VI SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302
V ELBE
Encontro Luso-Brasileiro de Estratégia
Iberoamerican Meeting on Strategic Management

Compliance uma ferramenta estratégica para a segurança das informações nas organizações

DEIVERSON FELIPE SOUZA XAVIER
Faculdade Pitágoras de Betim
deiverson_felipe@hotmail.com

DÁPHINE PEREIRA COSTA
Faculdade Pitágoras de Betim
dphinepcosta2006@gmail.com

LUIZ OSVALDO VILAR DE ALMEIDA
Fundação Pedro Leopoldo (FPL)
lovalmeida50@yahoo.com.br

LUCAS BERALDO SOARES
Faculdade Pitágoras de Betim
lucasberalldo@gmail.com

Compliance uma ferramenta estratégica para a segurança das informações nas organizações

Resumo

Estudos a respeito do programa *Compliance* têm despertado grande interesse para os administradores e consultores com o propósito de desenvolver e solidificar a conformidade das organizações em relação às leis, normas, procedimentos. Este trabalho tem como principal foco o programa *Compliance*, sua definição e seus parâmetros; aborda seu histórico em âmbito global, e implantado no Brasil após a promulgação da lei 12.846/13, o perfil de um profissional da importância do compliance nas organizações, os benefícios da implantação e os malefícios e riscos da não implantação do programa nas organizações. Este estudo foi desenvolvido através de uma pesquisa exploratória com análise qualitativa, e tem como questão norteadora: Qual a importância de se implantar um programa Compliance para a segurança das informações dentro das organizações? Dessa forma o trabalho tem como objetivo geral analisar os benefícios para a segurança da informação obtidos com a implantação do programa *Compliance* dentro da organização do ramo siderúrgico em Contagem, e especificamente, descrever os parâmetros do Sistema Compliance para a segurança das informações na organização, identificar os aspectos positivos da implantação do programa Compliance para a organização e verificar a quais vulnerabilidades a organização estaria exposta por não implantar o programa. O programa na organização lhes passa a sensação de segurança, em função de garantir o monitoramento do cumprimento das leis, normas e procedimentos para que os estímulos para se cometer atos inaceitáveis eticamente ou ilícitos sejam sempre reprimidos, tornando o ambiente mais seguro e propenso às boas práticas

Palavras chave: Compliance, Segurança, Informação

Abstract

Studies regarding the Compliance program have aroused great interest to administrators and consultants for the purpose of developing and solidifying the organizations' compliance with laws, regulations, and procedures. This work has as main focus the Compliance program, its definition, and its parameters; Addresses its history at a global level, and implemented in Brazil after the enactment of Law 12.846 / 13, the profile of a professional, the importance of compliance in organizations, the benefits of implementation and the wrongs and risks of not implementing the program in organizations . This study was developed through an exploratory research with qualitative analysis, and has as guiding question: What is the importance of implementing a Compliance program for information security within organizations? In this way the work has as general objective to analyze the benefits for the information security obtained with the implementation of the Compliance program within the organization of the steel industry in Contagem, and specifically, to describe the parameters of the Compliance System for information security in the organization, to identify The positive aspects of implementing the Compliance program for the organization and to verify to which vulnerabilities the organization would be exposed for failing to implement the program. The program in the organization gives them a sense of security in order to ensure compliance with laws, regulations, and procedures so that the stimuli to commit unacceptable ethically or illicit acts are always repressed, making the environment safer and prone to good Practices

Key Words: complaince, segurança, segurança da informação

1 INTRODUÇÃO

Quando se fala em segurança da informação, automaticamente se pensa em Tecnologia da Informação, mas na verdade a segurança da informação ultrapassa este conceito. Segundo a NBR ISO/IEC 17799 (2005) a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Todavia com o aumento da competitividade e a facilidade em se obter dados, as organizações enfrentam diversos desafios para se protegerem de crackers, vírus, e o escoamento de informações sigilosas, principalmente em relação à concorrência.

Mesmo a informação sendo peça fundamental para a garantia do negócio, as organizações não garantem a proteção adequada e podem ter dados importantes divulgados. A falta de conhecimento, conscientização e crença por parte da liderança, dos funcionários e dos parceiros de negócios; falta de plano de ação constante e pragas virtuais, como Vírus, *Worms*, *Trojan Horse*, *Spyware*, *Adware*, *RootKits*, *Botnet* e Bombas Lógicas são os principais perigos que ameaçam a Segurança da Informação de uma empresa.

A NBR ISO/IEC 17799:2005 define que a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. A aplicabilidade deste programa promove a conformidade, segurança dos processos, informações, posicionamentos e decisões empresariais aplicados pelos *share* e *stakeholders.*

De acordo com Mello (2015) a transmissão da informação se dá por diversos meios: e-mail, papel, voz, pen drives, CDs, DVDs e por aí vai. Assim, as vulnerabilidades estão por toda parte. As exposições percebidas por diversos autores os instigaram a pesquisar sobre, e definiram ações para mitigação do escoamento de informações e garantissem a proteção dos mesmos. Por tanto, para dar suporte à importância do programa *Compliance*, o presente estudo busca responder à seguinte questão: Qual a importância de se implantar um programa Compliance para a segurança das informações dentro das organizações? Dessa forma o trabalho tem como objetivo geral Analisar os benefícios para a segurança da informação obtidos com a implantação do programa *Compliance* dentro da organização SiderMax do ramo siderúrgico em Contagem, e especificamente, descrever os parâmetros do Sistema Compliance para a segurança das informações na organização SiderMax, identificar os aspectos positivos da implantação do programa Compliance e a proteção das informações para a organização SiderMax e verificar a quais vulnerabilidades a organização SiderMax estaria exposta por não implantar o programa *Compliance* sem garantir a segurança nas informações.

