UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS
NÍVEL MESTRADO

KAREN HACKBART SOUZA FONTANA

ANÁLISE DAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO CONTÁBIL E SUA CONTRIBUIÇÃO PARA A GOVERNANÇA CORPORATIVA NO REQUISITO DE CONFORMIDADE

São Leopoldo
2017

Karen Hackbart Souza Fontana

ANÁLISE DAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO CONTÁBIL E SUA CONTRIBUIÇÃO PARA A GOVERNANÇA CORPORATIVA NO REQUISITO DE CONFORMIDADE

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Ciências Contábeis, pelo Programa de Pós-Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos - UNISINOS

Orientador: Prof. Dr. Tiago Wickstrom Alves

São Leopoldo

2017

F679a Fontana, Karen Hackbart Souza.
Análise das práticas de segurança da informação contábil e sua contribuição para a governança corporativa no requisito de conformidade / por Karen Hackbart Souza Fontana. – São Leopoldo, 2017.

193 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Ciências Contábeis, São Leopoldo, RS, 2017.
Orientação: Prof. Dr. Tiago Wickstrom Alves, Escola de Gestão e Negócios.

1.Contabilidade. 2.Divulgação de informações contábeis. 3.Sistemas de informação gerencial – Medidas de segurança. 4.Governança corporativa. I.Alves, Tiago Wickstrom. II.Título.

CDU 657
658.012.43

Catalogação na publicação:
Bibliotecária Carla Maria Goulart de Moraes – CRB 10/1252

Karen Hackbart Souza Fontana

ANÁLISE DAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO CONTÁBIL E SUA CONTRIBUIÇÃO PARA A GOVERNANÇA CORPORATIVA NO REQUISITO DE CONFORMIDADE

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Ciências Contábeis, pelo Programa de Pós-Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos - UNISINOS

Aprovado em 15 de março de 2017.

BANCA EXAMINADORA

Profª. Dra. Amarolinda Iara da Costa Zanela Klein – UNISINOS

Prof. Dr. Ernani Ott – UNISINOS

Prof. Dr. Norberto Hoppen – UNISINOS

À minha filha Mariana e meu esposo Cleber:
vocês são a minha inspiração.
Dedico à vocês com muito amor e gratidão!

AGRADECIMENTOS

Primeiramente agradeço a Deus pela vida, pela saúde, por oportunizar este momento. Agradeço a Ele por permitir que os desafios fossem superados, tornando-me mais forte para seguir adiante.

Agradeço ao meu esposo Cleber, meu companheiro, meu amigo. Muito obrigada por estar ao meu lado em todos os momentos, principalmente naqueles mais difíceis! Obrigada meu amor pela paciência, compreensão, amor e apoio para a realização do meu sonho que se tornou seu também. Obrigada pelos lanchinhos, por cuidar de mim enquanto eu estava horas em frente ao computador pesquisando, escrevendo... Te amo meu amor!

Agradeço a pequena Mariana, minha filha. A mamãe pede desculpas pela ausência e por não ter brincado tanto como você gostaria. Hoje você fala para seus amiguinhos que a mamãe é “a professora dos adultos” e eu fico toda orgulhosa. Te amo minha florzinha!

Agradeço aos meus pais Kira e Luiz Juelci, vocês sempre incentivaram os meus estudos e apoiaram as minhas escolhas. Vocês são o meu exemplo de caráter, honestidade e humildade. Meu pai, você se foi tão de repente....sinto tanta saudade! Tenho certeza que estás bem, junto com o mano Daniel. Amo vocês!

Agradeço ao meu irmão caçula Michel pela força, pelo incentivo, pela palavra amiga, já passamos por muitos momentos difíceis e juntos superamos todos eles. Estamos e estaremos sempre juntos. Te amo!

Agradeço a minha vó Selma, que com seus 91 anos me enche de orgulho e alegria. Te amo vovozinha!

Agradeço ao professor Dr. Adolfo Alberto Vanti pela paciência, dedicação e por transmitir o seu conhecimento, me indicando o caminho a seguir. Aos demais professores do PPGCC, obrigada pelos ensinamentos e críticas construtivas durante este curso.

Agradeço a minha amiga Geruza, grande presente que o mestrado me deu, muito obrigada pela parceria, pelo incentivo e por muitas vezes apenas me ouvir.

Agradeço a minha amiga Cristina pela amizade e por estar sempre disponível. Sou grata também a todos os respondentes da minha pesquisa.

Muito obrigada a todos, vocês são pessoas especiais!

RESUMO

Esta pesquisa teve como objetivo analisar como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade. Trata-se de uma pesquisa descritiva, qualitativa cuja estratégia de pesquisa deu-se mediante um estudo de caso único, realizado em uma empresa localizada no Rio Grande do Sul que está listada no Nível 2 de Governança Corporativa. Como técnicas de coleta de dados, utilizou-se entrevistas em profundidade, documentos e questionário. Aplicou-se o questionário aos usuários de nível operacional e gerencial para os setores de contabilidade, custos, fiscal, financeiro e tecnologia da informação. Por meio desse instrumento identificou-se que as práticas de segurança da informação contábil apresentam um nível razoável de proteção; apenas domínios D3 com D4; D4 com D2; D7 com D8 possuem correlação forte e são estatisticamente significantes ao nível de 1%. Para aprofundar a pesquisa, verificou-se por meio de entrevistas com os gestores que a empresa utiliza 27 das 41 práticas apresentadas nesse estudo. Conclui-se que as práticas utilizadas contribuem para a conformidade da governança corporativa proporcionando uma informação acessível, conforme, confiável, disponível, íntegra, responsável, válida, segura, bem como na mitigação de riscos. Em complemento, verificou-se na análise documental que a empresa possui políticas de segurança da informação, bem como não teve ressalvas da auditoria independente no período analisado.

Palavras-chave: Segurança da Informação. Informação Contábil. Governança Corporativa. Conformidade.

ABSTRACT

This research had as objective to analyze security practices of accounting information can contribute to the corporate governance compliance requirement. It is a descriptive, qualitative research whose research strategy was by a single case study, carried out in a company located in Rio Grande do Sul that is listed at level 2 of corporate governance. As data collection techniques, using in-depth interviews, documents and questionnaire. The questionnaire was applied to managerial and operational level users for accounting, tax, financial costs, and information technology. Through this instrument identified that the accounting information security practices have a reasonable level of protection; only domains with D3 D4; D4 with D2; D7 with D8 have strong correlation and are statistically significant at the 1% level. For further research, it was found through interviews with managers the company uses 27 of 41 practices presented in this study. It is concluded that the practices contribute to compliance of corporate governance by providing accessible information, as available, reliable, responsible, valid, safe, as well as on risk mitigation. In addition, it was found in the documentary analysis that the company has information security policies, as well as the independent audit had caveats analysis period.

Key-words: Information Security. Accounting Informationl. Corporate Governance. Compliance.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BIS	Bank for International Settlements
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
BP	Balanço Patrimonial
CFC	Conselho Federal de Contabilidade
CPC	Comitê de Pronunciamentos Contábeis
CVM	Comissão de Valores Mobiliários
DRE	Demonstração do Resultado do Exercício
FASB	Financial Accounting Standards Board
GC	Governança Corporativa
IASB	International Accounting Standards Board
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NBR	Normas Brasileiras de Regulação
OECD	Organisation for Economics Cooperation and Development
SAP	Systems Applications and Products in Data Processing
SEC	Security and Exchange Commission
SOX	Sarbanes-Oxley
SPSS	Statistical Package for Social Science
VSM	Value Stream Mapping Software

SUMÁRIO

1 INTRODUÇÃO

A governança corporativa compreende orientações e métodos sob os quais as empresas são governadas. Permite a empresa operar com mais competência, diminuir o risco, oferecer proteção para as limitações de gestão, a fim de apoiar seu o crescimento. (YOUSUF; ISLAM, 2015). Essa temática ganhou crescente atenção nos últimos anos devido aos escândalos contábeis que introduziram uma crise de confiança na prática de emissão de relatórios financeiros. (MATEESCU, 2015; BHASIN, 2016).

No intuito de proteger os acionistas há um conjunto de princípios de governança corporativa que, no Brasil, é sugerido pelo Instituto Brasileiro de Governança Corporativa. (IBGC, 2009). Dentre esses princípios, a conformidade (*compliance*) é destacada devido ao fortalecimento do respeito às normas e políticas, bem como a mitigação de riscos. (OLIVEIRA *et al.*, 2015).

A conformidade pode ser definida como a obediência às leis e normas que regulam o ambiente interno e externo (DEDONATO; BEUREN, 2010). Essa obediência, especificamente na área contábil, dá-se pela adoção dos padrões estipulados pelo *International Accounting Standards Board* (IASB). (JORISSEN, 2015; AZAD *et al*., 2016).

O processo de convergência às normas do IASB no Brasil, se dá por meio de pronunciamentos emitidos pelo Comitê de Pronunciamentos Contábeis (CPC) que orientam as práticas contábeis que originam as demonstrações contábeis, porém para estas serem úteis aos usuários devem possuir determinadas características qualitativas (HENDRIKSEN; VAN BREDA, 1999; RIBEIRO FILHO; LOPES; PEDERNEIRAS, 2009; IUDÍCIBUS, 2010; CPC 00 R1, 2011). De acordo com Hendriksen e Van Breda (1999, p. 95) “as características qualitativas da informação contábil são definidas como sendo as propriedades da informação que são necessárias para torná-la útil”.

Este estudo trata das práticas de segurança da informação, das características qualitativas da informação contábil e da governança corporativa.

Neste sentido, destacam-se os estudos recentes que investigaram as características qualitativas das demonstrações contábeis por meio de métricas sob a ótica de especialistas contábeis (BARBOSA *et al.*, 2015), estágios de ciclo de vida das companhias listadas na BM&FBovespa (LIMA *et al.*, 2015), atributos da

contabilidade gerencial no setor de energia elétrica (SOUZA *et al.*, 2015), normas contábeis e qualidade das informações prestadas (JORISSEN *et al.*, 2015).

Sendo assim, verifica-se que as informações são essenciais para o negócio de uma organização, portanto recomenda-se que sejam protegidas. (SÊMOLA, 2014). A segurança da informação é uma das principais preocupações da gestão organizacional (MONTESDIOCA; MAÇADA, 2015), e pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (SÊMOLA, 2014).

Desta forma, para que os objetivos de segurança da informação (DHILLON; BACKHOUSE, 2000; ALBERTIN; PINOCHET, 2010; BULGURCU; CAVUSOGRU; BENBASAT, 2010; SÊMOLA, 2014; UDDIN; PRESTON, 2015) sejam atendidos adotam-se práticas que relacionam as tecnologias de segurança (uso de *software* e outros recursos) e o comportamento do usuário (efetuam-se ações preventivas para o uso seguro do computador). (RHEE; KIM; RYU, 2009; BULGURCU; CAVUSOGLU; BENBASAT, 2010*;* SÊMOLA, 2014, MONTESDIOCA; MAÇADA, 2015, PARSONS *et al.*, 2015; SAFA *et al.*, 2015).

Este trabalho está estruturado em cinco capítulos, iniciando por esta introdução, de forma a contextualizar o tema de pesquisa e após apresentam-se o problema de pesquisa, delimitação do tema, objetivos e justificativa do estudo. No segundo capítulo aborda-se o referencial teórico que contempla os temas: Governança Corporativa, Informação Contábil e Segurança da Informação. No terceiro capítulo, descreve-se a metodologia da pesquisa, sua classificação, procedimentos de coleta de dados, tratamento, análise de dados e o caso estudado, o qual se refere a um estudo de caso único em uma indústria metalúrgica de capital aberto.

No quarto capítulo apresentam-se os resultados e a análise dos resultados do caso estudado, com o intuito de cumprir os objetivos da pesquisa e responder a questão de pesquisa. No quinto capítulo, apresentam-se as considerações finais do estudo, bem como sugestões para pesquisas futuras, incluindo as limitações desta pesquisa. Por fim, listam-se referências utilizadas para fundamentar esta pesquisa.

1.1 DEFINIÇÃO DO PROBLEMA

A governança corporativa no princípio de conformidade pode existir em vários locais funcionais e para cada local há vantagens e limitações, pois exige a transparência e harmonia com os padrões éticos. (GERARD; WEBER, 2015). Possui uma variedade de abordagens e relaciona-se com diversas áreas, inclusive com a contabilidade. (MATEESCU, 2015).

Na contabilidade, a informação é essencial à tomada de decisão deve possuir determinadas características qualitativas, as quais são definidas como as propriedades necessárias para tornar a informação útil (HENDRIKSEN; VAN BREDA, 1999; RIBEIRO FILHO; LOPES; PEDERNEIRAS, 2009; IUDÍCIBUS, 2010; CPC 00 R1, 2011), porém estudos recentes revelaram dificuldades de evidenciá-las. (BARBOSA *et al*., 2015; SOUZA *et al.*, 2015; LIMA *et al.*, 2015; JORISSEN, 2015; KLANN; BEUREN, 2015).

No estudo de Barbosa *et al.* (2015) houve dificuldade de encontrar fatores para representar a compreensibilidade e a materialidade, bem como a falta de construtos relacionados à tempestividade. Referente à tempestividade das informações, o estudo de Souza *et al.* (2015) revelou que os gestores das empresas possuem necessidade de obter informações em tempo hábil, porém são obtidas com pouca frequência.

A pesquisa de Lima *et al.* (2015) sugere que o ciclo de vida explica parcialmente o comportamento da qualidade das informações contábeis. Os autores encontraram evidências de que a qualidade das informações contábeis variou de acordo com os estágios de ciclo de vida das empresas brasileiras no período de 1995 a 2011.

Klann e Beuren (2015) enfatizam que a convergência às normas internacionais não é suficiente para obter a melhoria da qualidade da informação contábil. É preciso adequação à legislação, boas práticas de governança corporativa, treinamento de profissionais para utilizarem o conjunto de normas contábeis de forma competente e, investimento na proteção aos investidores.

No sentido de proteger as informações evidencia-se o conceito de segurança da informação. (ALBERTIN; PINOCHET, 2010). A segurança da informação pode ser afetada pela qualidade da informação influenciada pelo usuário, como por exemplo, *inputs* destas no sistema de informação. (SCHNEIDER *et al.*, 2014). Desta

forma, a tecnologia unicamente não pode garantir um ambiente seguro, os usuários intencionalmente ou por negligência são considerados como uma ameaça. (RHEE; KIM; RYU, 2009; BULGURCU; CAVUSOGLU; BENBASAT, 2010; MONTESDIOCA; MAÇADA, 2015; PARSONS *et al.*, 2015; SAFA *et al*., 2015).

Sendo assim, nota-se que há vários estudos que tratam de forma isolada os temas segurança da informação, características qualitativas da informação contábil e governança corporativa. A presente pesquisa busca a junção destes temas, acredita-se que as práticas de segurança da informação podem estar relacionadas às características qualitativas das informações contábeis, pois ambas dependem do comportamento dos usuários internos e externos e, para mitigar os riscos e fortalecer o cumprimento às normas e políticas, evidencia-se o requisito de conformidade da governança corporativa.

Neste contexto surge o problema de pesquisa norteador desse estudo: como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade?

1.2 DELIMITAÇÕES DO TEMA

O tema está delimitado em âmbito da governança corporativa no requisito de conformidade. Portanto, não foram examinados os princípios de transparência, equidade, prestação de contas e responsabilidade corporativa.

Quanto ao tema Informação Contábil, investiga-se nesta pesquisa as características qualitativas das informações contábeis que são: comparabilidade, compreensibilidade, confiabilidade, consistência, disponibilidade, integridade, materialidade, neutralidade, oportunidade, preditiva, primazia da essência sobre a forma, prudência ou conservadorismo, relevância, representação fidedigna, tempestividade, uniformidade, utilidade e verificabilidade. Não foi objeto de estudo verificar a publicação das demonstrações contábeis no sentido de atendimento às Normas Brasileiras de Contabilidade, pois a organização em estudo é auditada por empresa de auditoria externa independente, e desta forma presume-se que suas demonstrações atendem as recomendações das normas.

