contratação o equipamento já deveria ser solicitado ao ICT que o teria pronto quando o novo funcionario começasse na empresa.
Mais treinamento quanto aos processos que atingem em especial às áreas ligadas a manufatura que fica de certa forma distante da TI.
Todas as solicitações serem feitas via helpdesk telefônico sem a necessidade de parar para registrar em um sistema.
Ainda não identifiquei um item a ser modificado para processos de TI.
Apenas torna-los mais simples para qualquer tipo de solicitante.
Uso do processo em dispositivos mobile.
Um portal único com todos os serviços ICT.
Não sei responder neste momento.
Faria processos mais simples, rápidos e que resolvessem o problema do usuário com o minimo de burocracia.
Não alteraria nada!
Desenvolvimento de um aplicativo para celulares que responda por comandos de voz.
Apenas mecanismos para tornar o atendimento ainda mais rápido. Exemplo: Um sistema leva mais de 15 dias para ser alterado em pequenas mudanças que muitas vezes trarão agilidade ao negócio.
Ainda não observei necessidade de mudanças a serem realizadas.
Ainda não pensei nisto.
Simplificar cada vez mais, para tornar mais ágil e de fácil entendimento.
Não tenho uma opinião formada quanto a esta questão!
Todo o atendimento ser feito por apenas uma ou duas pessoas e estes fazem os processos burocráticos tirando esta ação das áreas.

Fonte: Própria (2018)

ANEXO A – Descrição dos Controles ITGC SOX da organização Ind-Force **(continua)**