2 REVISÃO DA LITERATURA

2.1 Conceito de Compliance

Compliance significa agir de acordo ou estar conforme a algo. Segundo o Conselho O *Compliance* é um programa que visa à prevenção e a minimização de riscos as quais as organizações estão expostas, muitos podem comprometer a efetividade do negócio trazendo diversos prejuízos para as organizações por não cumprirem legislações, normas, procedimentos, regulamentos. De acordo com Bittencourt (2014) citado por Leal e Fockink (2014, p.54) o termo *Compliance*, originário da expressão anglosaxão *to comply*, exprime, em sentido literal o sentido de agir de acordo com uma regra ou comando. Refere-se então dessa forma que o *Compliance* busca cumprir todas as normas que lhe sejam atribuídas sejam elas de dentro da própria organização, ou normas externas.

Almeida (2015) aponta que o *Compliance* é compreendido como o conjunto de práticas e disciplinas adotadas pelas pessoas jurídicas no intuito de alinhar o seu comportamento coorporativo à observância das normas legais e das políticas governamentais aplicáveis ao setor de atuação, prevenindo e detectando ilícitos, a partir da criação de estruturas internas e procedimentos de integridade, auditoria e incentivos à comunicação de irregularidades, que forneçam um diagnóstico e elaborem um prognóstico das condutas e de seus colaboradores, com a aplicação efetiva de códigos de ética no respectivo âmbito interno.

O Conselho Administrativo de Defesa Econômica (2016) afirma que por meio dos programas de *Compliance*, os agentes reforçam seu compromisso com os valores e objetivos ali explicitados, primordialmente com o cumprimento da legislação. Esse objetivo é bastante ambicioso e por isso mesmo ele requer não apenas a elaboração de uma série de procedimentos, mas também uma mudança na cultura corporativa.

2.2 Histórico *Compliance*

De acordo com Vieira (2013) o *Compliance* sempre esteve presente, de alguma forma ou de outra, desde os primórdios do comércio organizado. Empresas têm adotado os seus próprios códigos de conduta, muitas vezes, levados pelos escândalos de outras empresas.

Manzi (2008) afirma que o programa *Compliance* teve origem nas instituições financeiras, com a criação do Banco Central Americano, em 1913, que objetivou a formação de um sistema financeiro mais flexível, seguro e estável. Contudo o programa *Compliance* começou a ser discutido nas instituições financeiras dos Estados Unidos onde buscavam a obtenção de um sistema seguro, protegido e que seguissem conforme legislações.

Segundo a Associação Brasileira de Bancos Internacionais e Federação Brasileira de Bancos citado por Freire (2016, p.2) as atividades de *Compliance* podem ser entendidas como uma necessidade decorrente de fatos anteriores a estes que foram exigindo maiores atividades de controles e necessidades de se estar em *Compliance*, e remetem a 1913 a criação do Banco Central Americano, e a outros registros das primeiras atividades de *Compliance*. Apesar de sua origem e seu avançado desenvolvimento, o conceito e os programas de *Compliance* não são exclusivos das instituições bancárias, uma vez que compreendem a busca pela aderência entre a ética individual e coletiva (Federação Brasileira de Bancos, 2010).

O programa *Compliance* de fato começou a ser discutido nos Estados Unidos quando as agências regulamentadoras começaram a emergir. O governo americano criou o programa como forma de fiscalização das instituições financeiras, mas aproximadamente em 1992 se ampliou para as atividades de saúde, comercio de alimentos e atividade ilícitas como a venda de entorpecentes. Buscavam ter um melhor controle dos atos que iriam contra as regulamentações americanas, e com o passar do tempo foi se adaptando a outras áreas. .

2.3 Compliance no Brasil

Segundo Moura e Oliveira (2015) no Brasil, a adoção do *compliance* foi através da Lei Anticorrupção, assim como a própria lei, teve grande influência externa, sendo os Estados Unidos, em 1977, o primeiro país a se comprometer com o combate a corrupção internacional, através do *Foreign Corrupt Pratice Act*, bem como o Reino Unido, que possui uma legislação rígida e ampla.

Rodrigues (2014) aponta que nos Estados Unidos existe um órgão chamado *Securities and Exchange Commission*, o correspondente à Comissão de Valores Mobiliários, que regula as atividades do mercado financeiro no Brasil. O *Securities and Exchange Commission* busca tentar promover a transparência e combater a anticorrupção nos mercados financeiros e

principalmente na bolsa de valores em todo o mundo, porque segundo a visão dos EUA a corrupção pode afetar negativamente um país.

De acordo com Rodrigues (2014) o primeiro resultado concreto da parceria entre o Brasil e EUA, no tocante o combate à corrupção está sendo visto mediante o desdobramento da Operação Lava Jato que tem como alvo principal a corrupção na Petrobrás, onde milhões de investidores estão em jogo, uma vez que as ações da Petrobrás estão disponíveis e sendo negociadas em bolsas de valores de diversos países, dentre os quais EUA.

Spinetto (2015) aponta que o Brasil aprovou uma nova lei anticorrupção, unindo-se a uma tendência internacional entre os países que buscam reprimir a corrupção. Rodrigues (2014) complementa que a Lei nº 12.846 publicada no Diário Oficial da União de 02 de agosto de 2013, a chamada Lei Anticorrupção Empresarial estabelece que empresas, fundações e associações passarão a responder civil e administrativamente sempre que a ação de um empregado ou representante causar prejuízos ao patrimônio público, infringir princípios da administração pública ou compromissos internacionais assumidos pelo Brasil. É a chamada responsabilização objetiva, prevista nas esferas civil e administrativa.

Amaral (2015) descreve que a Lei Anticorrupção oferece às empresas um indicativo do caminho a ser seguido para mitigar os desvios de conduta de seus membros e, assim, minimizar os riscos de eventuais punições decorrentes de atos ilícitos a elas relacionados. Nessa linha, a forma encontrada para estimular as empresas à adoção de programas de *Compliance* foi à possibilidade de redução das penalidades eventualmente aplicadas, conforme expresso no dispositivo acima.