No que se refere à segurança da informação, apesar de existirem outras normas que compõem a família da ISO/IEC 27000, nesta pesquisa utiliza-se a ISO/IEC 27002, pois ela estabelece um conjunto adequado de controles, políticas e

procedimentos de segurança da informação, com a finalidade de adoção de boas práticas. A ISO/IEC 27002 é utilizada para identificar a conformidade da segurança de informação, especificamente a seção 18 – Conformidade, cujos principais elementos são: (i) conformidade com requisitos legais e contratuais; (ii) análise crítica da segurança da informação.

O contexto de aplicação da pesquisa dá-se em uma indústria metalúrgica líder no mercado nacional que exporta para mais de oitenta países. Foi fundada em 1939 e localiza-se no estado do Rio Grande do Sul. Atualmente a empresa tem 775 funcionários, possui capital aberto com ações negociadas na bolsa de valores, onde os investidores acompanham a situação econômica e financeira da empresa por meio de informações trimestrais envidas a CVM e à BM&FBovespa.

1.3 OBJETIVOS

Neste capítulo, apresentam-se os objetivos geral e específicos do trabalho.

1.3.1 Objetivo Geral

O objetivo geral do estudo é analisar como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade.

1.3.2 Objetivos Específicos

Para alcance do objetivo principal, foram definidos os seguintes objetivos específicos:

a) identificar as recomendações teóricas de governança corporativa no requisito de conformidade, segurança da informação e características qualitativas da informação contábil;
b) verificar o nível de controle das práticas de segurança da informação dispostas na ISO/IEC 27002 (2013) no requisito de conformidade, relacionadas às características qualitativas da informação contábil e a conformidade da governança corporativa;
c) identificar as diferenças de percepção dos grupos operacional e gerencial;

d) avaliar qualitativamente se a empresa estudada adota as práticas de segurança da informação no requisito de conformidade da ISO/IEC 27002 (2013) relacionadas com as características qualitativas da informação contábil e conformidade da governança corporativa.

1.4 JUSTIFICATIVA

A literatura evidencia que a informação contábil para ser considerada útil e de qualidade deve apresentar determinadas características qualitativas. (HENDRIKSEN; VAN BREDA, 1999; RIBEIRO FILHO; LOPES; PEDERNEIRAS, 2009; IUDÍCIBUS, 2010; CPC 00 R1, 2011). Porém, estudos recentes evidenciam que há dificuldade de encontrar fatores que as representem (BARBOSA *et al.*, 2015), as informações são obtidas parcialmente (LIMA *et al.*, 2015) ou com pouca frequência (SOUZA *et al.*, 2015). Elas dependem das características do ambiente institucional que a empresa opera (JORISSEN; 2015) e a convergência às normas internacionais não é o suficiente para obter a melhoria da qualidade da informação contábil (KLANN; BEUREN, 2015). Desta forma, Souza *et al.* (2015, p. 228) recomendam pesquisas sobre o uso da contabilidade gerencial a fim de surgirem novas discussões sobre o tema.

A qualidade da informação pode ser influenciada por aspectos relacionados ao usuário, como por exemplo o curto prazo de tempo para divulgar as informações. A respeito disso, Schneider *et al.* (2014, p. 15) abordam que “para fornecer uma informação na época oportuna, pode ser necessário divulgá-la antes que todos os aspectos de uma transação ou evento sejam conhecidos, prejudicando assim sua confiabilidade”. Isto significa que os usuários intencionalmente ou por negligência são considerados uma ameaça à segurança da informação. (RHEE; KIM; RYU, 2009; BULGURCU; CAVUSOGLU; BENBASAT, 2010; MONTESDIOCA; MAÇADA, 2015; PARSONS *et al.*, 2015; SAFA *et al*., 2015).

De acordo com Uddin e Preston (2015) a tecnologia isoladamente não é suficiente para tornar a organização segura, são as pessoas, os processos e a TI que precisam trabalhar coerentemente para garantir um sistema de informação seguro. Os autores recomendam como pesquisa futura preencher a lacuna entre os

requisitos de segurança do fluxo de informação alinhando-os com o gerenciamento de acessos de uma organização.

Neste sentido, como proteção à segurança da informação têm-se as normas que representam um padrão estabelecido, um consenso de regras, princípios, leis, sobre características como, por exemplo: qualidade, segurança, confiabilidade e conformidade. Elas devem permanecer aplicáveis, documentadas e publicadas. (DISTERER; 2013).

A norma ISO/IEC 27002 (2013) trata especificamente sobre a segurança da informação e pode ser utilizada como documento de orientação para as organizações implementarem controles de segurança da informação. Essa norma pode ser aplicada a todas as organizações, independente do tipo e tamanho, e garante à direção e outras partes interessadas a proteção dos ativos contra danos, atuando como um facilitador dos negócios, motivos pelos quais optou-se por ela.

Diante deste contexto, no qual as empresas divulgam suas informações contábeis por meio de um sistema de informação, e este pode conter dados equivocados, prejudicando sua utilidade e qualidade, surge uma oportunidade de pesquisa.

Este trabalho procura atender a governança corporativa e refere-se à utilização das práticas de segurança da informação ISO/IEC 27002 seção 18 – Conformidade relacionadas aos conceitos de qualidade da informação contábil. Desta forma, torna-se relevante para o meio acadêmico e profissional, pois permite averiguar sua contribuição para a governança corporativa no requisito de conformidade.

A contribuição desta pesquisa dá-se por ampliar o estudo de Schneider *et al.* (2014) no sentido de analisar especificamente e de forma aprofundada a seção 18 - Conformidade da ISO/IEC 27002. Schneider *et al.* (2014) revelam que a conformidade da ISO/IEC 27002 possui controles mínimos para a regulamentação de controles de criptografia, conformidade com as políticas e normas de segurança da informação e à proteção de ferramentas de auditoria de sistemas de informação.

Procura-se expandir a pesquisa de Brum (2014) na temática de características qualitativas da informação contábil relacionando-as com as práticas de segurança da informação. O estudo de Brum (2014) identificou que a conformidade das informações tem base nos controles internos estabelecidos em

nível operacional, pois as ferramentas de tecnologia da informação não atendem plenamente o processo do negócio.

Foi proposta também nesta pesquisa, avaliar qualitativamente a contribuição da governança corporativa no requisito de conformidade, utilizando-se conjuntamente as temáticas de segurança da informação e características qualitativas da informação contábil. Desta forma, diferencia-se também do estudo de Darounco (2013) o qual objetivou a avaliação dos processos de controles internos e de TI. Como resultado Darounco (2013) revelou que os processos internos são mantidos diante das constantes auditorias e estão em nível de limitada maturidade.

Outra contribuição desta pesquisa é fornecer um modelo conceitual e suas respectivas análises, bem como um instrumento de pesquisa que relaciona os temas segurança da informação no requisito de conformidade com as características qualitativas das informações contábeis, agregando os conceitos da literatura e estudos empíricos.

2 REVISÃO DA LITERATURA

Neste capítulo apresenta-se o referencial teórico que fundamenta a questão problema definida anteriormente. O referencial teórico contempla os temas Governança Corporativa, Informação Contábil e Segurança de Informação.

2.1 GOVERNANÇA CORPORATIVA

A governança corporativa refere-se à qualidade, transparência, fiabilidade das relações entre os acionistas, conselho de administração, gestão e funcionários que definem a autoridade e a responsabilidade de cada um na entrega de valor sustentável para todos os *stakeholders*. (ADILOGLU; VURAN, 2012). Está direcionada por orientações e métodos pelos quais as empresas são governadas, o que lhes permite operar com mais competência, diminuir o risco, oferecer proteção contra a má gestão, a fim de apoiar o seu crescimento. (YOUSUF; ISLAM, 2015).

O principal objetivo da governança corporativa é maximizar o valor do acionista e proteger seu interesse (YOUSUF; ISLAM, 2015). Foi após o estudo acadêmico de Berle e Means em 1932 que a governança corporativa recebeu maior ênfase, considerado por muitos o marco inicial da governança corporativa. (SAITO; SILVEIRA, 2008).

Berle e Means (1984) afirmam que com o desenvolvimento das empresas e suas complexidades houve a necessidade de delegar o controle do proprietário para os administradores da organização. Os autores abordam os conflitos de interesses, os custos e benefícios da separação da propriedade e controle em empresas norte-americanas. Desta forma, a fragmentação fortalecia o poder dos gestores sendo favorável que agissem em próprio interesse e não no interesse dos acionistas.

O conflito de interesses foi tratado por Jensen e Mecking (1976) e refere-se, essencialmente, na divergência entre os proprietários (principal) e seus representantes (agentes), dando origem a Teoria da Agência. Para estes autores, a relação de agência é definida como um contrato em que o principal nomeia o agente para exercer algumas atividades. Quando há diferentes interesses nessa relação, ou seja, um conflito de interesses, diz-se que existe um problema de agência.

Para minimizar esses conflitos de interesse e devido aos escândalos corporativos que geraram uma crise de confiança na prática de emissão de relatórios financeiros (BHASIN, 2016) nos Estados Unidos, foram impostas às empresas determinadas exigências por meio da criação da lei *Sarbanes-Oxley* (SOX).

O objetivo da SOX foi de recuperar a credibilidade do mercado de capitais norte-americano, através da transparência das informações, permitindo auditorias preventivas pela *Security and Exchange Comission* (SEC). (SANTOS; LEMES, 2007).

No intuito de alinhar e monitorar as relações e interesses entre os gestores, conselho de administração, acionistas e demais *stakeholders* surge a *Organisation for Economic Cooperation and Development* (OECD, 2004) com vistas à definição dos objetivos da empresa e das melhores alternativas de monitoramento por meio de um conjunto de princípios de governança corporativa. No Brasil, esses princípios são abordados pelo Instituto Brasileiro de Governança Corporativa (IBGC, 2009).

A governança corporativa tem sido estudada por pesquisadores em todo o mundo e ganhou lugar especial na estratégia das empresas. (MATEESCU, 2015). Dentre os estudos atuais sobre a temática de governança corporativa, destacam-se os estudos relacionados com a remuneração de executivos (KANAPATHIPILLAI *et al.,* 2015; SOLER; MARIN, 2015; REDDY; ABIDIN; YOU, 2015), aspectos comportamentais como cultura organizacional (LU; WENCHANG, 2015), ética, liderança, responsabilidade social e confiança (OLIVEIRA *et al.*, 2015), fraudes corporativas (KHANNA; KIM; LU, 2015), assimetria de informação (CAI *et al*., 2015), evolução do valor das ações no mercado (Souza *et al*., 2015; Carlesso Neto *et al*., 2015; Santana *et al*., 2015), convergência às normas internacionais de contabilidade (MARTINS *et al.*, 2014), risco (ZAGORCHEV; GAO, 2015; ELLUL, 2015; CHANG; YU; HUNG, 2015), e assim por diante.

O risco foi considerado elemento determinante para as causas da crise financeira de 2007-2008 (ELLUL, 2015). Neste sentido, Zagorchev e Gao (2015) estudaram como a governança corporativa afetou as instituições financeiras dos Estados Unidos. Os autores verificaram que uma melhor governança está negativamente relacionada ao risco e positivamente relacionada com o desempenho.

Em contrapartida, Ellul (2015) afirma que a exposição ao risco em instituições financeiras apenas pode ser mitigada com um forte gerenciamento de risco. O autor evidencia que o gerenciamento de risco deve ser compatível com o modelo de negócio para promover a maximização de valor em longo prazo. Sendo assim, Damodaran (2009, p. 305) diferencia risco e gestão de risco, mencionando que “diferente da proteção contra riscos, que é vista como tarefa do departamento financeiro, a gestão de riscos precisa estar na agenda de cada um na empresa”. O autor destaca que o sucesso não está em evitar o risco, mas tirar proveito de suas oportunidades, de forma a agregar valor à organização.

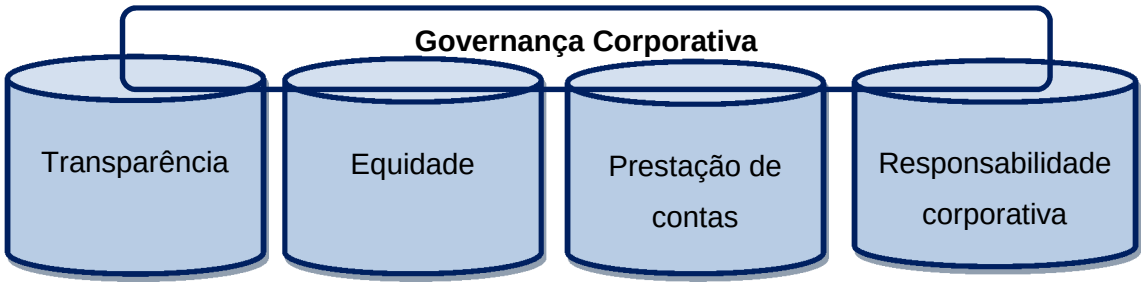
A criação de valor e o controle de risco são considerados por Chang, Yu e Hung (2015) como requisitos fundamentais na estratégia de governança corporativa. Os autores afirmam que a governança corporativa serve de proteção para mitigar o risco às empresas, destacando a participação em assembleias gerais, transparência da estrutura de administração, conselhos de administração, presidente e diretores. Os autores constataram que o nível elevado de governança corporativa permite um desempenho alto e um risco baixo.

A importância da aplicação dos princípios de boa governança corporativa também é ressaltada por Kearney e Kruger (2013). Os autores registram que ao longo da última década, muitos estudos têm sido realizados para investigar o papel e o impacto de tais princípios.

2.1.1 Princípios de Governança Corporativa

Os princípios de governança corporativa são destinados a orientar as autoridades na implementação de códigos nacionais eficientes de governança. (MATEESCU, 2015). Esse conjunto de princípios de governança corporativa, no Brasil, é sugerido pelo Instituto Brasileiro de Governança Corporativa (IBGC, 2009). Conforme o IBGC (2009, p. 15) esses princípios são recomendações objetivas e buscam alinhar os interesses da empresa com os interesses de seus *stakeholders*, e podem ser aplicados a todas as empresas, independente do seu porte, natureza jurídica ou tipo de controle. A Figura 1 apresenta os princípios recomendados pelo IBGC.

Figura 1 - Princípios da Boa Governança Corporativa



Fonte: Elaborado a partir de IBGC (2009, p. 19).

Apresenta-se na Figura 1 o princípio da transparência que significa disponibilizar para as partes interessadas não só as informações impostas por regulamentos, mas também as que possam ser úteis aos usuários, permitindo um clima de confiança interna e externamente à organização. (IBGC, 2009).

Neste sentido, o Comitê de Basiléia de Supervisão Bancária (BIS, 1998, p. 15) já definia a transparência da informação como a "publicação de informação fiável e oportuna que permite aos usuários dessas informações a avaliação precisa das condições financeiras e desempenho das atividades operacionais e riscos relacionados a essas atividades". Destaca ainda que a transparência da informação deve possuir características qualitativas mais elaboradas, considerando a abrangência, pertinência e atualidade, confiabilidade, comparabilidade e materialidade.

Desta forma, uma informação transparente deve: (i) agregar, consolidar e avaliar informações das atividades e entidades (abrangência); (ii) ser relevante para a tomada de decisão e oportuna de forma a apresentar informações frequentes e suficientes de uma instituição, incluindo o perfil de risco e gestão de risco (pertinência e atualidade); (iii) representar fielmente aquilo que se propõe representar (confiabilidade); (iv) ser comparada a outras instituições e países ao longo do tempo (comparabilidade); divulgar, disponibilizar a informação sem omiti-la ou distorcê-la (materialidade). (BIS, 1998).