INDFORCE GROUP - ITGC BRASIL					
BLOCO	**ITGC CODE**	**CONTROLE ITGC**	**RISCO**	**DESCRIÇÃO DO CONTROLE**	**CHAVE DE RISCO**
1	SD15.1	Aquisição e Manutenção de Softw are	Sem uma abordagem estruturada e formal para o gerenciamento de softw are que inclui controles sobre o design, aquisição e implementação de sistemas de aplicativos, os requisitos de negócios e segurança não podem ser atendidos, especialmente quando o envolvimento do usuário não foi identificado para cada etapa do processo, desde a definição de requisitos até fase de teste.	A organização possui uma metodologia de ciclo de vida de desenvolvimento de sistemas (SDLC), que inclui requisitos de segurança e processamento de integridade da organização.	Politica SDLC
	SD15.3	Aquisição e Manutenção de Softw are	Sem uma abordagem estruturada e formal para o gerenciamento de softw are que inclui controles sobre o design, aquisição e implementação de sistemas de aplicativos, os requisitos de negócios e segurança não podem ser atendidos, especialmente quando o envolvimento do usuário não foi identificado para cada etapa do processo, desde a definição de requisitos até fase de teste.	A metodologia SDLC inclui requisitos que os sistemas de informação serão projetados para incluir controles de aplicativos que suportem processamento de transações completo, preciso, autorizado e válido.	Politica SDLC
	SD15.5	Aquisição e Manutenção de Softw are	Sem uma abordagem estruturada e formal para o gerenciamento de softw are que inclui controles sobre o design, aquisição e implementação de sistemas de aplicativos, os requisitos de negócios e segurança não podem ser atendidos, especialmente quando o envolvimento do usuário não foi identificado para cada etapa do processo, desde a definição de requisitos até fase de teste.	Para manter um ambiente confiável, o gerenciamento de TI envolve usuários na fase de design de aplicativos, na seleção do softw are, nos requerimentos de négocio e no teste integrado.	Implementação de sistemas / Conversão de teste do usuário final
2	CM19.1	Gestão de Mudanças	Sem controles adequados sobre o processo de gerenciamento de mudanças, alterações no sistema de informações erradas ou não autorizadas podem resultar em distorção significativa em relação ao relatório financeiro, afetando os controles e os dados relacionados à aplicação.	Os pedidos de alterações de programas, alterações de sistema e manutenção (incluindo mudanças no softw are do sistema) são padronizados, registrados, aprovados, documentados e sujeitos a procedimentos formais de gerenciamento de mudanças.	Testes de Mudança de Programa e Aprovações
	CM19.2	Gestão de Mudanças	Sem controles adequados sobre o processo de gerenciamento de mudanças, alterações no sistema de informações erradas ou não autorizadas podem resultar em distorção significativa em relação ao relatório financeiro, afetando os controles e os dados relacionados à aplicação.	Os pedidos de mudança de emergência são documentados e sujeitos a procedimentos formais de gerenciamento de mudanças.	Mudanças Emergênciais
	CM19.2b	Gestão de Mudanças	Sem controles adequados sobre o processo de gerenciamento de mudanças, alterações no sistema de informações erradas ou não autorizadas podem resultar em distorção significativa em relação ao relatório financeiro, afetando os controles e os dados relacionados à aplicação.	As intervenções manuais em ambiente de produção a partir de contas FireCallID, são documentadas e sujeitas ao procedimento formal de gestão de FireCallID.	Firecall Ids (Usuários com super acesso no ambiente produtivo)
	CM19.3	Gestão de Mudanças	Sem um forte controle de autorização sobre a atividade de migração de programas, mudanças no sistema de informações erradas ou não autorizadas, bem como fraude, podem resultar em distorção significativa em relação aos relatórios financeiros, afetando os controles e dados relacionados com aplicativos.	Existem controles para restringir a migração de programas para a produção apenas por indivíduos autorizados.	Permissão para aplicação de mudanças no ambiente produtivo
3	SD18.1	Implementação e Validação de Soluções	Sem uma abordagem estruturada e formal para testar atividades, os requisitos de negócios e segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação ao relatório financeiro, afetando controles e dados relacionados com aplicativos.	Uma estratégia de teste é desenvolvida e seguida para todas as mudanças significativas em aplicativos e tecnologia de infra-estrutura, que aborda testes de unidade, sistema, integração e nível de aceitação de usuários para que os sistemas implantados funcionem como pretendido.	Implementação do sistema / Teste de conversão
	SD18.3	Implementação e Validação de Soluções	Sem uma abordagem estruturada e formal para testar atividades, os requisitos de negócios e segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação ao relatório financeiro, afetando controles e dados relacionados com aplicativos.	Interfaces com outros sistemas são testadas para confirmar que as transmissões de dados são completas, precisas e válidas.	Teste de Interface
	SD18.4	Implementação e Validação de Soluções	Sem uma abordagem estruturada e formal para testar atividades, os requisitos de negócios e segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação ao relatório financeiro, afetando controles e dados relacionados com aplicativos.	A conversão de dados é testada entre sua origem e seu destino para confirmar que os dados são completos, precisos e válidos.	Teste de conversão de dados
4	SA22.1	Garantir a Segurança dos Sistemas	Sem controles adequados sobre questões de segurança, os requisitos de segurança não podem ser abordados. Isso poderia afetar significativamente os sistemas de aplicativos, bem como o nível de conformidade com os requisitos externos, elevando o nível de exposição à perda de dados e acesso não autorizado..	Existe uma politica de segurança da informação e foi aprovada por um nível apropriado de gerenciamento executivo.	Politicas e procedimentos de segurança da informação
	SA22.5	Garantir a Segurança dos Sistemas	Sem controles adequados sobre questões de segurança, os requisitos de segurança não podem ser abordados. Isso pode afetar significativamente os sistemas de aplicativos, bem como o nível de conformidade com os requisitos externos, aumentando o nível de exposição à perda de dados e acesso não autorizado. Sem controles adequados sobre os processos de identificação e autenticação, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a aplicativos do sistema que apoiem o processo .	Os procedimentos existem e são seguidos para autenticar todos os usuários no sistema (interno e externo).	IDs de usuário e autenticação
	SA22.6	Garantir a Segurança dos Sistemas	Sem controles adequados sobre os processos de identificação e autenticação, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação ao relatório financeiro, devido ao acesso não autorizado a aplicativos do sistema que suportam o processo.	Os procedimentos existem e são seguidos para manter a eficácia dos mecanismos de autenticação e acesso.	Configurações de senha
	SA22.7b	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o processo de gerenciamento de conta de usuário, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a aplicativos do sistema que suportam o processo ou alocação inadequada de direitos ou privilégios de usuários.	Existem procedimentos e são seguidos relacionados a ações oportunas para solicitar, estabelecer, emitir, suspender e fechar contas de usuários. (Incluir procedimentos para autenticar transações originadas fora da organização.)	Acesso Novo Empregado
	SA22.12	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o processo de gerenciamento de conta de usuário, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a aplicativos do sistema que suportam o processo ou alocação inadequada de direitos ou privilégios de usuários.	Os controles relativos à segregação adequada dos direitos sobre solicitação e concessão de acesso a sistemas e dados existem e são seguidos.	A segregação de funções dos deveres entre os requerentes de acesso e os administradores