Assim, por meio da Lei nº 12.846/2013, a Administração Pública incentiva às empresas a instituírem procedimentos internos de controle com o objetivo de se evitar a prática de atos ilícitos, bem como a quebra de sigilo de informações por meio de empregados ou qualquer outra pessoa que tenha algum vínculo com a empresa.

2.3.1 A importância do *Compliance* para as empresas brasileiras

Segundo Neves (2013) com a promulgação da Lei 12.846/13, que entrou em vigor em 29 de janeiro de 2014, todas as empresas brasileiras e seus dirigentes passam, agora, a ser expostos a graves consequências, na esfera civil e administrativa, por práticas de atos lesivos à administração pública, nacional ou estrangeira, for praticado em seu interesse ou benefício, exclusivo ou não.

A Lei Anticorrupção buscou fazer com que as empresas criem mecanismos internos de fiscalização e de incentivo à denúncia de irregularidades, em seu art. 7º, inciso VIII, ou seja, que busquem descobrir desvios de conduta ética e, como consequência, incentivar a elaboração e aperfeiçoamento de Códigos de Ética.

Segundo Leal e Fockink (2014) a lei evidencia dessa forma, uma direção, um caminho para que as empresas mitiguem e atuem prontamente a desvios cometidos pelos seus funcionários, fomentando a escolha desse caminho através de redução de penalidades.

Nesse passo, com a gradativa aplicação dessa cultura, o uso de código de ética, código de conduta, canal de denúncia, desenvolvimento de controles internos, procedimentos de divulgação de questões relacionadas à corrupção, análise de procedimentos éticos dos profissionais e parceiros comerciais além de crescente nas organizações, na incessante perseguição da mitigação das ações internas e externas, também se tornou peça fundamental para a atenuação de possíveis sanções administrativas, de vez que a Lei Anticorrupção, como fartamente mencionado, ao estabelecer o regime de responsabilidade objetiva, coloca as pessoas jurídicas em risco, impondo a elas a necessidade de se precaverem. (Bittencourt, 2014).

2.4 Os Pilares do programa *compliance*

Segundo a *Legal Ethics Compliance* (2016) o programa *compliance* é um sistema complexo e organizado, composto de diversos componentes, que interage com outros componentes de outros processos de negócios de empresas e, também, com outros temas. É um sistema que depende de uma estrutura múltipla que inclui pessoas, processos, sistemas eletrônicos, documentos, ações e ideias. A estes componentes se dá o nome de "pilares" do programa de *compliance*. A escola de *compliance* define então os pilares em:

a) 1° Pilar – Suporte da Alta Direção: Deve receber o aval explícito e apoio incondicional dos mais altos executivos da empresa.

b) 2° Pilar – Avaliação de Riscos: Riscos são eventos com impactos negativos no atingimento de um objetivo. É uma das bases do sucesso do programa, uma vez que o código de conduta, as políticas e os esforços de monitoramento deverão ser construídos com bases nos riscos que forem identificados como relevantes durante as análises..

c) 3° Pilar – Código de Conduta e Políticas de *Compliance*: Essa documentação serve como formalização inicial daquilo que é a postura da empresa em relação aos diversos assuntos relacionados à suas práticas de negócios, e servirá como uma bússola que guiará em conjunto com as ações e exemplos da alta administração, evidenciando o compromisso da empresa com o programa de *compliance,*

d) 4° Pilar – Controles Internos: São mecanismos, geralmente formalizados por escrito nas políticas e procedimentos da empresa, que, além de minimizar riscos operacionais e de *compliance*, asseguram que os livros e registros contábeis e financeiros reflitam completa e precisamente os negócios e operações da empresa.

e) 5° Pilar – Treinamento e comunicação: Cada funcionário da empresa, do chão de fábrica à alta direção deve entender os objetivos do programa, as regras e, talvez o mais importante seu papel para garantir o sucesso do programa.

f) 6° Pilar – Canais de Denúncias: Os canais de comunicação do tipo "canais de denúncias" fornecem aos funcionários e parceiros comerciais uma forma de alerta a empresa para potenciais violações ao código de conduta, a outras políticas ou mesmo a respeito de condutas inadequadas de funcionários ou terceiros que agem em nome da empresa.

g) 7° Pilar – Investigações Internas: As empresas devem possuir processos internos que permitam investigações para atender prontamente às denúncias de comportamentos ilícitos ou antiéticos. garantir que os fatos sejam verificados, responsabilidades identificadas.

h) 8° Pilar – Diligência adequada (Due Diligence): Due Diligence (ou avaliação prévia à contratação) para entender de forma abrangente a estrutura societária e situação financeira do terceiro, bem como levantar histórico dos potenciais agentes e outros parceiros comerciais, de forma a verificar se estes têm históricos de práticas comerciais antiéticas ou que, de outra forma, poderá expor a empresa a um negócio inaceitável ou que envolva riscos legais.

i) 9° Pilar – Auditoria e Monitoramento: A robustez do programa *compliance* se mede pela sua efetividade e para saber se o programa está caminhando na direção correta, é necessário implementar um processo de avaliação constante, chamado monitoramento, bem como auditorias regulares, que visam identificar se os diversos pilares do programa estão funcionando conforme planejado.

2.5 Beneficiar do programa *compliance*

Segundo o Conselho Administrativo de Defesa Econômica (2016) Organizações de todos os portes podem se beneficiar de um programa de *compliance*. No entanto, os riscos principalmente de ordem concorrencial a que uma organização está exposta variam de acordo com seu porte, posição de mercado, setor de atividades, objetivos. Por esta razão, não há um modelo único de programa de *compliance*. Cada programa deve respeitar as peculiaridades de cada indústria e ser revisto constantemente de modo a contemplar novos riscos que eventualmente possam surgir, como aqueles decorrentes de operações de fusões e aquisições, da introdução de um novo produto no mercado ou da entrada em um novo mercado geográfico com histórico de infrações em defesa da concorrência.