Considerando essas características, Liu *et al.* (2015) afirmam que não existe uma definição específica de transparência, trata-se de um conceito muito abrangente. Os autores complementam que apesar da falta de definição única, os investidores estão preocupados com a transparência relacionada às informações

contábeis e preços das ações no mercado de capitais, afetando diretamente suas decisões de investimento.

Corroborando com Liu *et al*. (2015), Stein, Salterio e Shearer (2015) também encontraram diferentes significados à transparência. Os autores compararam os conceitos de transparência obtidos por meio de jornais norte-americanos de circulação diária (444 publicações no período de 2001 a 2011) e pesquisas acadêmicas (1845 artigos no período de 2002 a 2011). O período escolhido refere-se à antes, durante e após a maioria dos escândalos das empresas norte-americanas, como por exemplo a Enron, WorldCom, Global Crossing, Livent.

Stein, Salterio e Shearer (2015) buscaram respostas à três perguntas envolvendo a temática transparência: (i) o que é transparência? (ii) por que a transparência é desejável? (iii) como a transparência é conseguida ou melhorada?

As publicações em jornais norte-americanos sugerem que a transparência está relacionada com as seguintes propriedades de informações: qualidade, divulgação, pontualidade e precisão. O desejo de transparência refere-se à melhoria na tomada de decisão e alinhamento de interesses entre agente e principal. A transparência é melhorada com padrões contábeis para reduzir viés nas demonstrações contábeis incluindo disponibilidade de informações com maior precisão, confiabilidade, comparabilidade, honestidade e integridade. (STEIN; SALTERIO, SHEARER, 2015).

Já para as publicações em artigos acadêmicos, o conceito de transparência é consistente com o IASB (*International Accounting Standards Board*) e FASB (*Financial Accounting Standards Board*). A maioria dos pesquisadores identifica a transparência com características de pontualidade, conservadorismo, representação fidedigna, neutralidade, imparcialidade. Os autores evidenciaram também que a transparência está associada ao indivíduo, referindo-se a interpretação e entendimento pessoal. (STEIN; SALTERIO, SHEARER, 2015).

Para Morris, Susilowati e Gray (2012) a transparência está além das divulgações exigidas pelos órgãos reguladores, deve conter divulgações de informações voluntárias. Os autores afirmam que as empresas mais rentáveis tendem a divulgar mais informações voluntárias para os investidores, permitindo à avaliação de sua credibilidade e ganhos. Porém, Mateescu (2015) evidencia que o acesso a essas informações pelos concorrentes, pode ser vista como uma

desvantagem, razão pela qual algumas empresas são relutantes em divulgar voluntariamente a informação.

O estudo de Mateescu (2015) revelou que a presença de investidores institucionais não influencia significativamente o nível de transparência ou conformidade das empresas analisadas, sugerindo que o ambiente legal influencia os mecanismos de governança corporativa mais do que os fatores internos.

Outro princípio da boa governança, destacado na Figura 1, é a equidade. A equidade refere-se ao senso de justiça entre as partes interessadas: funcionários, clientes, credores, fornecedores, órgãos reguladores, financiadores e comunidade, propiciando a valorização de relacionamentos internos e externos da organização (ÁLVARES; GIACOMETTI; GUSSO, 2008) de forma que as atitudes ou políticas discriminatórias não são aceitas. (IBGC, 2009).

Ferreira *et al.* (2015) complementam que a participação dos minoritários e majoritários deve ser equânime referente aos resultados das operações, aumento de riqueza e presença nas assembleias gerais. Já na prestação de contas, o IBGC (2009) recomenda que os sócios, administradores, conselheiros e auditores (agentes) devem prestar contas de sua atuação, ou seja, são os responsáveis por seus atos e omissões. Os agentes devem atuar com responsabilidade corporativa, zelando pelas empresas, permitindo sua sustentabilidade em longo prazo, incorporando questões sociais e ambientais.

A prestação de contas é abordada por Ozkan e Tanç (2012) como um dever que é cumprido por uma pessoa ou empresa, de forma voluntária ou não, sendo interligada ao conceito de responsabilidade. Neste sentido, Ferreira *et al.* (2015) afirmam que a prestação de contas é fundamentada nas melhores práticas contábeis e de auditoria, remete ao conceito de conformidade, no cumprimento de normas reguladoras, tanto no ambiente interno quanto externo da organização.

Sintetizando os princípios de governança corporativa, Silveira (2015) afirma que eles buscam aprimorar continuamente o processo decisório a fim de assegurar a sustentabilidade da empresa no longo prazo, reduzir ações negativas por parte de executivos e colaboradores, favorecer a transparência para os usuários internos e externos em relação as finanças, impactos não financeiros e perspectivas do negócio, promovendo a equidade de tratamento e assegurando os direitos dos acionistas.

Verifica-se por meio dos estudos apresentados que a governança corporativa tem sido amplamente estudada. Mateescu (2015) corrobora esta afirmação, quando enfatiza que a governança corporativa tem uma variedade de abordagens, relacionando-se com as áreas como: direito, finanças, contabilidade e gestão. No intuito de consolidar a revisão teórica sobre os princípios de governança corporativa, elaborou-se o Quadro 1.

Quadro 1 - Princípios de governança corporativa

Princípios		**Descrição**	**Autor/ano**
Transparência	Disponibilidade	Estar acessível aos usuários.	IBGC (2009); BIS (1998); Stein, Slaterio e Shearer (2015); Morris, Susilowati e Gray (2012); Mateescu (2015); Dedonatto e Beuren (2015); Silveira *et al.* (2015)
	Oportunidade	Informações íntegras e tempestivas.	
	Abrangência	Agregar, consolidar e avaliar informações das atividades e entidades.	
	Pertinência e atualidade	Ser relevante, oportuna e frequente à tomada de decisão.	
	Materialidade	Divulgar, disponibilizar informações sem omiti-la ou distorcê-la.	
	Qualidade	Características de propriedade que determina a essência ou a natureza.	
	Pontualidade	Disponibilizar informação em tempo hábil para a tomada de decisão.	
	Precisão	Rigor na determinação do registro.	
	Confiabilidade	O usuário aceita a informação e a utiliza como base de decisão.	
	Comparabilidade	Permitir ao usuário identificar diferenças e semelhanças.	
	Honestidade	Preceitos morais socialmente aceitos.	
	Integridade	Informação mais completa possível, sem omissão de algum fato relevante.	
	Alinhamento	Alinhamento de interesses entre agente e principal.	
	Conservadorismo	Cautela quando incertezas estiverem envolvidas	
	Representação fidedigna	Estar livre de erros, vieses e manipulações.	
	Neutralidade	Não há viés de resultado predeterminado.	
	Imparcialidade	Não revela preferência por nenhuma parte envolvida.	
Equidade	Tratamento justo	Senso de justiça entre as partes interessadas	Álvares, Giacometti e Gusso (2008); IBGC (2009); Ferreira *et al.* (2015); Silveira *et al.* (2015); Dedonatto e Beuren (2015)
Prestação de Contas	Responsabilidade	Responsáveis por seus atos e omissões	IBGC (2009); Okzan e Tanç (2012); Ferreira *et al.* (2015)
	Conformidade	Cumprimento de normas reguladoras no ambiente interno e externo	

Responsabilidade corporativa	Zelo	Zelar pela empresa permitindo sua sustentabilidade a longo prazo, incorporando questões sociais e ambientais	IBGC (2009); Dedonatto e Beuren (2015)
	Sustentabilidade		

Fonte: Elaborado com base nas obras consultadas.

No Quadro 1 evidencia-se os conceitos relacionados com os princípios de governança corporativa recomendados pelo IBGC (2009), que são transparência, equidade, prestação de contas e responsabilidade corporativa, porém a conformidade também pode ser considerada um princípio de governança corporativa.

Neste sentido, Dedonatto e Beuren (2010, p. 27) evidenciam que a governança corporativa “deve assegurar aos sócios ou investidores a equidade, transparência, responsabilidade pelos resultados (*accountability*) e obediência às legislações do país (*compliance*) em que está inserida”.

A seguir aprofunda-se o requisito de Conformidade da Governança Corporativa.

2.1.2 Conformidade

A conformidade (*compliance*) refere-se ao cumprimento de normas reguladoras, tanto no ambiente interno quanto externo da organização. (FERREIRA *et al.*, 2015; MATEESCU, 2015). É considerada importante na proteção, criação de valor e reputação corporativa, pois a boa governança exige transparência, harmonia com os padrões éticos, conformidade com normas internas e externas, ajuda na mitigação de riscos e preserva a imagem da organização (OLIVEIRA *et al.*, 2015).

Estudos recentes têm sido evidenciados envolvendo as temáticas conformidade e governança corporativa. (DAROUNCO; 2013; GERARD; WEBER, 2015; AKBAR *et al.,* 2016; GRIFFITH *et al.,* 2016; TURRENT; ARIZA, 2016).

O estudo de Darounco (2013) objetivou avaliar a contribuição dos processos de controles internos e de TI na governança corporativa no aspecto relacionado a conformidade. A aplicação deu-se em uma entidade sem fins lucrativos, os principais achados da pesquisa referem-se à falta de processos, sistemas e controles padronizados e sistematizados, fatores determinantes para a manutenção da conformidade.

Gerard e Weber (2015) analisaram teoricamente os resultados de oito pesquisas (BERNSTEIN et al. 2013; BERNSTEIN; FALCIONE, 2014; SANDFORD et al. 2013; 2014; PROTIVITI 2013; 2014; *ETHICS RESOURCE CENTER* 2013; *SCCE AND NYSE GOVERNANCE SERVICES* 2014) com o objetivo de aprofundar o conhecimento sobre governança corporativa examinando as vantagens e limitações da função de conformidade (*compliance*) na presidência, diretoria executiva, departamento jurídico, recursos humanos, auditoria interna, conselho de administração, sub-comitê do conselho de administração. No Quadro 2, apresentam-se os principais resultados da pesquisa.

Quadro 2 - Vantagens e limitações da conformidade em locais funcionais

Local Funcional	**Vantagens**	**Limitações**
Presidência	Sugere que o CEO está envolvido na avaliação de riscos e atividades de conformidade; cria legitimidade perante os *stakeholders.*	CEO pode filtrar ou suprimir informações sobre violações; pode visualizar a função de *compliance* como um incômodo, pois consome tempo e recursos.
Diretor Executivo	Executivo sob orientação de processos de negócio, possui acesso a muitos dados.	Preocupa-se mais com questões internas do que externas à organização.
Departamento Jurídico	A conformidade e os regulamentos internos alinham as responsabilidades; interpreta e avalia regulamentos para limitar as perdas, avaliar os riscos.	A profundidade jurídica pode limitar o foco para evitar violações, multas e infrações ao invés de incentivar comportamentos desejáveis.
Recursos Humanos	Geralmente o RH orienta os novos funcionários por meio de códigos de conduta ética e comportamental.	O RH é uma função de apoio à organização, sugere-se que a responsabilidade delegada não é considerada estratégica.
Auditoria Interna	Acesso a dados que muitos não possuem; relata suas conclusões para diversos níveis de gestão proporciona legitimidade à função de *compliance*.	A responsabilidade por uma atividade operacional limita a independência e objetividade.
Conselho Administrativo	Grupo de mais alto nível no centro de conformidade tem a responsabilidade de acompanhar a gestão e apoiar seus esforços para controlar e governar a organização.	As informações podem ser filtradas antes de chegarem ao CA, há necessidade de recursos adicionais capaz de disponibilizar a informação.
Comitê do Conselho Administrativo	O comitê leva experiência de fora à organização; Reforça o processo de governança.	As informações podem ser filtradas antes de chegarem ao Comitê, há necessidade de recursos adicionais capaz de disponibilizar a informação.

Fonte: Elaborado com base em Gerard e Weber (2015).

Evidencia-se no Quadro 2, que a conformidade pode existir em vários locais funcionais, nota-se também que para cada local funcional à vantagens e limitações. De acordo com Gerard e Weber (2015), cada local funcional possibilita uma perspectiva especial de decisões, atividades e desempenho da unidade. Os autores afirmam ainda que “uma função de conformidade eficaz suporta uma forte governança corporativa”. (GERARD; WEBER, 2015, p. 17).

Akbar *et al.* (2016) analisaram 435 empresas não financeiras de capital aberto do Reino Unido, no período de 1999 a 2009. Os resultados obtidos sugerem que a conformidade de governança corporativa não é um fator determinante de desempenho. Os autores afirmam que a metodologia utilizada por eles (*Generalized Method of Moments Estimation*) permite conclusões mais robustas quando comparados com os resultados de outros estudos.

Griffith *et al.* (2016) em um simpósio organizado pela *Fordham Journal of Corporate & Financial Law* abordaram a conformidade como “um meio de assegurar que os funcionários ou outras partes estão cumprindo com as normas e regulamentos internos e externos da organização”. (GRIFFITH *et al.*,2016, p. 9). Os autores afirmam que a conformidade possibilita a avaliação do risco, porém pode restringir a atividade da empresa. “O cumprimento de regras (conformidade) torna-se cada vez mais rotineiro, como uma espécie de processo repetitivo, podendo expulsar o pensamento criativo e inovador da organização”. (GRIFFITH *et al.*,2016, p. 70).

O estudo de Turrent e Ariza (2016) analisou o nível de conformidade da governança corporativa de empresas não financeiras que possuem melhor classificação nos índices da bolsa de valores da Argentina, Brasil, Chile e México, no período de 2004 a 2010. A pesquisa consiste em 826 observações. Os autores indicam uma tendência crescente de conformidade da governança corporativa, cujos objetivos são propiciar maior controle e manutenção da reputação no mercado.

Com base nos estudos apresentados, elaborou-se o Quadro 3 cujo objetivo é consolidar o entendimento dos conceitos de governança corporativa no requisito de conformidade.

Quadro 3 - Governança corporativa no requisito de conformidade

	Elementos	Descrição	Autor/ano
Conformidade	Acessibilidade	Acesso às informações para a tomada de decisão.	Ferreira *et al.* (2015); Gerard e Weber (2015); Mateescu (2015); Oliveira *et al.* (2015); Griffith *et al.* (2016)
	Avaliação de Risco	Capacidade de interpretar e avaliar regulamentos para limitar as perdas.	
	Criação de valor	Padrão de excelência operacional percebida pelos *stakeholders.*	
	Ética	Comportamentos informais, valores morais.	
	Legitimidade	Fornece evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo o seu dever.	
	Locais funcionais	Locais dentro de uma estrutura organizacional.	
	Reputação corporativa	Construir uma boa imagem perante os *stakeholders*.	
	Responsabilidade	Obrigação de responder pelas ações próprias ou dos outros.	
	Transparência	Disponibilizar informações úteis aos usuários, permitindo um clima de confiança.	

Fonte: Elaborado com base nas obras consultadas.

Nota-se no Quadro 3 que a acessibilidade, avaliação de risco, criação de valor, ética, legitimidade, locais funcionais, reputação corporativa, responsabilidade e transparência são elementos destacados pela governança corporativa no requisito de conformidade. Estes elementos foram utilizados para a construção do instrumento de coleta de dados juntamente com a temática informação contábil apresentada no capítulo seguinte.

2.2 INFORMAÇÃO CONTÁBIL

A etimologia da palavra informação está referenciada a uma forma de representar, de apresentar ou de criar uma ideia (ZEMAN, 1970). Pode ser definida como: (i) aquilo que apresenta conhecimento novo acerca de fatos, (ii) um conjunto de dados utilizados para a troca de mensagens entre indivíduos e/ou máquinas e, (iii) a transferência de valores monetários. (SÊMOLA, 2014).