ANEXO A – Descrição dos Controles ITGC SOX da organização Ind-Force
(conclusão)

INDFORCE GROUP - ITGC BRASIL					
BLOCO	**ITGC CODE**	**CONTROLE ITGC**	**RISCO**	**DESCRIÇÃO DO CONTROLE**	**CHAVE DE RISCO**
4	SA22.13	Garantir a Segurança dos Sistemas	Sem controles adequados sobre os processos de segurança física, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso físico não autorizado aos sistemas que suportam o processo.	O acesso às instalações é restrito ao pessoal autorizado e requer identificação e autenticação apropriadas.	Segurança Física
	SA22.8	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o processo de revalidação do usuário, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a sistemas de aplicativos que suportam o processo ou alocação inadequada de direitos ou privilégios de usuários.	Existe um processo de controle e é seguido para periodicamente rever e confirmar os direitos de acesso.	Revalidação de Acesso Lógico
	SA22.11	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o processo de monitoramento de violação de segurança, os requisitos de segurança não puderam ser atendidos e as atividades de melhoria não poderiam ocorrer. Isso pode resultar em distorção significativa em relação ao relatório financeiro, indisponibilidade do serviço, perda ou dano de dados, devido ao acesso não autorizado aos sistemas de informação.	A administração de segurança de TI monitora e registra a atividade de segurança no sistema operacional, os níveis de aplicativos e bancos de dados e as violações de segurança identificadas são relatadas para o gerenciamento sênior.	Monitoramento de Logs de Segurança
	SA22.7a	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o processo de gerenciamento de conta de usuário, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a aplicativos do sistema que suportam o processo ou alocação inadequada de direitos ou privilégios de usuários.	Existem procedimentos e são seguidos relacionados a ações oportunas para solicitar, estabelecer, emitir, suspender e fechar contas de usuários.	Remoção de Permissões de Acesso para Usuários Desligados
	SA22.7c	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o processo de gerenciamento de conta de usuário, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a aplicativos do sistema que suportam o processo ou alocação inadequada de direitos ou privilégios de usuários.	Existem procedimentos e são seguidos relacionados a ações oportunas para solicitar, estabelecer, emitir, suspender e fechar contas de usuários.	Remoção de Permissões de Acesso para Usuários Transferidos
	OS / DB	Garantir a Segurança dos Sistemas	Sem controles adequados sobre o acesso do administrador do sistema operacional e do banco de dados, os requisitos de segurança não podem ser atendidos. Isso pode resultar em distorção significativa em relação aos relatórios financeiros, devido ao acesso não autorizado a aplicativos do sistema e bancos de dados que suportam o processo ou alocação inadequada de direitos ou privilégios de usuários.	O acesso do administrador do sistema operacional e do banco de dados é restrito ao pessoal adequado	Acesso de Administrador de SO e DB
5	OP24.1	Gestão de Problemas e Incidentes	Sem controles adequados sobre o gerenciamento de problemas e incidentes, os requisitos de nível de serviço não puderam ser atendidos e as atividades de melhoria não poderiam ocorrer. Isso poderia afetar significativamente o processo de relatórios financeiros, causando perda ou dano de dados.	O gerenciamento de TI definiu e implementou um sistema de gerenciamento de incidentes e problemas de modo que a integridade dos dados e os incidentes de controle de acesso sejam registrados, analisados, resolvidos em tempo hábil e reportados ao gerenciamento.	Gestão de Problemas / Incidentes
6	SA23.3	Gestão de Configuração	Sem controles adequados sobre a configuração dos sistemas, pode haver uma exposição de segurança significativa que pode permitir o acesso não autorizado a sistemas e dados que possam afetar os relatórios financeiros. A integridade dos dados e a disponibilidade do sistema podem ser afetadas por um controle fraco da configuração ao fazer alterações no sistema ou na instalação de componentes não autorizados do sistema.	Existem ambientes devidamene segregados para Desenvolvimento, Teste e Produção	Os ambientes de produção, teste e desenvolvimento são separados
7	DR25.4	Gestão de Dados	Sem controles adequados sobre o processo de armazenamento de dados e programas, a integridade, a existência e os requisitos de autorização da informação não puderam ser atendidos. Isso pode resultar em distorção significativa em relação ao relatório financeiro, devido à falta de definição de procedimentos de backup, períodos de retenção e termos de armazenamento, de acordo com os requisitos de negócios e conformidade.	A administração IT implementou uma estratégia de backup cíclico de dados e programas	Backups de dados
	DR25.5	Gestão de Dados	Sem controles adequados sobre o processo de armazenamento de dados e programas, a integridade, a existência e os requisitos de autorização da informação não puderam ser atendidos. Isso pode resultar em distorção significativa em relação ao relatório financeiro, causando indisponibilidade de dados e programas de backup quando necessário.	A restauração de informações é testada periodicamente.	Teste de Backups
8	OP26.1	Gestão de Operações	Sem controles adequados sobre as operações de TI e desvios ou erros relacionados, os requisitos de existência e integridade das transações não puderam ser atendidos, levando a distorção significativa em relação aos relatórios financeiros.	A administração IT estabeleceu, documentou e segue os procedimentos padronizados para operações de TI, incluindo o monitoramento de Jobs e resposta aos eventos de segurança e integridade.	Processamento e Monitoramento de Jobs