Além das próprias empresas, a adoção de programas de *compliance* beneficia terceiros, entre eles investidores, consumidores e parceiros comerciais, na medida em que garante que os mercados permaneçam competitivos, previne a ocorrência de infrações e danos delas decorrentes e evita perda de valor da empresa. Ainda, para as autoridades, a prevenção é sempre preferível à repressão e representa menor custo à sociedade. Conselho Administrativo de Defesa Econômica (2016).

2.4A importância do profissional de *Compliance*

Existem vários riscos aos quais as organizações estão expostas por não estarem em *compliance*, dentre estes estão a desproteção e escoamento de informações, fraudes, descumprimentos de procedimentos. Existe ainda o risco de danos à imagem da organização decorrentes de possíveis envolvimentos em casos de corrupção e demais descumprimento das normas, o que nos dá uma dimensão da importância da aplicação de um programa de *Compliance*., além do caráter legal, os deveres de *Compliance* relacionam-se com a observância de princípios éticos ligados à honestidade e transparência, de forma que a desatenção desses preceitos certamente possui o condão de acarretar em penalidades à imagem da empresa e seus gestores.

O gestor de *compliance* deve dispor de habilidades como capacidade de coordenação, conhecimento da legislação aplicável ao ramo de atividade da organização, conhecimento das normas e código de ética da própria organização e claro conhecer a fundo o programa e métodos de aplicação para que o mesmo seja efetivo.

2.5 A importância da informação

A informação é um elemento necessário para o processo de comunicação, tornando o ato de comunicar uma atividade importante para a convivência em sociedade. É através da comunicação que as pessoas transmitem informações e recebem outra como reposta. Conceituar informação não tem sido tarefa fácil, existem por trás deste contexto uma longa e antiga discussão e inúmeras definições para este termo. Lancaster (1989) citado por Cordeiro (2005) apresenta a seguinte afirmação: "É extremamente difícil definir informação, e até mesmo obter consenso sobre como deveria ser definida. O fato é, naturalmente, que informação significa coisas diferentes para pessoas diferentes".

2.5.1 A segurança da informação

A segurança da informação é necessária à organização para garantir a proteção das informações de ameaças. Haja vista que garante as empresas de minimizar os riscos e dar continuidade aos negócios. Segundo Rocha e Silva (2012) define a Segurança da Informação como conceito visto por ele como suporte para o bom funcionamento da segurança das informações.

Manter a segurança das informações através de processos de apoio, sistemas e redes, são importantes mecanismos para os negócios e necessários, tendo em vista a continuidade, competitividade, o fluxo do caixa, a lucratividade, etc. Norma ISO 17799 (2005) Segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

2.5.2 O *Compliance* para a segurança da informação

Nos cenários atuais de grandes movimentações coorporativas, vem sendo cada vez mais discutido sobre o programa *Compliance*, que visa à conformidade com as legislações e a garantia de proteções principalmente das informações das empresas. Para a proteção da informação se estar em *Compliance* é essencial que haja um processo de segurança da informação; O *Compliance* não acontece sem a segurança da informação, pois é ela toda base para seu processo.

De acordo com o *Compliance* Brasil (2015) Informação é todo e qualquer ativo, dado ou conteúdo desenvolvido e/ou gerenciado, os quais devem ser protegidos de forma adequada e compatível com a missão da organização. Já por segurança da informação, temos os procedimentos de proteção das informações contra ameaças à sua disponibilidade, integridade e confidencialidade, de modo a se evitar riscos e vulnerabilidades, visando preservar a sua estrutura e assegurar a continuidade dos negócios.

Segundo o Congresso de Segurança da Informação, Auditoria e Governança (2012) *Compliance* é fazer valer as políticas estabelecidas pela empresa. É o conjunto de disciplinas para que sejam cumpridas as normas legais e as diretrizes de negócio da instituição, ou definidas internacionalmente, principalmente para a área de segurança da informação.

2.6 Os benefícios do programa de *compliance* para as organizações.

A inserção do *Compliance* como ferramenta que visa à segurança, legalidade e a padronização dos processos foi percebida como uma evolução que seria latente e cíclica nas empresas, adquiriu base técnica e científica para fundamentar transformações que iriam além da teoria, e que seriam agentes transformadores e pioneiros da segurança das informações, a fim de garantir o controle, treinamento e adequação dos processos para assegurar o respaldo legal e empresarial.

De acordo com a Federação Brasileira de Bancos (2010), o programa *Compliance* possui algumas funções. A inserção do programa propõe benefícios mensuráveis e sólidos e visa proporcionar a melhoria contínua das empresas, sendo explicitados em:

2.6.1 Prevenção de Riscos

De acordo com a Associação Brasileiras de Normas Técnicas NBR ISO/IEC 17799:2005 o risco é a combinação da probabilidade de um evento e de suas consequências, portanto a inserção do *Compliance* nas organizações possibilita a otimização estrutural com ações preventivas que projetam o risco e trabalham para minimizá-lo e colocá-lo na menor dimensão possível.

São inúmeros os riscos a que as empresas estão expostas, riscos tecnológicos, financeiros, documentais, informativos, operacionais, dentre outros. Sendo assim o fluxo e o gerenciamento dos processos devem acontecer de forma ordenada a fim de se obter as avaliações com base em probabilidades ou impactos e transformá-los em soluções que promovam a seguridade do sistema e da estrutura corporativa, através da análise dos eventos identificam-se os impactos ou probabilidades e posteriormente definem-se critérios para a identificação do grau de sua importância dentro da organização, identificado quais são os impactos são definidas as medidas necessárias para se extinguir os riscos que porventura prejudiquem a organização e toda a sua cadeia.