Na contabilidade a informação é essencial. Ribeiro Filho, Lopes e Pederneiras (2009) afirmam que o objetivo da contabilidade é identificar, mensurar, registrar, divulgar as informações sobre a situação patrimonial, financeira e de resultado das

entidades. Já para Azad *et al.* (2016) a contabilidade pode ser definida como um sistema que mede as atividades do negócio, processando as informações em relatórios, tornando-os disponíveis aos tomadores de decisão. Os documentos que apresentam o desempenho monetário da organização são chamados de demonstrações contábeis.

Neste sentido, Iudícibus (2010) destacam que as demonstrações contábeis têm como objetivo promover informações úteis para a tomada de decisão de seus usuários, representando a posição econômico-financeira da entidade, suas alterações e seus resultados. Porém, para que essas informações cheguem aos usuários internos e externos da organização, esta precisa cumprir um processo estruturado de comunicação contábil, adotando práticas contábeis que determinam a forma destas informações. (RIBEIRO FILHO; LOPES; PEDERNEIRAS, 2009). Deste modo, são as práticas contábeis que determinam a maneira como as informações chegam aos usuários, internos e externos da organização.

Hendriksen e Van Breda (1999) consideram que as informações contábeis devem ser divulgadas para os investidores, clientes, credores, funcionários, órgãos do governo e ao público em geral. Para que isso ocorra, Iudícibus (2009) destaca que é necessário um intermediador (auditores, analistas de mercado de capitais e empresas de *rating*), conhecedor de contabilidade que irá interpretar e traduzir a informação.

As informações contábeis são divulgadas por meio das demonstrações contábeis e devem ser padronizadas. (AZAD *et al*., 2016). Como padrão para a elaboração das demonstrações contábeis o *International Accounting Standards Board* (IASB) desenvolveu um conjunto de normas contábeis de alta qualidade para servir de referência mundial. (JORISSEN, 2015).

No Brasil, o processo de convergência às normas do IASB está sendo pronunciado pelo Comitê de Pronunciamentos Contábeis (CPC) e pelos órgãos reguladores Comissão de Valores Mobiliários (CVM) e Conselho Federal de Contabilidade (CFC). (IUDÍCIBUS, 2010).

Para auxiliar na tomada de decisão, a informação contábil precisa possuir determinadas características qualitativas. (HENDRIKSEN; VAN BREDA, 1999; RIBEIRO FILHO; LOPES; PEDERNEIRAS, 2009; CPC 00 R1, 2011). As características qualitativas da informação contábil são definidas como sendo as

propriedades da informação que são necessárias para torná-la útil. (HENDRIKSEN; VAN BREDA, 1999, p. 95).

Sendo assim, o CPC 00 R1 (2011) classifica as características qualitativas da informação contábil como “fundamentais” e de “melhoria”. Já Hendriksen e Van Breda (1999) denominam essas características como “específicas para usuários” e “específicas para decisões”.

De acordo com Souza *et al.* (2015) as características qualitativas da informação contábil também podem ser chamadas de atributos da contabilidade gerencial, pois muitos autores utilizam esta linguagem. Os autores complementam que tais características agregam qualidade aos relatórios, tornando-os comparáveis a outros e facilmente compreensíveis pelos usuários (acionistas, *stakeholders*, entre outras partes interessadas). O Quadro 4 apresenta as características qualitativas abordadas por CPC 00 R1 (2011), Hendriksen e Van Breda (1999) e Ribeiro Filho, Lopes e Pederneiras (2009).

Quadro 4 - Características qualitativas das informações contábeis

CPC 00 R1 (2011)	**Hendriksen e Van Breda (1999, p. 96)**	**Ribeiro Filho, Lopes e Perdeneiras (2009, p. 81)**
Qualidades fundamentais	**Qualidades específicas para usuários**	Compreensibilidade
Relevância	Compreensibilidade	Relevância
* Valor preditivo	**Qualidades específicas para decisões**	* Valor preditivo
* Valor como *feedback*	Relevância	*Valor como *feedback*
* Materialidade	* Oportunidade	* Materialidade
Representação fidedigna	* Valor preditivo	Confiabilidade
* Informação completa	*Valor como *feedback*	* Primazia da essência sobre a forma
* Informação neutra	Confiabilidade	* Fidelidade de representação
* Informação livre de erro	* Verificabilidade	* Neutralidade
Qualidades de melhoria	* Fidelidade de representação	* Prudência ou Conservadorismo
Comparabilidade	* Neutralidade	* Integridade
* Consistência	Comparabilidade	Comparabilidade
* Uniformidade	*Uniformidade	
Verificabilidade	* Consistência	
* Direta	Materialidade	
* Indireta		
Tempestividade		
Compreensibilidade		

Fonte: Elaborado com base nas obras consultadas.

Evidencia-se no Quadro 4 diferentes classificações às características qualitativas da informação contábil. Como menciona anteriormente, o CPC 00 R1 (2011) classifica as características qualitativas como “fundamentais” e de “melhoria”, já Hendriksen e Van Breda (1999) consideram como “qualidades específicas para usuários” e “qualidades específicas para decisões”. Ribeiro Filho, Lopes e Pederneiras (2009) não efetuam distinção de denominações. Apesar de haver diferentes denominações, verifica-se de forma geral que os atributos são os mesmos.

O CPC 00 R1 (2011) declara que as informações qualitativas de melhoria (comparabilidade, verificabilidade, tempestividade e compreensibilidade) para serem úteis devem possuir também os requisitos qualitativos fundamentais (relevância e representação fidedigna).

Hendriksen e Van Breda (1999) denominam as características qualitativas “específicas para usuários” como determinantes, pois referem-se à compreensão (compreensibilidade) de um atributo específico do usuário. Já às qualidades “específicas para decisões” são compostas pelos requisitos de relevância, confiabilidade, comparabilidade e materialidade.

Para Souza *et al.* (2015) a relevância é aquela capaz de fazer diferença nas decisões tomadas pelos usuários. Neste sentido, Hendriksen e Van Breda (1999) explicam que para ser relevante a informação deve ser oportuna (oportunidade) e estar disponível ao usuário antes que ela perca a sua capacidade de influência.

Barbosa *et al.* (2015) complementam que a relevância refere-se à capacidade da informação em fazer diferença nas decisões dos usuários, devendo ser de valor preditivo e confirmatório. O valor preditivo possibilita predizer resultados futuros, já no valor confirmatório a informação serve de *feedback*, permitindo a confirmação ou alteração das informações prévias.

Outra característica qualitativa evidenciada no Quadro 4 é a confiabilidade. A confiabilidade tem como atributos a verificabilidade, a fidelidade de representação e a neutralidade. A verificabilidade significa que os usuários devem chegar a um consenso nas informações, mas não necessariamente a um completo acordo. A representação fidedigna deve estar livre de erros, vieses e manipulações. Já a neutralidade quer dizer que não há viés de um resultado predeterminado. (HENDRIKSEN; VAN BREDA, 1999).

Em complemento, Ribeiro Filho, Lopes e Pederneiras (2009) acrescentam a primazia da essência sobre a forma (reflete o que de fato ocorreu independente de um contrato), prudência ou conservadorismo (cautela quando incertezas estiverem envolvidas) e a integridade (informação mais completa possível, sem omissão de algum fato relevante).

Quanto à comparabilidade, Souza *et al.* (2015) destacam que a informação contábil deve permitir aos usuários identificar as diferenças e semelhanças entre elas. Porém, Hendriksen e Van Breda (1999) afirmam que para serem comparáveis, são necessários os atributos de uniformidade e consistência da informação. A uniformidade significa que eventos iguais são representados de forma idêntica, já a consistência refere-se ao uso de conceitos e procedimentos de mensuração semelhantes para itens afins.

Ribeiro Filho, Lopes e Pederneiras (2009) consideram uma informação material quando a sua omissão ou distorção da informação provocar influência nas decisões dos usuários. Neste sentido, Hendriksen e Van Breda (1999) afirmam que a informação só pode ser considerada material se for importante para os usuários. Porém, segundo o CPC 00 R1 (2011, QC11), “não se pode especificar um limite quantitativo uniforme para materialidade ou predeterminar o que seria julgado material para uma situação particular”. Desta forma, depreende-se que a informação contábil para ser útil, de qualidade e auxiliar na tomada de decisão, precisa possuir determinadas características qualitativas.

Neste contexto, estudos empíricos evidenciam as características qualitativas da informação contábil. O estudo de Barbosa *et al.* (2015) construiu uma métrica de qualidade da informação contábil sob a ótica de analistas fundamentalistas. Os principais achados da pesquisa são a concordância de percepção dos analistas fundamentalistas para as características qualitativas de representação fidedigna, relevância e comparabilidade. Porém, os autores comentam que houve dificuldade de encontrar fatores para representam a compreensibilidade e a materialidade. Os autores não identificaram as características de tempestividade devido à falta de construtos.

Quanto a tempestividade, os achados de Souza *et al.* (2015) revelam que os gestores solicitam a informação em tempo hábil (tempestiva) para a tomada de decisão, porém isso ocorre com pouca frequência.

Lima *et al.* (2015) analisaram o comportamento da qualidade das informações contábeis nos diferentes estágios de ciclo de vida das companhias listadas na BM&FBovespa, por meio da investigação do comportamento do conservadorismo, persistência e gerenciamento de resultados. Os resultados sugerem que existem diferenças significativas na qualidade das informações contábeis, exceto para o gerenciamento de resultados contábeis.

Diante dos conceitos teóricos abordados neste capítulo, apresenta-se no Quadro 5 as principais características qualitativas das informações contábeis.

Quadro 5 - Principais características qualitativas das informações contábeis

Características	Descrição	Autor/ano
Comparabilidade	Permitir ao usuário identificar diferenças e semelhanças.	Hendriksen e Van Breda (1999); Ribeiro Filho, Lopes e Pederneiras (2009) Iudícibus (2010); CPC 00 R1 (2011); Souza *et al.* (2015); Jorissen (2015); Azad *et al.* (2016)
Compreensibilidade	Deve ser exposta na forma mais compreensível ao usuário.	
Confiabilidade	O usuário aceita a informação e a utiliza como base de decisão.	
Consistência	Uso de conceitos e procedimentos de mensuração semelhantes para itens afins.	
Disponibilidade	Estar acessível aos usuários.	
Integridade	Informação mais completa possível, sem omissão de algum fato relevante	
Materialidade	Omissão ou distorção provocar influência nas decisões dos usuários.	
Neutralidade	Não há viés de resultado predeterminado.	
Oportunidade	Informações íntegras e tempestivas	
Preditiva	Predizer resultados futuros.	
Primazia da essência sobre a forma	Reflete o que de fato ocorreu independente de um contrato.	
Prudência ou conservadorismo	Cautela quando incertezas estiverem envolvidas	
Relevância	Capaz de fazer diferença nas decisões dos usuários.	
Representação Fidedigna	Estar livre de erros, vieses e manipulações.	
Tempestividade	Disponibilizar informação em tempo hábil para a tomada de decisão.	
Uniformidade	Eventos iguais são representados de forma idêntica.	
Utilidade	Deve ser relevante e fidedigna.	
Verificabilidade	Os usuários devem chegar a um consenso, mas não a um acordo.	

Fonte: Elaborado com base nas obras consultadas.

Para que a informação contábil seja útil e de qualidade são necessárias as características apresentadas no Quadro 5. A consolidação teórica evidenciada neste Quadro foi utilizada para a construção do instrumento metodológico desta pesquisa. Verifica-se que a informação é essencial para os negócios de uma organização, é considerada um dos ativos mais relevantes, ela circula por toda a empresa tanto

internamente quanto externamente, portanto precisa ser protegida. (SÊMOLA, 2014). Neste sentido, a seguir aborda-se o tema Segurança de Informação.

2.3 SEGURANÇA DA INFORMAÇÃO

A segurança da informação tornou-se mundialmente um elemento essencial para as organizações, a fim de eliminar os riscos de falta de segurança da informação (SHAMALA *et al*., 2015) e melhorar a conformidade das informações (SAFA; VON SOLMS; FURNELL, 2016). Pode ser definida, conforme Sêmola (2014, p. 41), como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

O objetivo da segurança da informação é garantir a proteção das informações contra acessos indesejados, disponibilizando-as no momento desejado de forma confiável. (ALBERTIN; PINOCHET, 2010). Deste modo, a segurança da informação é influenciada por três propriedades principais: a confidencialidade, a integridade e a disponibilidade da informação. (SÊMOLA 2014).

A confidencialidade refere-se à proteção da informação de acordo com o sigilo de seu conteúdo, limitando o seu acesso e uso somente às pessoas destinadas. No que tange a integridade, significa a proteção da informação contra alterações indevidas, de forma intencional ou acidental. Já a disponibilidade significa disponibilizar a informação aos seus usuários no momento que os mesmos necessitem. (SÊMOLA, 2014).

Uddin e Preston (2015) também evidenciam a importância da disponibilidade da informação de forma íntegra fornecendo confidencialidade. Segundo os autores, a não entrega das informações em tempo hábil para a tomada de decisão e/ou a falta de integridade poderá resultar em compensações, perda de negócio, problemas de conformidade e divulgação de informações sigilosas.

Outros objetivos da segurança de informação são destacados por Albertin e Pinochet (2010). Os autores acrescentam a legalidade (estar em conformidade com a legislação), consciência (atuação do sistema de acordo com a expectativa dos usuários), isolamento ou uso legítimo (controlar o acesso do sistema), auditoria (proteção contra erros e atos cometidos por usuários autorizados) e confiabilidade (garantir a atuação do sistema conforme o esperado).

Neste sentido, Sêmola (2014, p. 45) apresenta os seguintes aspectos da segurança da informação: autorização (permissão para o acesso às informações), auditoria (identificar as entidades envolvidas na troca de informações), autenticidade (garantia que a informação não foi alterada após o seu envio ou validação), severidade (gravidade do dano que o ativo pode sofrer mediante uma ameaça), relevância do ativo (grau de importância de um ativo para a operacionalização de um processo de negócio), relevância do processo de negócio (grau de importância do processo de negócio para o alcance dos objetivos e sobrevivência da empresa), criticidade (gravidade referente ao impacto ao negócio causado por problemas de segurança) e irretratabilidade (identificação do emissor, autor de informações). O autor destaca que a legalidade é ampliada para o conceito de conformidade, pois refere-se ao cumprimento de obrigações legais e regulatórios da empresa para seus *stakeholders*.

Já para Dhillon e Backhouse (2000) além de confidencialidade, integridade e disponibilidade, são necessários à organização os princípios de responsabilidade (a capacidade de responder com as obrigações e saber lidar com novas oportunidades de desenvolvimento), confiança (divisão de demandas trabalhistas com os colegas de acordo com normas da empresa, padrões aceitos e acordados de comportamento) e ética (comportamentos informais, regras e procedimentos não podem ser aplicados a todos os procedimentos, são os valores morais) para o sucesso na gestão de segurança da informação.

Bulgurcu, Cavusoglu e Benbasat (2010, p. 524) afirmam que “o sucesso em segurança da informação pode ser alcançado quando as organizações investem em recursos técnicos e sócio organizacionais”. Isto significa que o foco da segurança da informação está no indivíduo e nas perspectivas organizacionais. Os autores destacam também, a importância no cumprimento de políticas de segurança da informação, definindo-as como (2010, p. 526-527) “uma declaração dos papéis e responsabilidades dos empregados para salvaguardar as informações e recursos de suas organizações”. Segundo Albertin e Pinochet (2010) elas estabelecem as responsabilidades funcionais, princípios institucionais de proteção, controle, monitoramento e especificam os principais riscos e impactos.

De acordo com Sêmola (2014) a política de segurança da informação é subdividida em três blocos: diretrizes, normas e procedimentos e instruções, sendo destinadas respectivamente aos níveis estratégico, tático e operacional. As diretrizes

precisam expressar a importância da informação para a organização, incrementando a segurança à cultura organizacional por meio de ações que orientam as atividades. As normas devem fornecer as orientações para o uso adequado das informações. Já os procedimentos e instruções significa descrever meticulosamente cada ação e atividade do uso das informações. O autor complementa que os funcionários devem estar envolvidos para a segurança do negócio e proteção das informações.