Fonte: Ind-Force (2017)

ANEXO B – Questionário para definição das aplicações escopo da auditoria ITGC SOX

(continua)

IndForce Brasil - Questionário de Escopo ITGC SOX		
Processo/Sub-Processo	**Processes/Subprocesses**	**Aplicação/Aplication**
Compra a pagar	**Purchase-to-pay**	
Verificação de fatura	Invoice verification	
Gerenciamento de contas a pagar	Managing accounts payable	
Processamento de contas a pagar	Processing accounts payable	
Processamento de nota de crédito / débito	Processing credit/debit note	
Reconciliações	Reconciliations	
Gerenciando o envelhecimento dos fornecedores	Managing suppliers' ageing	
Processamento de pagamentos	Processing payments	
Coleção de vendas e crédito	**Sales & credit collection**	
Adquirir e aprovar clientes	Acquiring and approving customers	
Manter o arquivo mestre do cliente	Maintaining customer master file	
Gerenciando dados de preços	Managing pricing data	
Gerenciando contratos de vendas	Managing sales contracts	
Gerenciando e processando ordens	Managing and processing orders	
Distribuição e entrega	Distribution and delivery	
Gerando faturas e notas de crédito / débito	Generating invoices and credit/debit notes	

ANEXO B – Questionário para definição das aplicações escopo da auditoria ITGC SOX