2.6.2 Os benefícios da segurança da informação para as organizações

Segundo a NBR ISO/IEC 17799 (2005) a segurança da informação é importante tanto no setor público como no setor privado, manter a segurança das informações de uma empresa é essencial principalmente pelo fato de assegurar a competitividade, atender aos requisitos legais e também pela imagem da empresa junto ao mercado. A segurança das informações é obtida através de processos, políticas de informação, programas de *compliance*, procedimentos, estruturas organizacionais e funções de software e hardware.

> Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. (Associação Brasileiras de Normas Técnicas ISO/IEC 17799, 2005, p. 10).

Para Sawyer (2012) as ameaças internas ocorrem principalmente pelo fato de que a Tecnologia da Informação tende a focar a segurança contra-ataques externos, e com isso a rede se torna mais vulnerável a ataques internos. Em pesquisa, Sawyer aponta que a grande maioria dos ataques maliciosos internos é causado por funcionários insatisfeitos que planejam deixar a empresa, ou pensam que perderão seu emprego por algum motivo, com isso, Este mesmo autor define que existem 3 (três) camadas alvo para lidar com ameaças internas, são elas; rede, dispositivo host e as pessoas, neste caso, os funcionários. Na camada de rede, deve-se analisar todo o tráfego da rede, visando detectar e evitar a transmissão de dados sigilosos. Para a proteção em host devem ser usados softwares como um anti-maware, criptografia de dados e até mesmo, se for o caso, uma mudança de gestão e de controles de segurança

2.6.3 Vulnerabilidades as quais as organizações estão expostas por não implantarem o programa *Compliance*

Existem vários riscos aos quais as organizações estão expostas por não estar em *compliance*, dentre os riscos, o não cumprimento de normas aplicáveis à organização é passível de várias sanções como as previstas na lei anticorrupção brasileiras - 12.846/2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Existem também riscos operacionais, riscos a imagem dentre outros que podem comprometer a efetividade de uma organização. Esses riscos podem variar de acordo com o tipo de atividade, porte da empresa e peculiaridades que cada organização traz.

2.6.4 Vulnerabilidades as quais as organizações estão expostas por não garantirem a segurança da informação

Escândalos advindos de empresas em todo o mundo estão levando cada vez mais as organizações a investirem na segurança da informação. As informações são peças fundamentais para as organizações principalmente para as tomadas de decisões, e manter sua segurança é de extrema importância para garantir a efetividade de qualquer negócio.
Segundo Carvalho (2003) os riscos à segurança da informação podem ser classificados em três tipos:

- **Acesso não autorizado**: Descoberta da informação de um dado utilizador, que é posteriormente utilizada por outro para aceder aos recursos disponíveis ao primeiro.

- **Ataques por imitação:** consistem em fazer que um dado utilizador ou sistema se comporte como outro, para a obtenção de informação, recursos críticos ou perturbação do funcionamento de serviços.
- **Negação de serviços:** (Denial of Service), é uma forma bastante freqüente de ataque, cujo objetivo é a interrupção ou perturbação de um serviço, devido a danos (físicos ou lógicos) causados nos sistemas que o suportam.

Contudo as desproteções da informação podem trazer prejuízos incalculáveis para as organizações, haja vista que podem aumentar os riscos de efetividade do negócio, denegrir a imagem reputacional da marca, aumentar desvantagens em relação à concorrência, ocasionar fraudes, exposições, dentre outros.

3 METODOLOGIA

Para a produção deste estudo, inicialmente, foi definida a natureza da pesquisa. Neste caso, foi adotada a metodologia da pesquisa exploratória com abordagem qualitativa, pretendendo-se investigar se o programa *Compliance* pode garantir a seguridade das informações na organização SiderMax. Assim, trata-se de investigar questões subjetivas, relevantes para a pesquisa, com ênfase para a dimensão cotidiana que o fenômeno ocupa.

Segundo Selltiz, Jahoda, Deutsch e Cook (1967, p.63), "uma pesquisa pode ser considerada de natureza exploratória, quando esta envolver levantamento bibliográfico, entrevistas com pessoas que tiveram, ou têm, experiências práticas com o problema pesquisado e análise de exemplos que estimulem a compreensão. As pesquisas exploratórias visam proporcionar uma visão geral de um determinado fato, do tipo aproximativo". A pesquisa exploratória pode também avaliar quais teorias ou conceitos existentes podem ser aplicados a um determinado problema ou se novas teorias e conceitos devem ser desenvolvidos. Babbie (1986) resume as finalidades da pesquisa exploratória dizendo:

> Estudos exploratórios são tipicamente terminados para três propósitos: (1) simplesmente satisfazer a curiosidade e desejo do investigador para melhor compreensão, (2) testar a viabilidade de empreender um estudo mais cuidadoso, e (3) desenvolver os métodos a ser empregados em um estudo mais cuidadoso. O estudo exploratório pode ajudar a resolver algumas dificuldades em pesquisa. (Babbie, p.72, 1986)

A escolha da unidade de análise recaiu sobre uma organização SiderMax do ramo siderúrgico no município de Contagem/MG.

Para a unidade de observação foram selecionados 10 integrantes funcionários desta organização, baseando-se no julgamento do pesquisador e de acordo com os objetivos da

pesquisa, A coleta de dados se deu a partir da elaboração do roteiro de pesquisa contendo doze questões abertas, referenciadas pela vivência dos funcionários com o programa de *compliance*, descreveu-se a caracterização dos entrevistados como: gênero, estado civil, tempo de empresa e cargo; a análise de dados objetivou relacionar os objetivos gerais e específicos para então respondermos ao problema de pesquisa.