Neste sentido, o alinhamento entre a tecnologia e os usuários torna-se essencial para a segurança de informações. Safa *et al.* (2015) evidenciam que a tecnologia unicamente não pode garantir um ambiente seguro para obter informações, o comportamento de usuários deve ser considerado um fator importante neste domínio. Os autores explicam que os *hackers* usam diferentes métodos para alterar o objetivo básico da segurança de informação (a confidencialidade, integridade e a disponibilidade de informações), enquanto que os usuários intencionalmente ou por negligência são uma grande ameaça para a segurança da informação.

Há uma série de erros cometidos pelos usuários que afetam a segurança da informação: compartilhamento de informações de conta, download de qualquer software da internet, escrever senhas em local visível, senhas de acesso com o nome do usuário. (SAFA *et al.*, 2015). O estudo de Parsons *et al.* (2015) sugere que a melhoria da cultura de segurança de uma organização influencia positivamente o comportamento dos empregados, que por sua vez possibilita a melhor conformidade com políticas de segurança, atenuando o risco para dados e sistemas de informação da organização.

Desta forma, quando as ameaças colocam em risco as propriedades e segurança da informação, é preciso atenção para o ciclo de vida da informação. De acordo com Sêmola (2014) o ciclo de vida da informação significa a visão corporativa em que o elo mais fraco determina o grau de resistência e proteção, representa as fases de: manuseio (momento em que a informação é criada e manipulada), armazenamento (momento em que a informação é armazenada), transporte (momento em que a informação é transportada) e descarte (momento em que a informação é descartada). O autor destaca que todas essas fases devem ser protegidas. No entanto, para obter-se sucesso na proteção dos ativos de informação é necessária à organização a mudança de paradigma, com vistas à segurança da informação por meio de um sistema de gestão de segurança da informação. (ELOF;

ELOF, 2003). Fontes (2012) complementa que o sucesso na implantação da política de segurança da informação está condicionado ao respaldo da alta direção, não apenas em investimentos financeiros, mas também por meio do apoio à equipe.

Diante dos conceitos teóricos abordados evidenciam-se no Quadro 6 os requisitos da segurança de informação.

Quadro 6 - Requisitos da segurança de informação

Requisitos	**Descrição**	**Autor/ano**
Conformidade	Cumprimento de requisitos.	Sêmola (2014); Buccafurri *et al.* (2015); Safa, Von Solms e Furnell (2016)
Proteção	Proteção das informações contra acessos indesejados.	Albertin e Pinochet (2010)
Confidencialidade	Sigilo de conteúdo, limitando o seu acesso e uso restrito às pessoas autorizadas.	Dhillon e Backhouse (2000); Albertin e Pinochet (2010); Sêmola (2014); Uddin e Preston (2015); Safa *et al.* (2015)
Integridade	Proteção contra alterações indevidas.	
Disponibilidade	Disponível aos usuários.	
Legalidade	Estar em conformidade com a legislação.	Albertin e Albertin e Pinochet (2010
Consciência	Atuação de acordo com a expectativa do usuário.	
Uso legítimo	Controle de acesso ao sistema.	
Confiabilidade	Atuação do sistema conforme o esperado.	
Responsabilidade	Responder com as obrigações e lidar com novas oportunidades.	Dhillon e Backhouse (2000)
Confiança comportamental	Padrões aceitos e acordados de comportamento.	
Ética	Comportamentos informais, valores morais.	
Políticas de segurança	Declarações de papéis e responsabilidades dos empregados para salvaguardar as informações e recursos.	Bulgurcu, Cavusoglu e Benbasat (2010); Albertin e Pinochet (2010); Fontes (2012)
Autorização	Permissão para o acesso às informações.	Sêmola (2014)
Auditoria	Identificar as entidades envolvidas na troca de informações.	
Autenticidade	Garantia que a informação não foi alterada após o seu envio ou validação.	
Severidade	Gravidade do dano que o ativo pode sofrer mediante uma ameaça.	
Relevância do ativo	Grau de importância de um ativo para a operacionalização de um processo de negócio.	
Relevância do processo de negócio	Grau de importância do processo de negócio para o alcance dos objetivos e sobrevivência da empresa.	
Criticidade	Gravidade referente ao impacto ao negócio causado por problemas de segurança.	
Irretratabilidade	Identificação do emissor, autor de informações.	

Fonte: Elaborado com base nas obras consultadas.

O Quadro 6 mostra os requisitos e suas definições para a segurança da informação sob a ótica teórica e de estudos empíricos, porém para fazer parte do instrumento de coleta desta pesquisa os requisitos de segurança da informação foram classificados em primários e secundários. Os requisitos primários são os requisitos essenciais para a segurança da informação, necessariamente devem estar presentes para que existam os secundários. No Quadro 7, apresentam-se os requisitos primários da segurança da informação.

Quadro 7 - Requisitos primários da segurança de informação

Requisitos	**Descrição**	**Autor/ano**
Autenticidade	Garantia que a informação não foi alterada após o seu envio ou validação.	Sêmola (2014)
Confiabilidade	Atuação do sistema conforme o esperado.	Albertin e Pinochet (2010)
Confidencialidade	Sigilo de conteúdo, limitando o seu acesso e uso restrito às pessoas autorizadas.	Dhillon e Backhouse (2000); Albertin e Pinochet (2010); Sêmola (2014);Uddin e Preston (2015); Safa *et al.* (2015)
Conformidade	Cumprimento de requisitos.	Sêmola (2014); Buccafurri *et al.* (2015); Safa, Von Solms e Furnell (2016)
Disponibilidade	Disponível aos usuários.	Dhillon e Backhouse (2000); Albertin e Pinochet (2010); Sêmola (2014);Uddin e Preston (2015); Safa *et al.* (2015)
Integridade	Proteção contra alterações indevidas.	Dhillon e Backhouse (2000); Albertin e Pinochet (2010); Sêmola (2014);Uddin e Preston (2015); Safa *et al.* (2015)
Políticas de segurança	Declarações de papéis e responsabilidades dos empregados para salvaguardar as informações e recursos.	Bulgurcu, Cavusoglu e Benbasat (2010); Albertin e Pinochet (2010); Fontes (2012)

Fonte: Elaborado com base nas obras consultadas.

Evidencia-se no Quadro 7 os requisitos primários da segurança de informação: conformidade, confidencialidade, integridade, disponibilidade, confiabilidade, políticas de segurança e autenticidade. Estes requisitos estão contemplados no instrumento de coleta desta pesquisa.

Sendo assim, para que os objetivos de segurança da informação (DHILLON; BACKHOUSE, 2000; ALBERTIN; PINOCHET, 2010; BULGURCU; CAVUSOGLU; BENBASAT, 2010; SÊMOLA, 2014; UDDIN; PRESTON, 2015) possam ser atendidos utilizam-se práticas de segurança de informações que estão relacionadas à adoção de tecnologias de segurança e comportamento do usuário (RHEE; KIM;

RYU, 2009; BULGURCU; CAVUSOGLU; BENBASAT, 2010*;* SÊMOLA, 2014; MONTESDIOCA; MAÇADA, 2015, PARSONS *et al.*, 2015; SAFA *et al.*, 2015).

As práticas de segurança da informação podem reduzir as vulnerabilidades, limitar os impactos e evitar os riscos ao negócio. (SÊMOLA, 2014). Desta forma, destaca-se a ISO/IEC 27002 (2013) que trata especificamente das práticas de segurança da informação. A ISO/IEC 27002 (2013) trata especificamente de segurança da informação por meio de um conjunto adequado de controles, políticas e procedimentos organizacionais e funções de *software* e *hardware*. Desta forma, segundo a ISO/IEC 27002 (2013, p. 4) “estes controles precisam ser estabelecidos, implementados, monitorados, analisados e criticamente melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos”. Isto significa que a segurança da informação eficaz protege os ativos da organização atuando como um facilitador dos negócios.

De acordo com Sêmola (2014) essa norma representa um importante instrumento sinalizador da direção para as empresas preocupadas com a operação de seu negócio e a proteção das informações. A ISO/IEC 27002 (2013) recomenda que a organização identifique os seus requisitos de segurança da informação. Deste modo, a norma estabelece várias categorias que têm como objetivo analisar o nível de proteção das práticas de segurança da informação nas organizações. O Quadro 8 mostra as categorias existentes na norma.

Quadro 8 - Categorias de segurança da informação

Seção	**Categorias**
5	Política de segurança da informação
6	Organização da segurança da informação
7	Segurança em recursos humanos
8	Gestão de ativos
9	Controle de acesso
10	Criptografia
11	Segurança física e do ambiente
12	Segurança nas operações
13	Segurança nas comunicações
14	Aquisição, desenvolvimento e manutenção de sistemas
15	Relacionamento na cadeia de suprimento
16	Gestão de incidentes de segurança da informação
17	Aspectos da segurança da informação na gestão da continuidade do negócio
18	Conformidade

Fonte: Elaborado com base em ISO/IEC 27002 (2013).

Observa-se no Quadro 8 que a ISO/IEC 27002 (2013) possui 18 categorias de segurança da informação, sendo as quatro primeiras consideradas introdutórias e as demais são compostas por 14 categorias. Conforme a norma, cada categoria possui um objetivo de controle (o que espera ser alcançado) e as diretrizes para implementação (informações detalhadas de apoio ao controle). O posicionamento deste trabalho contempla o detalhamento da seção 18 referente à categoria “Conformidade”. Há dois objetivos macros à conformidade, o primeiro é “evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança” (ABNT NBR ISO/IEC 27002, 2013 p. 103) e, o segundo trata de “garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização” (ABNT NBR ISO/IEC 27002, 2013 p. 108).

Para o alcance desses objetivos, apresenta-se no “APÊNDICE C”, um conjunto de controles e recomendações que permitem a conformidade de segurança da informação. A aplicação destes possibilita uma visão sistêmica sobre a temática conformidade em segurança da informação. A conformidade torna-se importante para o processo de sistemas de gestão de segurança, pois se destina a aumentar a qualidade e reduzir as vulnerabilidades de serviços, por meio do cumprimento de requisitos. Já as falhas de conformidade podem causar custos à organização relacionados com disposições normativas não atendidas, perda de certificações e aumento de incidentes de segurança. (BUCCAFURRI *et al.*, 2015).

Neste sentido, Sêmola (2014) evidencia que a conformidade é um dos componentes do modelo de GRC (gestão da governança, risco e conformidade), cujo objetivo é garantir o cumprimento das obrigações com os *stakeholders* e aspectos legais e regulatórios. O autor complementa que a conformidade é considerada como um dos aspectos mais importantes da segurança da informação.

De forma geral, as normas de segurança ISO/IEC 27002 podem ser utilizadas como orientação ou estrutura para desenvolver e manter um sistema de gestão de segurança da informação adequado, prevenindo violações de privacidade e segurança, práticas contábeis fraudulentas e ataques a sistemas de TI. (DISTERER, 2013). A seguir apresenta-se o construto utilizado nesta pesquisa.

2.4 CONSTRUTO DA PESQUISA

No Quadro 9 mostra-se o construto utilizado nesta pesquisa. Com base nos conceitos apresentados anteriormente, construiu-se o instrumento de coleta de dados (questionário). Os autores foram suprimidos, pois já foram referenciados nos quadros anteriores.

Quadro 9 - Construto da pesquisa

	Elementos	**Descrição**
Conformidade (GC)	Acessibilidade	Acesso às informações para a tomada de decisão.
	Avaliação de Risco	Gestão preventiva de riscos, monitoramento e supervisão contínua dos processos.
	Criação de valor	Padrão de excelência operacional percebida pelos *stakeholders.*
	Ética	Comportamentos informais, valores morais.
	Legitimidade	Fornece evidências aos stakeholders sobre o atendimento de uma expectativa, cumprindo o seu dever.
	Locais funcionais	Locais dentro de uma estrutura organizacional:
	Reputação corporativa	Construir uma boa imagem perante os *stakeholders*.
	Responsabilidade	Obrigação de responder pelas ações próprias ou dos outros.
	Transparência	Disponibilizar informações úteis aos usuários, permitindo um clima de confiança.
Informação Contábil	Comparabilidade	Permitir ao usuário identificar diferenças e semelhanças.
	Compreensibilidade	Deve ser exposta na forma mais compreensível ao usuário.
	Confiabilidade	O usuário aceita a informação e a utiliza como base de decisão.
	Consistência	Uso de conceitos e procedimentos de mensuração semelhantes para itens afins.
	Disponibilidade	Estar acessível aos usuários.
	Integridade	Informação mais completa possível, sem omissão de algum fato relevante.
	Materialidade	Omissão ou distorção provocar influência nas decisões dos usuários.
	Neutralidade	Não há viés de resultado predeterminado.
	Oportunidade	Informações íntegras e tempestivas.
	Preditiva	Predizer resultados futuros.
	Primazia da essência sobre a forma	Reflete o que de fato ocorreu independente de um contrato.
	Prudência ou conservadorismo	Cautela quando incertezas estiverem envolvidas.
	Relevância	Capaz de fazer diferença nas decisões dos usuários.
	Representação Fidedigna	Estar livre de erros, vieses e manipulações.
	Tempestividade	Disponibilizar informação em tempo hábil para a decisão.
	Uniformidade	Eventos iguais são representados de forma idêntica.
	Utilidade	Deve ser relevante e fidedigna.
	Verificabilidade	Os usuários devem chegar a um consenso, mas não a um acordo.

Segurança de Informação	Autenticidade	Garantia que a informação não foi alterada após o seu envio ou validação.
	Confiabilidade	Atuação do sistema conforme o esperado.
	Confidencialidade	Sigilo de conteúdo, limitando o seu acesso e uso restrito às pessoas autorizadas.
	Conformidade	Cumprimento de requisitos.
	Disponibilidade	Disponível aos usuários.
	Integridade	Proteção contra alterações indevidas.
	Políticas de segurança	Declarações de papéis e responsabilidades dos empregados para salvaguardar as informações e recursos.

Fonte: Elaborado com base nos Quadros 3, 5 e 7.

O Quadro 9 integrado à aplicação técnica da ISO/IEC 27002 compõe o instrumento de coleta de dados. A proposição teórica desta pesquisa é que as práticas de segurança da informação ISO/IEC 27002 relacionadas às características qualitativas da informação contábil contribuem para a governança corporativa no requisito de conformidade. Apresenta-se no capítulo seguinte a metodologia empregada nesta pesquisa.

3 METODOLOGIA

A seguir apresenta-se a classificação da pesquisa, os procedimentos metodológicos utilizados para a coleta, tratamento e análise dos dados, bem como a empresa em estudo.

3.1 CLASSIFICAÇÃO DA PESQUISA

Esta pesquisa caracteriza-se como descritiva, pois tem como objetivo descrever o comportamento dos fenômenos estudados, de forma a identificar e obter informações sobre as características de um determinado problema ou questão. (COLLIS; HUSSEY, 2005). Sendo assim, procura-se analisar as práticas de segurança da informação contábil no requisito de conformidade da governança corporativa.

A estratégia metodológica utilizada é o estudo de caso único, ou seja, organizado sob um único caso. Segundo Yin (2015, p. 54) “o estudo de caso único pode representar uma contribuição significativa para a formação do conhecimento e da teoria, confirmando, desafiando ou ampliando a teoria”. Desta forma, é considerada uma importante estratégia metodológica, pois permite ao investigador um aprofundamento em relação ao fenômeno estudado e seu diferencial é a capacidade de lidar com uma ampla variedade de evidências: documentos, artefatos, entrevistas e observações.

Quanto a abordagem do problema, delineia-se como qualitativa. Conforme Collis e Hussey (2005) o método qualitativo enfatiza os aspectos subjetivos da atividade humana, focando no significado do fenômeno estudado.