(continuação)

IndForce Brasil - Questionário de Escopo ITGC SOX		
Processo/Sub-Processo	**Processes/Subprocesses**	**Aplicação/Aplication**
Processamento de contas a receber e notas de crédito / débito	Processing account receivables and credit/debit notes	
Processamento de recibos de caixa e gerenciamento de créditos	Processing cash receipts and managing credits	
Atividades de factoring / securitização	Factoring/securitization activities	
Gerenciamento de insolvências e provisão para devedores duvidosos	Managing insolvencies and allowance for doubtful accounts	
· Ofertas comerciais e incentivos ao cliente	Trade deals and customer incentives	
Em Processamento	Processing	
Gravação	Recording	
Forma de pagamento	Payment	
Serviços pós-venda	After-sale services	
Gestão de inventário	**Inventory management**	
Fornecer segurança física de inventário	Providing inventory physical security	
Manter o arquivo mestre de inventário	Maintaining inventory master file	
Processamento de recibos de produtos	Processing product receipts	
Manuseio de mercadorias	Handling goods	
Envio de produtos	Shipping products	
Gerenciando bens / materiais detidos por terceiros	Managing goods/materials held by third party	
Gerenciamento de bens / materiais de terceiros detidos pela empresa	Managing third party goods/materials held by the company	
Processamento de retornos de clientes / fornecedores	Processing customer/vendor returns	
Gerenciando e controlando o inventário físico	Managing and controlling physical inventory	
Avaliação de inventário (contabilidade e custos) e fundos	Inventory valuation (accounting and costing) and funds	
Avaliação de inventário de matérias-primas, WIP, produtos acabados, peças sobressalentes	Inventory valuation of raw materials, WIP, finished goods, spare parts	
Custo padrão;	standard cost;	
Método FIFO (para fins de relatório do grupo)	FIFO method (for Group reporting purposes)	
Identificar / Gerenciar / Avaliar o excesso / materiais obsoletos e restos	Identify/Manage/Evaluate excess/obsolete materials and scraps	
Menor custo ou Avaliação do mercado	Lower cost or market evaluation	
Ativo Fixo e Intangíveis	**Fixed Assets and intangibles**	
Fornecer segurança física de ativos fixos	Providing fixed assets physical security	
Identificar / aprovar investimentos / alienações	Identifying/approving investments/disposals	
Adquirir / Produzir / Transferir ativos fixos	Acquire/Produce/Transfer fixed assets	
Gerenciamento de instalações de processamento e despesas	Processing facility management and expenditures	
Manutenção do registro de ativos fixos	Maintaining fixed assets register	
Realizar inventário físico	Perform physical inventory	
Eliminação de ativos fixos	Fixed asset disposals	
Depreciação / write-down, write-up e restabelecimento do valor original	Depreciation/ write-down, write-up and reinstatement of original value	
Contabilidade de ativos fixos	Fixed asset accounting	
Ativos tangíveis	Tangible assets	
Ativos intangíveis	Intangible assets	
Gestão de folha de pagamento e pessoal	**Payroll and personnel management**	
Manutenção do arquivo mestre HR / folha de pagamento	Maintaining HR/payroll master file	
Tempo de gravação	Recording time	
Cálculo e relatório da folha de pagamento	Calculating and reporting payroll	
Processamento do imposto pessoal e contribuições	Processing personnel tax and contributions	
Auto-emprego (contrato, requisitos fiscais)	Self-employment (contract, fiscal requirements)	
Processamento de adiantamentos e reembolso de despesas	Processing advances and reimbursement of expenses	
Bônus de processamento, opções de compra de ações, outros benefícios	Processing bonus, stock options, other benefits	
Gerenciando fundos de pensão	Managing pension funds	

ANEXO B – Questionário para definição das aplicações escopo da auditoria ITGC SOX

(conclusão)