O instrumento utilizado para o tratamento dos dados foi o roteiro de entrevista, contendo as doze questões respondidas pelos funcionários da organização SiderMax. Sendo assim, o paradigma que orientou tanto a coleta, quanto a análise dos dados foi o fenomenológico, segundo a análise de seu conteúdo. Assim, para Bardin (1977) a análise de conteúdo é um conjunto de instrumentos metodológicos cada vez mais sutis em constante aperfeiçoamento, que se aplicam aos discursos (conteúdos e continentes) extremamente diversificados. O fator comum destas técnicas múltiplas e multiplicadas – desde o cálculo de frequências que fornece dados cifrados, até à extração de estruturas traduzíveis em modelos – é uma hermenêutica controlada, baseada na dedução: a inferência. (BARDIN, 1977).

4DISCUSSÃO DOS RESULTADOS DA PESQUISA

A presente seção tem como objetivo realizar uma discussão sobre os resultados de acordo com os objetivos propostos no referencial teórico.

Para responder o primeiro objetivo especifico - descrever os parâmetros do sistema de *Compliance* para a segurança das informações nas organizações – apresentam-se as categorias que designam os entrevistados, assim exposta: na primeira coluna são apresentados os códigos dos respectivos entrevistados, na segunda coluna os parâmetros do sistema de *Compliance* para a segurança das informações nas organizações.

De acordo com os resultados, nota-se que há uma semelhança entre as respostas dos entrevistados para os parâmetros, levando em consideração a importância para o sistema. A maioria dos entrevistados levou em consideração ser importante o código de conduta, as políticas da organização e as frequentes auditorias, como as idéias de Almeida (2015) onde cita que o *Compliance* compreende-se o conjunto de práticas e disciplinas adotadas pelas pessoas jurídicas no intuito de alinhar o seu comportamento coorporativo à observância das normas legais e das políticas governamentais aplicáveis ao setor de atuação, prevenindo e detectando ilícitos, a partir da criação de estruturas internas e procedimentos de integridade, auditoria e incentivos à comunicação de irregularidades, que forneçam um diagnóstico e elaborem um prognóstico das condutas e de seus colaboradores, com a aplicação efetiva de códigos de ética no respectivo âmbito interno.

A Federação Brasileira de Bancos (2010) ainda reforça que o *Compliance* executa as atividades de forma rotineira e permanente, monitorando-as para assegurar, de maneira corporativa e tempestiva, que as diversas unidades da instituição estejam respeitando as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para prevenção e controle dos riscos envolvidos em cada atividade.

Em relação ao segundo objetivo proposto – identificar os aspectos positivos da implantação do programa *Compliance* para garantir a segurança das informações – os resultados visam à vantagem competitiva como melhor benefício para a organização mediante o mercado. De acordo com Conselho Administrativo de Defesa Econômica (2016), ações afirmativas de incentivo à conformidade com a lei são parte essencial de uma cultura de ética nos negócios, que resulta em benefícios para a reputação da organização e sua atratividade para fins promocionais, de recrutamento e de retenção de colaboradores. Essas ações tendem a aumentar a satisfação e o comprometimento no trabalho e o senso de pertencimento e

identificação com o grupo. O comprometimento com a observância das leis também inspira confiança em investidores, parceiros comerciais, clientes e consumidores que valorizam organizações que operam de forma ética e que se sentiriam enganados em caso de infração.

Em relação ao terceiro objetivo especifico proposto - verificar as quais vulnerabilidades as organizações estão expostas por não implantarem o programa *Compliance* e por não garantirem a segurança das informações – apresenta os riscos que a empresa está exposta caso não implantasse o programa *Compliance*.

Sobre os resultados apresentados os entrevistados acreditam que a imagem da empresa está em risco, levando em consideração a confiabilidade, a competitividade, o envolvimento em atos ilícitos que possam ser levados a mídia entre outros. Para Scott citado por AMCHAM Brasil (2012), a reputação organizacional de uma empresa pode ser seriamente comprometida ao ficar exposta a situações adversas provenientes de uma má gestão de riscos, ocasionando então falta de credibilidade, fato que Scott julga como principal risco. “Todos os outros riscos (operacionais, legais etc.) geram o reputacional. No final, se você não está seguindo a lei, é o seu nome que vai para o mercado. Portanto, é a sua reputação que está sendo destruída pelo risco”, afirma Scott.
Reforça Cunha (2016) quando se chegam ao ponto de auditorias externas, órgãos reguladores, órgãos de controle ou, na pior das hipóteses, autoridades policiais e judiciais, tomarem a iniciativa para detectar e mitigar danos ao negócio, sem qualquer dúvida, todos os mecanismos internos de defesa falharam ou sequer foram utilizados

5 CONSIDERAÇÕES FINAIS, IMPLICAÇÕES, LIMITAÇÕES E SUGESTÕES PARA FUTURAS PESQUISAS

5.1Considerações finais

Os estudos feitos no referencial bibliográfico e pesquisa exploratória apontam que o Compliance, de fato é uma boa ferramenta de mitigação de riscos e com certeza auxilia na proteção das informações. Os colaboradores entrevistados na empresa SiderMax do ramo siderúrgico em Contagem reconhecem o Compliance como uma boa ferramenta de controle e mitigação de riscos relacionados à segurança da informação. Com base em suas respostas é possível notar que a existência do programa na organização lhes passa a sensação de segurança, em função de observarem que as atividades de Compliance cuidam para que os funcionários sejam treinados e preparados para fazer suas funções com a segurança de se estar fazendo o certo, além de garantir o monitoramento do cumprimento das leis, normas e procedimentos para que os estímulos para se cometer atos inaceitáveis eticamente ou ilícitos sejam sempre reprimidos, tornando o ambiente mais seguro e propenso às boas práticas.

As análises também indicam que o os colaboradores acreditam que caso não houvesse um programa de Compliance implantado na organização, os processos e atividades da empresa provavelmente não estariam operando no mesmo nível, e o ambiente seguro anteriormente citado daria lugar a outro, que aumentaria o nível de exposição da informação ao risco e não reprimiria práticas questionáveis com o mesmo rigor, e a desatenção a esses preceitos certamente aumentaria os riscos legais à imagem da empresa.