Acredita-se que a metodologia adotada possibilita um aprofundamento no caso estudado de forma a responder a questão de pesquisa e os objetivos propostos neste estudo, podendo ser transferível a outros contextos.

3.2 PROCEDIMENTO DE COLETA DOS DADOS

Como fontes de coleta de dados utilizou-se de questionário, entrevista e documentos, a fim de permitir a triangulação das fontes de dados. Conforme Yin (2015) a triangulação diz respeito ao uso de fontes múltiplas que visam reforçar a validade do construto do estudo de caso.

A primeira etapa para a coleta de dados refere-se à elaboração de um protocolo, conforme “APÊNDICE A”. Segundo Yin (2015) o protocolo é uma tática para se aumentar a confiabilidade da pesquisa e destina-se a orientar o pesquisador à condução do estudo.

A segunda etapa trata-se da aplicação de um questionário (APÊNDICE C) que foi construído mediante a aplicação técnica da ISO/IEC 27002 integrada aos conceitos teóricos apresentados no Quadro 9. Este instrumento possui dois blocos: (1) caracterização do respondente; (2) nível de controle das práticas de segurança da informação dispostas na seção 18 – Conformidade ISO/IEC 27002 (2013) relacionadas às características da informação contábil e à governança corporativa no requisito de conformidade.

Os respondentes do questionário são os funcionários (nível operacional e gerencial) das áreas que se relacionam diretamente com a contabilidade, incluindo os setores: controladoria (contabilidade, fiscal e custos), financeiro, tecnologia da informação (TI) e diretoria administrativa e financeira. A amostra corresponde a 42 funcionários, sendo 35 de nível operacional e 7 gerencial.

A pesquisadora obteve o auxílio de uma informante-chave para proporcionar o acesso aos respondentes e *insights* sobre o assunto pesquisado. Sendo assim, enviou-se o convite (APÊNDICE B) à participação do questionário para a informante-chave, a mesma responsabilizou-se por contatar os gestores. Essa informante-chave disponibilizou para a pesquisadora uma listagem contendo a quantidade, o nome dos funcionários e seus respectivos setores.

Optou-se em aplicar o questionário de forma presencial para os funcionários de nível operacional, conforme sugestão originada do pré-teste realizado com a *plant controller* da empresa analisada. Essa respondente argumentou que a aplicação desse instrumento de forma presencial poderia proporcionar maior taxa de resposta e, principalmente, um melhor entendimento das questões pelos respondentes. Desta forma, as questões contidas no instrumento foram lidas uma a

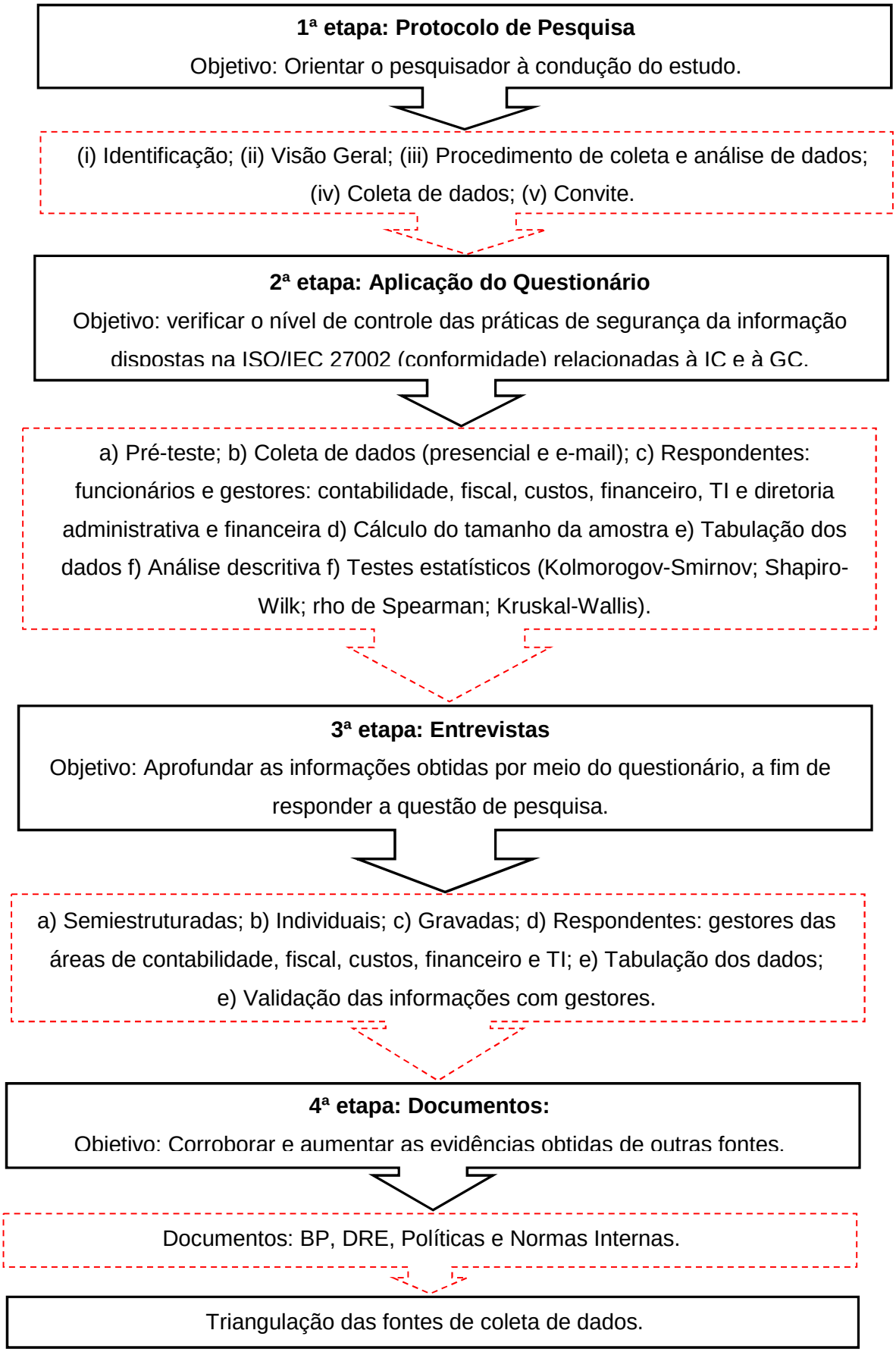
uma pela pesquisadora e esclarecidas a estes funcionários quando necessário. Já para os gestores, o questionário foi aplicado por e-mail.

A terceira etapa da coleta de dados refere-se às entrevistas, cujo objetivo é aprofundar as informações obtidas pelo questionário. Conforme Yin (2015, p. 244) a entrevista “é o modo de coleta de dados que envolve informação verbal de um participante de estudo de caso”. Utilizou-se de entrevistas semiestruturadas, pois possibilitam maior interação entre o entrevistador e o entrevistado, com auxílio de um roteiro com perguntas previamente estabelecidas (APÊNDICE D).

Realizaram-se as entrevistas com 7 gestores os quais possuem os seguintes cargos: coordenador de contabilidade, coordenador fiscal, coordenador de custos e orçamentos, gerente de TI, supervisor de TI, gerente de controladoria e gerente financeiro. As entrevistas foram executadas na empresa analisada de forma individual e gravadas mediante a autorização dos respondentes, para serem transcritas, possibilitando a análise e tratamento dos dados. Após essa transcrição enviou-se para cada gestor suas respectivas respostas para a validação das informações coletadas.

A quarta etapa refere-se à análise documental. O conjunto de documentos considerados no contexto da coleta de dados refere-se ao Balanço Patrimonial (BP), Demonstração do Resultado do Exercício (DRE), Políticas e Normas internas. O uso de documentos serve para corroborar e aumentar a evidência de outras fontes. (YIN; 2015). A Figura 2 apresenta o esquema de coleta de dados para a presente pesquisa.

Figura 2 - Esquema de coleta de dados



Fonte: Elaborado pela autora.

Nota-se na Figura 2, o esquema para a coleta de dados desta pesquisa referente às etapas, objetivos e os procedimentos de coleta.

3.3 TRATAMENTO E ANÁLISE DOS DADOS

Após a coleta dos dados, efetuou-se o tratamento e análise destes. A análise de dados consiste em examinar, categorizar, classificar ou recombinar as evidências do estudo. (YIN, 2015). Primeiramente, verificou-se o tamanho de amostra necessária, dado o grau de confiança almejado por meio da fórmula de população finita. (LEVIN, 1987).

Em síntese, a amostra quanto a aplicação do questionário compreende 42 funcionários de níveis operacional e gerencial, e quanto a aplicação da entrevista corresponde a 7 gestores. Após calcular o tamanho da amostra necessária ao nível de significância de 95%, investigou-se o comportamento dos dados da pesquisa.

3.3.1 Questionário e entrevista

Aplicou-se o instrumento para a coleta de dados em dois momentos. No primeiro momento aplicou-se um questionário em escala do tipo Likert para quantificar. Utilizou-se o *software Statistical Package for Social Science* (SPSS) for *Windows* versão 20.0 para tabular as respostas, onde analisou-se as estatísticas descritivas: média, mediana, desvio padrão, correlação e teste de médias.

Primeiramente, realizou-se a análise descritiva da percepção dos gestores e funcionários de nível operacional, após realizaram-se os testes estatísticos para corroborar essa análise. Esses testes são direcionados para dois grandes grupos: os testes paramétricos e os não-paramétricos.

Segundo Sprent e Smeeton (2016) para que os testes paramétricos possam ser aplicados, é necessário o cumprimento de três principais pressupostos: (i) distribuição normal dos dados, (ii) homogeneidade dos dados e, (iii) variáveis intervalares e contínuas. Já os não-paramétricos podem ser utilizados quando algum dos pressupostos básicos dos testes paramétricos são violados. Desta forma, para verificar o comportamento dos dados, efetuou-se o teste de normalidade Shapiro-

Wilk que, segundo Dancey e Reidy (2013), é utilizado para amostra inferior a 50 observações, condizente com esta pesquisa. Em complemento e, como procedimento de robustez, efetuou-se também o teste de normalidade Kolmogarov-Smirnov. O software SPSS fornece o resultado de ambos os testes.

A hipótese nula de ambos os testes é de que os dados seguem uma distribuição normal. Portanto, se o p-valor do teste for maior que o nível de significância estabelecido pelo pesquisador aceita-se a hipótese nula, permitindo inferir que os dados seguem uma distribuição normal. (CHAKRAVARTI; LAHA, 1967).

Esta pesquisa evoluiu para os testes não-paramétricos em função dos dados não possuírem distribuição normal, sendo que isto foi comprovado na Figura 3 . Desta forma, calculou-se o coeficiente de correlação de *rho* de Spearman (ρ) para verificar a correlação entre os domínios do estudo.

Como procedimento adicional à análise descritiva, analisou-se estatisticamente se há diferença entre a percepção dos funcionários de nível operacional e gerencial, utilizando-se o teste não-paramétrico KW de Kruskal e Wallis (1952). O teste KW possibilita essa análise, verificando se há diferenças entre as médias dos grupos. (DANCEY; REIDY, 2013, p. 539).

No segundo momento, após aplicação do questionário, voltou-se nas questões para qualifica-las e entender “como” determinada prática pode contribuir para a conformidade (APÊNDICE D). Os entrevistados são os gestores responsáveis das seguintes áreas: contabilidade, fiscal, custos/planejamento, controladoria, financeiro e TI, que correspondem a 7 entrevistados.

Utilizou-se o *software Word*® para transcrever as entrevistas e, em seguida efetuou-se a análise dos dados composta por: (i) categorização dos respondentes; (ii) práticas de segurança da informação contábil; e (iii) contribuição para a conformidade.

3.3.2 Documentos

Após as entrevistas e com o objetivo de corroborar as evidências das outras fontes apresentadas anteriormente. Os documentos referem-se às demonstrações contábeis, políticas e normas internas.

Os documentos contemplados nesta pesquisa referem-se à: (i) Política de segurança da informação; (ii) Políticas de tecnologia da informação; (iii) Política corporativa de segurança SAP; (iv) Manual de conduta sobre uso, divulgação e manutenção de sigilo acerca de informações; (v) Código de conduta; (vi) Relatórios dos Auditores Independentes sobre as Demonstrações Financeiras - 2015 e 2014 (RAI) e; (vii) Relatório sobre a Revisão de Informações Trimestrais - 2016.

3.4 EMPRESA EM ESTUDO

O estudo de caso foi do tipo “caso único”, selecionando-se uma indústria metalúrgica localizada no Estado do Rio Grande do Sul. A escolha pela empresa deu-se em função da mesma possuir os seguintes requisitos: (i) é uma empresa de capital aberto regida pelas disposições legais e regulamentares da Lei nº 6.404; (ii) possui classificação no Nível 2 de governança corporativa, (iii) é líder no seu segmento de atuação no Brasil; (iv) disponibilidade em participar da pesquisa.

O contato inicial com a empresa “X” deu-se em dezembro de 2015, de forma presencial com a informante-chave e o Vice-Presidente Administrativo e Financeiro. Explicou-se o objetivo geral da pesquisa e, procurou-se entender as principais características da Companhia, principalmente no que se refere à governança corporativa.

A empresa “X”, assim denominada por questão de sigilo, foi fundada em 1939, possui ações negociadas na BM&FBovespa desde 1982 e ingressou no Nível 2 de governança corporativa em 2011.

O Nível 2 de governança corporativa estabelece regras diferenciadas para a listagem das Companhias, além de regras aplicáveis aos seus administradores e acionistas. Dentre as regras estabelecidas, destacam-se:

(i) autorização para negociação de valores mobiliários no Nível 2 de governança corporativa;

(ii) permitir a negociação de ações ordinárias e/ou preferenciais em bolsa;

(iii) manter o percentual mínimo (25%) de ações em circulação;

(iv) eleição do Conselho de Administração com mandato unificado de no máximo 2 anos, composto por no mínimo 5 membros eleitos em assembleia geral dos quais, 20% deverão ser conselheiros independentes;

(v) os cargos de presidente do conselho de administração e de diretor presidente ou principal executivo da Companhia não poderão ser acumulados pela mesma pessoa;

(vi) informações periódicas observando as condições e prazos previstos na regulação (demonstrações financeiras, formulário de demonstrações financeiras padronizadas, formulário de informações trimestrais, formulário de referência). As demonstrações financeiras devem ser traduzidas para o inglês em até, no máximo, 15 dias contados da divulgação dessas demonstrações.

A empresa “X” atende todos os requisitos dispostos no regulamento de listagem do Nível 2 BM&FBovespa com destaque para: o Conselho de Administração que é formado por 40% de conselheiros independentes; departamento permanente de relações com investidores.

A organização em estudo é líder em seu segmento de atuação no Brasil, detém cerca de 90% de participação de mercado. Seus produtos são comercializados tanto no mercado interno quanto externo, sendo este último o responsável pelo maior faturamento da Companhia com 91% para o mercado norte-americano e 3% para outros países (comercializa seus produtos em mais de 100 países). Já o Brasil representa 6% do faturamento total da empresa.

Quanto ao porte, a empresa possui receita operacional bruta maior que R$ 300 milhões de reais e, segundo o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), classifica-se como grande porte.

Para esta pesquisa, a população refere-se aos funcionários que se relacionam diretamente com a contabilidade, totalizando 51.

Tem como missão satisfazer plenamente as necessidades dos clientes, através da prestação de serviços com padrão de qualidade internacional e a preços competitivos, mantendo o conceito de empresa de classe mundial.

Dentre as ações recentes efetuadas pela empresa “X” destacam-se: (i) a implementação do sistema SAP que se iniciou em dezembro de 2015; (ii) consolidação de fábricas, (iii) renegociação do endividamento, (iv) aumento de produção.