IndForce Brasil - Questionário de Escopo ITGC SOX		
Processo/Sub-Processo	**Processes/Subprocesses**	**Aplicação/Aplication**
Processamento de pagamentos de folha de pagamento	Processing payroll payments	
Pessoal de encerramento	Terminating personnel	
Acréscimos de pessoal final do período	Period end personnel accruals	
Contabilidade e processamento do custo da mão-de-obra	Accounting and processing labour cost	
Tesouro (CNH Industrial Finance)	**Treasury (CNH Industrial Finance)**	
Gerenciamento de empréstimos e empréstimos levantados (direto / em nome)	Managing loans and borrowing raised (direct/ on behalf)	
Gerenciamento de empréstimos e empréstimos concedidos (direto / em nome)	Managing loans and borrowing granted (direct/ on behalf)	
Gerenciamento de instrumentos financeiros derivativos (risco cambial, commodity, etc.)	Managing derivative financial instruments (exchange rate risk, commodity, etc.)	
Gerenciando títulos em mão	Managing securities on hand	
Emissão de ações / vínculo	Issuing shares/ bond	
Recapitalização de subsidiárias e empresas associadas	Subsidiaries and associated companies recapitalization	
Gerenciando dinheiro e equivalentes de caixa (exceto CNH Industrial Finance)	**Managing cash and cash equivalent (other than CNH Industrial Finance)**	
Gerenciando dinheiro	Managing cash	
Gerenciando contas bancárias	Managing bank accounts	
Gerenciamento de cobranças e pagamentos (Nacional / Estrangeiro)	Managing collections and payments (National/Foreign)	
Gerenciando o fluxo de caixa	Managing cash flow	
Gerenciando garantias	Managing guarantees	
Atividades de financiamento (Financiamento, Leasing, Factoring)	**Financing activities (Financing, Leasing, Factoring)**	
Gerenciando o financiamento do cliente / revendedor	Managing customer/dealer financing	
Gerenciando leasing	Managing leasing	
Gerenciamento de factoring / securitização	Managing factoring/securitization	
Impostos	**Taxes**	
Planejamento	Planning	
Gerenciamento de impostos diretos (IVA, impostos sobre a propriedade, outros impostos)	Managing direct taxes (VAT, property taxes, other taxes)	
Gerenciando impostos indiretos (IVA, impostos sobre a propriedade, outros impostos)	Managing indirect taxes (VAT, property taxes, other taxes)	
Gerenciamento de avaliações fiscais e procedimentos judiciais	Managing tax assessments and litigation procedures	
Avaliando impostos diferidos e pré-pagos	Evaluating deferred and prepaid taxes	
Gerenciando investimentos	**Managing investments**	
Aquisições / desinvestimentos	Acquisitions / disinvestments	
Avaliação	Valuation	
Gravação	Recording	
Gerenciando o Roteiro Geral	**Managing General Ledger**	
Gerenciando e mantendo o Plano de Contas	Managing and maintaining Chart of Accounts	
Gerenciando e mantendo o Roteiro Geral	Managing and maintaining General Ledger	
Gerenciando e reconciliando transações entre empresas	Managing and reconciling intercompany transactions	
Gerenciamento de livros e arquivos estatutários	Managing statutory books and files	
Fechamento financeiro e relatórios	**Financial closing and Reporting**	
Definição do processo de encerramento e relatórios financeiros	Defining the financial closing and reporting process	
Capturar e processar informações de fechamento	Capturing and processing closing information	
Preparando e revisando o Pacote de Relatórios	Preparing and reviewing the Reporting Package	
Reconciliação US GAAP	US GAAP Reconciliation	
Processo de consolidação	**Consolidation Process**	
Definição do processo de consolidação	Defining the consolidation process	
Consolidação de Pacotes de Relatórios (Empresa)	Reporting Packages consolidation (Company)	
Gerenciando Relatórios Financeiros de Divulgação	Managing Disclosure Financial Reporting	

Fonte: Ind-Force (2017)