Assim, após identificarmos que o programa de compliance é uma base para as empresas, mas não garante totalmente a proteção das informações nas organizações, deveria estar sempre atrelado a medidas efetivas de segurança para abrandar os riscos, como um sistema de TI, que pode se encarregar das atividades rotineiras de nível operacional da **segurança de informações** digitais, enquanto a equipe interna de SI se concentra nas estratégias de apoio aos programas de governança, por exemplo. Assim, as empresas podem

conseguir efeitos muito mais satisfatórios, estando adequadas as normas, leis, procedimentos e com a garantia que suas informações estão sendo tratadas corretamente e protegidas. A partir daí, sim, as companhias podem se considerar seguras de verdade.

5.2Implicações

Os resultados da pesquisa trazem contribuições tanto para a academia quanto para o âmbito empresarial e também para os profissionais de Compliance. Na vertente acadêmica, a pesquisa contribui para aumentar a disponibilidade de estudos que discutam a implementação do programa Compliance em uma organização.

No âmbito empresarial e para os profissionais de Compliance, demostra que o Compliance é uma ferramenta que fornece uma base quando se trata de prevenção de riscos para a segurança das informações, o que possibilita o desenvolvimento de uma boa estratégia empresarial para prever, e assim mitigar da melhor maneira, possíveis ameaças relacionadas à segurança das informações.

Por fim, espera-se despertar a atenção para o tema tanto na área acadêmica brasileira como nas organizações que hoje começam a valorizar o programa Compliance como mitigador de riscos e tentam se resguardar cada vez mais com relação ao vazamento de informações.

5.3Limitações da pesquisa

A presente pesquisa apresenta algumas limitações pelo que investigações futuras neste tema deverão ser conduzidas. O caráter exploratório da pesquisa se enquadra ao permitir baixo poder de generalização, limitando os resultados encontrados ao contexto de uma organização em questão.

Outra limitação é que todos os dez entrevistados são gestores que ocupam cargos de grande importância dentro da organização SiderMax e o contato com eles fora dificultado devido a disponibilidade limitada para responder ao questionário aplicado.

Também pode se citar a disponibilidade limitada por parte dos integrantes do grupo para aplicação da pesquisa, já que todos dispõem de pouco tempo disponíveis, levando em conta que todos os integrantes possuem compromisso profissional e compromisso acadêmico.

5.4Sugestões para futuras pesquisas

A realização da pesquisa identificou algumas possibilidades para estudos futuros. Em primeiro lugar e relacionado com as limitações apresentadas anteriormente, propõe-se a aplicação do roteiro de entrevistas a outras organizações, com o intuito de abranger um maior número de empresas de setores diferentes no mercado.

Outra pesquisa que poderia ser realizada refere-se à sua natureza. Acreditamos que novas pesquisas possam trazer novos e importantes resultados, já que se nota que o programa Compliance ainda é um tema pouco abordado em muitas organizações.

Sugerimos também estudos abordando o Compliance em outras áreas das organizações, já que é uma ferramenta importante não só para a mitigação de riscos quanto a informações sigilosas, mas também contribui para a conformidade de outros setores das organizações.

Sugerem-se também pesquisas em continuidade a esta, buscando disponibilizar ainda mais informações sobre o Compliance como ferramenta estratégica para segurança das informações nas organizações.

REFERÊNCIAS:

AMARAL, H. L. do.; "Compliance na Lei Anticorrupção: Uma Análise da Aplicação Prática do Art. 7º, VIII, Da Lei 12.846/2013". Boletim JURÍDICO - 2015. Disponível em: <http://www.boletimjuridico.com.br/m/texto.asp?id=3969>. Acesso em: 06 set. 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT. **ISO/IEC 17799**. 2005. Disponível em: <http://www.cienciianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf>. Acesso em: 07 set. 2016.

BARDIN, Laurence. **Análise de conteúdo**. Lisboa: 70, 1977.

BITTENCOURT, S.; **Comentários à Lei Anticorrupção: Lei 12.846/ 2013**. REVISTA DE DOUTRINA DA 4ª REGIÃO PUBLICAÇÃO DA ESCOLA DA MAGISTRATURA DO TRF DA 4ª REGIÃO – EMAGIS, ago. 2015.

CAMARGO, Rodrigo Oliveira de. **Compliance, Controle da Atividade Empresarial e da Prevenção do Delito**. 2016. Disponível em: <http://www.lecnews.com/web/compliance-controle-de-riscos-da-atividade-empresarial-e-de-prevencao-do-delito/>. Acesso em: 07 set. 2016.

CARVALHO, D. R. de.; **Segurança da Informação: Estudo de Caso da Aplicação da Norma NBR ISO/IEC 17799**. Faculdade de Ciências da Computação – UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS – UNIPAC, 2003.

COMPLIANCE BRASIL, Instituto. **Segurança da Informação e Compliance**. 2015. Disponível em: <http://compliancebrasil.org/seguranca-da-informacao-e-compliance/>. Acesso em: 09 set. 2016.

CONGRESSO DA SEGURANÇA DA INFORMAÇÃO, AUDITORIA E GOVERNANÇA, CSIAG. **Compliance Pode Trazer Segurança para a Empresa?** 2012. Disponível em: <http://www.cnasi.com.br/compliance-pode-trazer-seguranca-para-a-empresa/>. Acesso em: 09 set. 2016.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA, CADE. **Guia: Programas de Compliance**. 2015. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf>. Acesso em: 09 set. 2016.

CORDEIRO, L.; **Informação: um estudo exploratório do conceito em periódicos científicos brasileiros da área de Ciência da Informação**. Universidade Estadual Paulista Faculdade de Filosofia e Ciências Campus de Marília Programa de Pós Graduação em Ciência da Informação, 2005.