No próximo capítulo apresentam-se os resultados encontrados na pesquisa.

4 ANÁLISE DOS RESULTADOS

Os resultados a seguir fundamentam-se nas informações obtidas dos respondentes, por meio da aplicação do questionário, entrevistas e documentos.

4.1 ANÁLISE QUANTITATIVA - QUESTIONÁRIO

Essa análise de dados se compõe por: caracterização dos respondentes; controle das práticas de segurança da informação contábil; resultados consolidados análise descritiva; teste de normalidade; mapa de correlação entre os domínios *rho* de Spearman e; percepção dos usuários teste Kruskal-Wallis.

Os respondentes do questionário são os funcionários (nível operacional e gerencial) das áreas que se relacionam diretamente com a contabilidade, incluindo os setores: controladoria (contabilidade, fiscal e custos), financeiro, tecnologia da informação (TI) e diretoria administrativa e financeira. A população da pesquisa corresponde a 51 funcionários de nível operacional e gerencial, sendo que a amostra compõe-se de 42 respondentes.

A aplicação do questionário ocorreu em 09/08/2016, os respondentes de nível operacional foram agrupados em turma para facilitar a leitura e entendimento das questões, totalizando 8 turmas. Em média foram 4,375 respondentes por turma e o tempo médio de resposta foi de 39 minutos. Já para o nível gerencial, os funcionários responderam via e-mail. O Quadro 10 apresenta a quantidade de funcionários que responderam o questionário e suas respectivas áreas de atuação.

Quadro 10 - Quantidade de respondentes do questionário

	Quantidade de Funcionários			**Quantidade de Respondentes**			
Setores	**Nível operacional**	**Nível gerencial**	**Total**	**Nível operacional**	**Nível gerencial**	**Total**	**% partic**
Contabilidade	8	2	**10**	8	2	**10**	100,0%
Custos	4	1	**5**	4	1	**5**	100,0%
Financeiro	9	1	**10**	5	-	**5**	50,0%
Fiscal	14	1	**15**	10	1	**11**	73,3%
TI	8	2	**10**	8	2	**10**	100,0%
Diretoria adm e financ.	-	1	**1**	-	1	**1**	100,0%
Total	**43**	**8**	**51**	**35**	**7**	**42**	**82,4%**

Fonte: Dados da pesquisa.

Verifica-se no Quadro 10 que a população refere-se a 51 funcionários, sendo que 82,4% destes responderam o questionário, totalizando uma amostra de 42 respondentes. Destacam-se os setores de contabilidade, custos, tecnologia da informação e diretoria administrativa com 100% de participação cada e, em contrapartida, o setor Financeiro ficou bem abaixo da média, correspondendo 50,0% apenas, seguido pelo setor fiscal com 73,3%.

Primeiramente, verificou-se o tamanho da amostra necessária, dado o grau de confiança almejado. Com base na população desta pesquisa, ou seja 51 funcionários, considerando um nível de confiança de 95%, o tamanho da amostra exigida 37 respondentes. Nesta pesquisa, obteve-se uma amostra de 42 respondentes, confirmando-se, assim, que a amostra obtida é estatisticamente significante ao nível de 95%.

Após utilizou-se os *softwares Excel* e SPSS para tabular as respostas e analisar as estatísticas descritivas como média, mediana, desvio-padrão, correlação e teste de médias.

4.1.1 Categorização dos respondentes

O primeiro bloco do instrumento de coleta refere-se à categorização dos respondentes. Neste bloco evidenciam-se as áreas de atuação, tempo de trabalho, nível de escolaridade e formação acadêmica. A Tabela 1 apresenta a categorização dos respondentes.

Tabela 1 - Categorização dos respondentes de nível operacional e gerencial

Variável	Resposta	Nº	Freq.
Área de atuação na empresa	Contabilidade	10	23,8%
	Custos	5	11,9%
	Financeiro	5	11,9%
	Fiscal	11	26,2%
	Tecnologia da Informação	10	23,8%
	Diretoria adm. e financeira	1	2,4%
	Total	**42**	**100,0%**
Tempo de trabalho na empresa	Menos de 1 ano	17	40,5%
	Entre 1 e 3 anos	9	21,4%
	Entre 3 e 5 anos	5	11,9%
	Mais de 5 anos	11	26,2%
	Total	**42**	**100,0%**

Nível de escolaridade	Superior incompleto	11	26,2%
	Superior completo	14	33,3%
	Pós-graduação	15	35,7%
	Médio completo	1	2,4%
	Mestrado	1	2,4%
	Total	**42**	**100,0%**
Área de formação acadêmica	Ciências contábeis	22	52,3%
	Administração de empresas	12	28,5%
	Análise e desenvolvimento de sistemas	2	4,8%
	Tecnologia da Informação	2	4,8%
	Gestão Financeira	1	2,4%
	Gestão Produção Industrial	1	2,4%
	Redes de computadores	1	2,4%
	Processos gerenciais	1	2,4%
	Total	**42**	**100,0%**

Fonte: Dados da pesquisa.

Na Tabela 1 verifica-se que a amostra corresponde a 42 respondentes, os quais encontram-se nas seguintes áreas: Contabilidade, Custos, Financeiro, Fiscal, Tecnologia da Informação e Diretoria administrativa e financeira. Destaca-se a área Fiscal com 26,2%, seguida das áreas de TI e Contabilidade, ambas com 23,8%.

Evidencia-se também o tempo de trabalho na empresa “X”. Verifica-se que 73,8% dos respondentes possuem menos de 5 anos de empresa. Destaca-se que 40,5% dos respondentes possuem menos de 1 ano de empresa, corroborando com a informação obtida pelo Vice-presidente que a empresa “X” passa por um processo de reestruturação das áreas. Apenas 26,2% dos respondentes possuem mais de 5 anos de trabalho.

A Tabela 1 evidencia também o nível de escolaridade dos respondentes. Destacam-se os níveis de pós-graduação e superior completo com 15 e 14 respondentes, respectivamente. Identificou-se que 11 respondentes possuem superior incompleto. Os níveis de mestrado e médio completo representam apenas 2,4% dos respondentes.

Outra variável apresentada na Tabela 1 refere-se à área de formação acadêmica dos respondentes. Destacam-se Ciências Contábeis com 52,3% seguida de Administração de empresas com 28,5%. Estas áreas representam 80,8% dos respondentes. Os demais percentuais estão distribuídos em outras áreas acadêmicas.

4.1.2 Controle das práticas de segurança da informação contábil

O segundo bloco do questionário tem como objetivo identificar o nível de controle das práticas de segurança da informação dispostas na ISO/IEC 27002 (conformidade) integrado aos conceitos teóricos de segurança da informação, características qualitativas da informação contábil e governança corporativa, totalizando 41 práticas. Apresenta-se no Quadro 11 os níveis de proteção de segurança da informação.

Quadro 11 - Níveis de proteção de segurança da informação

Proteção	Descrição
1 - Inadequada	Não há esforço da empresa para implementar os controles recomendados.
2 – Mínima	A empresa adota o mínimo de controles recomendados.
3 – Razoável	A empresa implementa a maioria dos controles a um nível razoável, satisfazendo os procedimentos escritos e processos.
4 – Adequada	A empresa implementa todos os controles recomendados pelo domínio.
Não aplicável	Considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Fonte: Elaborado com base em Eloff e Eloff (2003).

A partir das estatísticas descritivas (média, mediana, desvio-padrão), verificou-se primeiramente, a percepção dos usuários de nível operacional e, após investigou-se a percepção dos gestores quanto às práticas de proteção de segurança da informação contábil. As percepções foram comparadas descritiva e estatisticamente.

4.1.2.1 Percepção dos usuários: análise descritiva

Na Tabela 2 aborda-se a identificação da legislação aplicável. Nesta questão evidenciam-se os conceitos de conformidade e comparabilidade, por meio da existência de controles específicos e responsabilidades para atender os requisitos estatutários, regulamentares, contratuais permitindo ao usuário sua comparabilidade.

Tabela 2 - Identificação da legislação aplicável

D1. Identificação da legislação aplicável	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
1.1 Os controles específicos e as responsabilidades individuais para atender aos requisitos estatutários, regulamentares, contratuais são definidos e documentados, permitindo ao usuário a identificação de diferenças e semelhanças com as normas no ambiente interno e externo.	0,0%	5,7%	57,1%	34,3%	2,9%	100,0%	0,0%	0,0%	85,7%	14,3%	0,0%	100,0%
					Média	3,2000					Média	3,1430
					Mediana	3,0000					Mediana	3,0000
					Desvio-padrão	0,7971					Desvio-padrão	0,3780

Fonte: Dados da pesquisa.

De acordo com a Tabela 2 verifica-se que 57,1% dos respondentes de nível operacional consideram razoável o nível de proteção referente à identificação da legislação aplicável. Quanto aos respondentes de nível gerencial, 85,7% consideram razoável, isto significa que a empresa implementa a maioria dos controles a um nível razoável, satisfazendo os procedimentos escritos e processos.

Analisando-se sob a ótica da estatística descritiva, verifica-se que a média deste domínio para os respondentes de nível operacional é 3,20 e mediana 3,00. Já a média e mediana referente aos respondentes de nível gerencial é de 3,14 e 3,00, respectivamente. Considerando-se o desvio-padrão pode-se afirmar o nível de proteção das práticas de segurança da informação contábil fica entre 2,40 e 3,99 sob a ótica operacional e, entre 2,77 e 3,51 gerencial.

A segunda questão refere-se aos direitos de propriedade intelectual, evidenciados na Tabela 3.

Tabela 3 - Direitos de propriedade intelectual

D2. Direitos de propriedade intelectual	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
2.1 A divulgação da política de uso legal de produtos de *software* e de informação é exposta de forma compreensível aos usuários atendendo às normas reguladoras no ambiente interno e externo.	2,9%	11,4%	20,0%	65,7%	0,0%	100,0%	0,0%	0,0%	71,4%	28,6%	0,0%	100,0%
2.2 A aquisição de *software* somente por meio de fontes conhecidas e de reputação para assegurar que o direito autoral não está sendo violado ocorre de forma idêntica e uniforme prevenindo o risco por meio de monitoramento e supervisão de processos operacionais.	0,0%	2,9%	8,6%	88,6%	0,0%	100,0%	0,0%	0,0%	42,9%	57,1%	0,0%	100,0%
2.3 A conscientização das políticas para proteger os direitos de propriedade intelectual é considerada útil com vistas à responsabilidade pelas ações próprias ou dos outros.	2,9%	0,0%	42,9%	54,3%	0,0%	100,0%	0,0%	14,3%	28,6%	57,1%	0,0%	100,0%
2.4 A manutenção e identificação dos registros de ativos para proteger os direitos de propriedade intelectual ocorre sem omissão ou distorção, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa.	0,0%	8,6%	45,7%	42,9%	2,9%	100,0%	0,0%	14,3%	42,9%	42,9%	0,0%	100,0%
2.5 A manutenção de provas e evidências de propriedade (ex: licenças, manuais, acessos) evitam a omissão ou distorção nas decisões dos usuários, mediante a responsabilidade sobre as ações próprias ou dos outros.	0,0%	14,3%	22,9%	60,0%	2,9%	100,0%	0,0%	0,0%	57,1%	42,9%	0,0%	100,0%
2.6 Os controles neutralizam os vieses e asseguram que o número máximo de usuários permitidos não exceda o número de licenças adquiridas por meio do cumprindo normas de regulação do ambiente interno.	0,0%	2,9%	28,6%	68,6%	0,0%	100,0%	0,0%	14,3%	71,4%	14,3%	0,0%	100,0%
2.7 As verificações de aquisição e instalação de *software* autorizados e licenciados ocorre de forma mais completa possível, sem omissão de algum fato relevante, permitindo um clima de confiança.	2,9%	0,0%	20,0%	74,3%	2,9%	100,0%	0,0%	0,0%	42,9%	57,1%	0,0%	100,0%
2.8 A política para a manutenção das condições adequadas de licenças é exposta de forma compreensível ao usuário, contribuindo para uma boa imagem perante os *stakeholders*.	2,9%	8,6%	45,7%	42,9%	0,0%	100,0%	0,0%	28,6%	28,6%	42,9%	0,0%	100,0%
2.9 A política para disposição ou transferência de *software* é exposta de forma compreensível ao usuário contribuindo na prevenção de risco, monitoramento e supervisão contínua dos processos.	0,0%	14,3%	48,6%	34,3%	2,9%	100,0%	0,0%	28,6%	42,9%	28,6%	0,0%	100,0%
2.10 O cumprimento de termos e condições para *software* e informação obtidos a partir de redes públicas pode ser verificável prevenindo o risco, monitoramento e supervisão contínua dos processos.	0,0%	5,7%	31,4%	60,0%	2,9%	100,0%	0,0%	14,3%	42,9%	42,9%	0,0%	100,0%
2.11 Não copiar no todo ou em partes documentos em geral, além daqueles permitidos pela lei de direito autoral. Este procedimento evita as manipulações e deve considerar o comportamento ético e moral.	0,0%	2,9%	31,4%	62,9%	2,9%	100,0%	42,9%	0,0%	42,9%	14,3%	0,0%	100,0%
					Média	3,5140					Média	3,2000
					Mediana	3,6000					Mediana	3,4000
					Desvio-padrão	0,3882					Desvio-padrão	0,5972

Fonte: Dados da pesquisa.

Destacam-se na Tabela 3 que os respondentes de nível operacional e gerencial possuem a mesma percepção para as questões sobre a aquisição de *software* (2.2), conscientização das políticas de proteção (2.3), verificações de aquisição e instalações de *software* (2.7), considerando-as como adequadas. O mesmo ocorre para as políticas de disposição ou transferência de software (2.9), porém encontra-se em nível regular. Evidenciam-se nestas questões os conceitos de confiabilidade, uniformidade, risco, políticas de segurança, utilidade, responsabilidade, autenticidade, integridade, transparência e compreensibilidade.

Em contrapartida, há um desalinhamento de percepção quanto à manutenção de provas e evidências de propriedade (2.5) e controles de licenças (2.6). Os respondentes de nível operacional consideram estas práticas adequadas, enquanto que o gerencial atribui o nível razoável de proteção. Apresentam-se os conceitos de integridade, materialidade, responsabilidade, conformidade, e neutralidade.

Não há consenso dos respondentes de nível gerencial referente ao cumprimento de termos e condições para software e informações obtidos a partir de redes públicas (2.10). Nesta questão, 42,9% consideram razoável e 42,9% adequado. Já na percepção operacional, 60% consideram essa prática adequada. Abordam-se os conceitos de conformidade, verificabilidade e risco.

Também não há consenso para a proteção de cópias de documentos em geral (2.11). Os gestores atribuem às práticas de segurança da informação contábil os níveis inadequado e razoável com 42,9% cada. Já 62,9% dos respondentes operacionais consideram essa prática adequada. Evidenciam-se os conceitos de autenticidade, representação fidedigna e ética.

Analisando-se as estatísticas descritivas deste domínio, no nível operacional, verifica-se que sua média é de 3,51 e 3,60 de mediana. Já para o nível gerencial a média é de 3,20 e 3,40 de mediana. De acordo com o desvio-padrão, pode-se afirmar o nível de proteção entre 3,12 e 3,90 para o nível operacional e, entre 2,60 e 3,80 para o nível gerencial.

Na Tabela 4 apresentam-se as questões referentes à proteção de registros organizacionais.