CUNHA, Matheus. **Quanto Vale a Confiança?** 2016. Disponível em: <http://www.lecnews.com/web/quanto-vale-a-confianca/>. Acesso em: 09 set. 2016.

FEDERAÇÃO BRASILEIRA DE BANCOS, FEBRABAN. **Função de Compliance**. 2010. Disponível em: <http://www.febraban.org.br/Arquivo/Destaques/Funcao_de_Compliance.pdf>. Acesso em: 02 out. 2016.

FREIRE, Débora. **Histórico de Compliance**. 2016. Disponível em: <http://www.academia.edu/19819682/Hist%C3%B3rico_da_Compliance >. Acesso em: 02 out. 2016.

KPMG, Cutting Through Complexity. **Pesquisa: Maturidade do Compliance no Brasil**. 2015. Disponível em: <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2015/09/pesquisa-comnpliance-brasil-2015.pdf>. Acesso em: 03 out. 2016.

LANCASTER, F. W. O currículo da Ciência da Informação. Revista de Biblioteconomia de Brasília, Brasília, v. 17, n.1, p. 01-05, jan./jun. 1989

LEAL, R. G.; FOCKINK, C.; **A previsão dos Mecanismos e Procedimentos Internos de Integridade: Compliance Corporativo na Lei Anticorrupção: Sua Importância Considerado Como Uma Mudança de Paradigmas e Educação Empresarial.** Universidade de Santa Cruz do Sul – UNISC – Brasil, 2014

LEGAL ETHICS COMPLIANCE, LEC. **Segurança da Informação e Compliance**. 2016. Disponível em: <http://www.lecnews.com/web/seguranca-da-informacao-e-compliance/>. Acesso em: 04 out. 2016.

GIN, C. de M.; OLIVEIRA, C. M. de.; **Lei anticorrupção Brasileira: Praticas de Compliance Aliadas ao Cadastro Nacional de Empresas Punidas. XI SEMINÁRIO NACIONAL DE DEMANDAS NACIONAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA – I MOSTRA NACIONAL DE TRABALHOS CIENTÍFICOS,** 2015.

NEVES, Stüssi. **Compliance no Brasil e a Lei 12.846/13**. 2013. Disponível em: <http://www.advantageaustria.org/br/events/8-CharlesWowk-Compliance.pdf>. Acesso em: 07 out. 2016.

NETO, E. M. A..; "Combate à Corrupção: Uma Análise do Acordo de Leniência e do Programa de Compliance na Lei Nº 12.846/2013".Faculdade de Direito, Universidade de Brasília - 2015..

ROCHA, D. L.; SILVA, R. M. S.; **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001**. Universidade do Porto, Faculdade de Engenharia – FEUP, Dezembro/2012

RODRIGUES, J.R. **EUA obriga Brasil a Cumprir a Lei Anticorrupção**. 2014. Disponível em: <http://www.fatoreal.blog.br/politica/eua-obriga-brasil-cumprir-lei-anticorrupcao/>. Acesso em: 09 out. 2016.

SAWYER, J. H.; **Como Prevenir Vazamento de Dados na Sua Organização**. 2012. Disponível em: <http://itforum365.com.br/noticias/detalhe/3624/como-prevenir-vazamento-de-dados-em-sua-organizacao>. Acesso em: 28 out. 2016.

SELLTIZ, C.; JAHODA, M.; DEUTSCH, M.; COOK, S. **"Alguns problemas gerais de mensuração" in Métodos de Pesquisa nas Relações Sociais.** S. Paulo, Ed. Herder e Editora, da Universidade de São Paulo, 1967, pp.163-222.

SPINETTO, Juan Pablo. **Após escândalos, Compliance é a nova palavra de ordem no Brasil**. 2015. Disponível em: <http://economia.uol.com.br/noticias/bloomberg/2015/01/20/apos-escandalos-compliance-e-a-nova-palavra-de-ordem-no-brasil.htm>. Acesso em: 01 out. 2016.

VIEIRA, M. P.: **Compliance: Ferramenta Estratégica Para Uma Boa Pratica de Gestão**. Universidade Federal de Viçosa Viçosa – MG 2013

.

Conteúdo da primeira página do arquivo:

- ✓ *Template* (obrigatório - Todas as páginas do artigo deverão conter o template)
- ✓ Título
- ✓ Resumo
- ✓ Palavras-chave
- ✓ Abstract
- ✓ Keywords

A introdução deverá iniciar na segunda página do arquivo.

Atenção:

- O uso do template é obrigatório. Este modelo já possui a formatação solicitada pelo congresso. Utilize-o para escrever o seu artigo.
- O Artigo Científico deve conter no mínimo 8 e no máximo 16 páginas (incluindo primeira página).

1 Introdução (os títulos das seções do artigo devem ser numerados, fonte Times New Roman, tamanho 12 e em negrito)

Texto justificado, fonte Times New Roman, corpo 12, espaçamento simples (entre linhas, palavras e caracteres). Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxx xxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxxxxx xxxxxxxxxxxxx xxxxxxxx xxxxxxxxxxxxxxxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxxxx xxxxxxxxx xxxxxxxxxxxxx xxxxxxxxxxxxxxxxx xxxxxxxxxx.

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxx xxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxxxxx xxxxxxxxxxxxx xxxxxxxx xxxxxxxxxxxxxxxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxxx xxxxxxxxxxxxxxxx xxxxxxxxx xxxxxxxxxxxxx xxxxxxxxxxxxxxxxx xxxxxxxxxx.

Para a parte textual do artigo (segunda página em diante), recomenda-se a seguinte estrutura:

- Introdução (contendo tema, problema de pesquisa e objetivos)
- Referencial Teórico
- Metodologia
- Análise dos resultados
- Conclusões/Considerações finais
- Referências