Tabela 4 - Proteção de registros organizacionais

D3. Proteção de registros organizacionais	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
3.1 Os registros são categorizados em tipos (ex: registros contábeis, bases de dados, de transações) e são disponibilizados em tempo hábil, permitindo um clima de confiança.	0,0%	17,1%	45,7%	34,3%	2,9%	100,0%	42,9%	0,0%	42,9%	14,3%	0,0%	100,0%
3.2 Os registros armazenados possuem detalhes de proteção ao longo do tempo e estão disponíveis em local adequado.	8,6%	11,4%	37,1%	40,0%	2,9%	100,0%	0,0%	0,0%	71,4%	28,6%	0,0%	100,0%
3.3 As chaves de criptografia ou assinaturas digitais são armazenadas de forma a permitir a decifração de registros pelo período de tempo que os registros são mantidos. Elas estão livres de erros, vieses e manipulações, auxiliando na prevenção de riscos, monitoramento e supervisão contínua dos processos.	0,0%	8,6%	48,6%	31,4%	11,4%	100,0%	0,0%	42,9%	14,3%	42,9%	0,0%	100,0%
3.4 Os cuidados quanto a possibilidade de deterioração das mídias armazenadas ocorre de forma semelhante para itens afins dentro da estrutura organizacional.	2,9%	11,4%	42,9%	31,4%	11,4%	100,0%	0,0%	42,9%	14,3%	42,9%	0,0%	100,0%
3.5 Os procedimentos para assegurar a capacidade de acesso aos dados contra perdas ocasionadas pelas futuras mudanças na tecnologia, permitem aos usuários identificar diferenças e semelhanças, interpretando e avaliando os regulamentos para limitar as perdas.	0,0%	20,0%	42,9%	34,3%	2,9%	100,0%	0,0%	0,0%	57,1%	42,9%	0,0%	100,0%
3.6 O dado pode ser recuperado de forma aceitável, mais completa possível e sem omissão, por meio de monitoramento e supervisão contínua dos processos.	0,0%	22,9%	34,3%	40,0%	2,9%	100,0%	0,0%	0,0%	42,9%	57,1%	0,0%	100,0%
3.7 A destruição apropriada dos registros, caso não sejam mais necessários à organização, ocorre com cautela cumprindo normas reguladoras no ambiente interno e externo.	0,0%	17,1%	28,6%	45,7%	8,6%	100,0%	0,0%	28,6%	42,9%	28,6%	0,0%	100,0%
3.8 A emissão de diretrizes gerais para retenção, armazenamento, tratamento e disposição de registro de informações é capaz de predizer resultados futuros por meio de normas reguladoras no ambiente interno e externo.	0,0%	17,1%	45,7%	28,6%	8,6%	100,0%	0,0%	28,6%	42,9%	28,6%	0,0%	100,0%
3.9 A programação para retenção, precisa identificar os registros essenciais e o período que cada um deve ser mantido de forma disponível e acessível aos usuários.	0,0%	11,4%	65,7%	17,1%	5,7%	100,0%	0,0%	28,6%	57,1%	14,3%	0,0%	100,0%
3.10 A manutenção de um inventário das fontes de informações-chave ocorre em tempo hábil permitindo o acesso às informações para a tomada de decisão.	0,0%	22,9%	54,3%	11,4%	11,4%	100,0%	14,3%	28,6%	28,6%	28,6%	0,0%	100,0%
					Média	3,1770					Média	3,0140
					Mediana	3,3000					Mediana	3,3000
					Desvio-padrão	0,5151					Desvio-padrão	0,7493

Fonte: Dados da pesquisa.

Nota-se na Tabela 4 a mesma percepção quanto às práticas de acesso aos dados (3.5), diretrizes gerais de proteção dos registros organizacionais (3.8) e programação para retenção (3.9). Os respondentes de nível operacional e gerencial consideram razoável as práticas de segurança da informação contábil. Já para a recuperação de dados (3.6), ambos respondentes atribuem o nível adequado. Evidenciam-se os conceitos de integridade, comparabilidade, avaliação de risco, política de segurança, preditiva, conformidade, confiabilidade, disponibilidade e acessibilidade.

Para as questões sobre armazenamento dos registros (3.2) e destruição apropriada dos registros (3.7), os respondentes operacionais consideram as práticas adequadas, enquanto que os de nível gerencial razoável. Abordam-se os conceitos de integridade, disponibilidade, locais funcionais, política de segurança, prudência ou conservadorismo e conformidade.

Para a questão referente à proteção dos registros categorizados em tipos bem como a sua disponibilidade em tempo hábil para a tomada de decisão (3.1), 45,7% dos respondentes de nível operacional consideram o nível razoável de proteção. Em contrapartida, no nível gerencial, 42,9% considera inadequada e 42,9% razoável, não há um consenso. Nesta questão evidenciam-se os conceitos de disponibilidade, tempestividade e transparência.

Também não há um consenso do nível gerencial para as questões referentes às chaves de criptografia (3.3), armazenamento de mídias (3.4) e manutenção de inventário das fontes de informações-chave (3.10). Porém os respondentes operacionais consideram razoável a proteção. Abordam-se os conceitos de disponibilidade, representação fidedigna, risco, política de segurança, consistência, locais funcionais, tempestividade e acessibilidade.

Analisando-se a estatística descritiva dos respondentes tem-se a média de 3,17 e mediana 3,30 para o nível operacional e 3,01 e 3,30 para o gerencial. Considerando o desvio padrão pode-se afirmar que os níveis de proteção deste domínio estão entre 2,66 e 3,69 para o nível operacional e entre 2,26 e 3,76 para o gerencial.

Na Tabela 5 apresentam-se as questões referentes à proteção e privacidade de informações de identificação pessoal.

Tabela 5 - Proteção e privacidade de informações de identificação pessoal

D4. Proteção e privacidade de informações de identificação pessoal	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
4.1 A política de privacidade e proteção de dados da organização é relevante, pois permite interpretar e avaliar os regulamentos para limitar as perdas.	**2,9%**	**2,9%**	**40,0%**	**48,6%**	**5,7%**	**100,0%**	**0,0%**	**28,6%**	**14,3%**	**57,1%**	**0,0%**	**100,0%**
4.2 A comunicação da política de privacidade e proteção de dados a todas as pessoas envolvidas no processo é exposta de forma mais compreensível possível ao usuário, possibilitando a construção de uma boa imagem perante os seus *stakeholders*.	**2,9%**	**17,1%**	**48,6%**	**25,7%**	**5,7%**	**100,0%**	**0,0%**	**14,3%**	**42,9%**	**42,9%**	**0,0%**	**100,0%**
4.3 Existe uma pessoa responsável (*privacy officer*) que tem a função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos a serem seguidos. Essas orientações devem ser expostas de forma compreensível ao usuário, possibilitando um padrão de excelência operacional percebida pelos *stakeholders*.	**25,7%**	**20,0%**	**17,1%**	**22,9%**	**14,3%**	**100,0%**	**0,0%**	**28,6%**	**57,1%**	**14,3%**	**0,0%**	**100,0%**
					Média	**3,0000**					**Média**	**3,1430**
					Mediana	**3,0000**					**Mediana**	**3,3000**
					Desvio-padrão	**0,8059**					**Desvio-padrão**	**0,6604**

Fonte: Dados da pesquisa.

Verifica-se na Tabela 5 que os respondentes de nível operacional e gerencial possuem a mesma percepção referente a política de privacidade e proteção de dados (4.1), ambos a consideram adequada, com 48,6% e 57,1% respectivamente. Esta questão evidencia os conceitos de confidencialidade, relevância e avaliação de risco.

Quanto à comunicação da política de privacidade e proteção de dados (4.2) a percepção dos níveis difere-se. A percepção do nível operacional é razoável (48,6%), enquanto que nos nível gerencial não há um consenso, 42,9% consideram razoável e 42,9% adequada. Também não há um consenso, porém desta vez na percepção operacional, quanto à existência de *privacy officer* (4.3). Obtiveram-se as seguintes respostas: 25,7% inadequada; 20,0% mínima; 17,1% razoável; 22,9% adequada e 14,3% não aplicável. No nível gerencial, 57,1% dos respondentes de nível gerencial a consideram razoável. Essa questão aborda os conceitos de política de segurança, compreensibilidade e criação de valor.

A média e mediana deste domínio, para os respondentes de nível operacional, encontra-se em nível regular de 3,00 e 3,00. Para os respondentes de nível gerencial, verificou-se 3,14 e 3,30 de média e mediana, respectivamente. Considerando-se o desvio padrão pode-se afirmar que o nível de proteção deste domínio está entre 2,19 e 3,80 para o operacional e, entre 2,48 e 3,80 para o gerencial.

Na Tabela 6 apresentam-se as questões relacionadas à regulamentação de controles de criptografia.

Tabela 6 - Regulamentação de controles de criptografia

D5. Regulamentação de controles de criptografia	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
5.1 As restrições quanto ao uso de criptografia ocorrem com cautela de acordo com o cumprimento de normas reguladoras internas.	0,0%	20,0%	34,3%	31,4%	14,3%	100,0%	14,3%	14,3%	57,1%	14,3%	0,0%	100,0%
5.2 A assessoria jurídica garante a conformidade com as legislações e regulamentações possibilitando a informação livre de erros, vieses e manipulações por meio do cumprimento de normas internas e externas.	0,0%	22,9%	40,0%	31,4%	5,7%	100,0%	0,0%	0,0%	71,4%	28,6%	0,0%	100,0%
					Média	2,9570					Média	3,0000
					Mediana	3,0000					Mediana	3,0000
					Desvio-padrão	1,0100					Desvio-padrão	0,6455

Fonte: Dados da pesquisa.

Verifica-se na Tabela 6 que não há um consenso dos respondentes de nível operacional quanto às restrições ao uso de criptografia (5.1), 34,3% consideram razoável e 31,4% adequado. Já 57,1% dos respondentes de nível gerencial consideram razoável. Abordam-se os conceitos de confidencialidade, prudência ou conservadorismo e conformidade.

Quanto à assessoria jurídica (5.2) os respondentes possuem a mesma percepção, ambos consideram razoável o nível de proteção, 40% para os de nível operacional e 71,4% para os de nível gerencial. Nesta questão evidenciam-se os conceitos de conformidade e representação fidedigna.

A estatística descritiva, para os respondentes de nível operacional, deste domínio é de 2,95 de média e 3,00 de mediana, sugerindo que este domínio encontra-se em nível regular de proteção. Os respondentes de nível gerencial também consideram regular a proteção, obteve-se 3,00 de média e 3,00 de mediana. Porém o nível de dispersão indicado pelo desvio-padrão sob a ótica operacional é maior do que os outros domínios, ou seja, 1,01. Isto indica que estatisticamente não há um consenso destes respondentes. Quanto à ótica gerencial, pode-se afirmar que o nível de proteção deste domínio está entre 2,35 e 3,64.

Na Tabela 7 mostram-se as questões relacionadas à análise crítica independente da segurança da informação.

Tabela 7 - Análise crítica independente da segurança da informação

D6. Análise crítica independente da segurança da informação	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
6.1 A análise crítica da segurança da informação é iniciada pela direção de forma confiável para que o usuário aceite a informação e a utilize, construindo uma boa imagem perante os *stakeholders*.	**2,9%**	**11,4%**	**54,3%**	**22,9%**	**8,6%**	**100,0%**	**0,0%**	**42,9%**	**28,6%**	**28,6%**	**0,0%**	**100,0%**
6.2 A análise crítica inclui a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação, evidenciando suas diferenças e semelhanças para a busca de excelência operacional percebida pelos *stakeholders*.	**2,9%**	**20,0%**	**42,9%**	**28,6%**	**5,7%**	**100,0%**	**0,0%**	**42,9%**	**28,6%**	**28,6%**	**0,0%**	**100,0%**
6.3 A análise crítica inclui política e objetivos de controle relevantes, capazes de fazer a diferença na gestão preventiva de riscos, monitoramento e supervisão contínua dos processos.	**0,0%**	**22,9%**	**51,4%**	**14,3%**	**11,4%**	**100,0%**	**0,0%**	**42,9%**	**28,6%**	**28,6%**	**0,0%**	**100,0%**
6.4 A análise crítica é executada por pessoas independentes (ex: auditoria interna, gerente independente ou uma organização externa especializada em tais análises críticas), refletindo de fato o que ocorreu independente de um contrato. Deve fornecer evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever.	**2,9%**	**17,1%**	**28,6%**	**34,3%**	**17,1%**	**100,0%**	**0,0%**	**28,6%**	**42,9%**	**28,6%**	**0,0%**	**100,0%**
6.5 Os resultados da análise crítica independente são registrados e relatados à direção, de forma neutra não havendo viés de resultado por meio de informações úteis aos usuários permitindo um clima de confiança.	**2,9%**	**14,3%**	**37,1%**	**28,6%**	**17,1%**	**100,0%**	**0,0%**	**14,3%**	**57,1%**	**28,6%**	**0,0%**	**100,0%**
6.6 A direção efetua ações corretivas quando os resultados da análise crítica forem inadequados ou não conforme pela segurança da informação, para garantir a confiança da informação e cumprir com obrigações de suas responsabilidades.	**5,7%**	**25,7%**	**28,6%**	**25,7%**	**14,3%**	**100,0%**	**0,0%**	**14,3%**	**42,9%**	**42,9%**	**0,0%**	**100,0%**
					Média	**2,7970**					**Média**	**3,0000**
					Mediana	**2,8000**					**Mediana**	**2,7000**
					Desvio-padrão	**0,9212**					**Desvio-padrão**	**0,7141**

Fonte: Dados da pesquisa.

Destacam-se na Tabela 7 as questões sobre análise crítica e segurança da informação que envolve a iniciativa da diretoria (6.1), avaliação de oportunidades para melhoria e necessidades de mudanças (6.2) e inclusão de políticas e objetivos de controle (6.3). Para estas questões a percepção quanto às práticas de segurança da informação contábil dos respondentes de nível operacional é razoável, já para os de nível gerencial a percepção é mínima, ou seja, a empresa adota o mínimo de controles recomendados. Destacam-se nestas questões os conceitos de política de segurança, confiabilidade, reputação corporativa, comparabilidade, criação de valor, relevância e risco.

Referente à execução da análise crítica por pessoas independentes (6.4) não há um consenso dos respondentes. Os de nível operacional consideram adequada, enquanto que os de nível gerencial razoável, correspondendo a 34,3% e 42,9% respectivamente. Abordam-se os conceitos de política de segurança, primazia da essência sobre a forma e legitimidade. O consenso também não prevalece quanto à execução das ações corretivas pela direção (6.6). Nesta questão, a percepção dos respondentes de nível operacional divide-se em: mínima, razoável e adequada, correspondendo a 25,7%, 28,6% e 25,7% respectivamente. O mesmo ocorre para os respondentes de nível gerencial, a percepção refere-se a 42,9% razoável e 42,9% adequada. Nesta questão abordam-se os conceitos de conformidade, confiabilidade e responsabilidade.

A única questão em que há a mesma percepção quanto às práticas de segurança da informação contábil diz respeito ao registro e relato dos resultados da análise crítica à direção (6.5). Ambos os níveis de respondentes a consideram razoável, ou seja, a empresa implementa a maioria dos controles a um nível razoável, satisfazendo os procedimentos escritos e processos. Evidencia-se nesta questão os conceitos de integridade, neutralidade e transparência.

Analisando-se as estatísticas descritivas de média, mediana e desvio-padrão dos respondentes de nível operacional tem-se 2,79, 2,80 e 0,92, respectivamente. Para os de nível gerencial verificou-se 3,00 de média, 2,70 de mediana e 0,71 de desvio-padrão. Considerando-se o desvio padrão, pode-se afirmar que os níveis de proteção deste domínio estão entre 1,87 e 3,71 para o nível operacional e entre 2,28 e 3,71 para o gerencial. Na Tabela 8 evidenciam-se as questões referentes à conformidade com as políticas e procedimentos de segurança da informação.

Tabela 8 - Conformidade com as políticas e procedimentos de SI

D7. Conformidade com as políticas e procedimentos de segurança da informação	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
7.1 Os gestores identificam as causas quando há qualquer não conformidade, evidenciando as diferenças e semelhanças, por meio de um comportamento ético e moral.	5,7%	11,4%	48,6%	25,7%	8,6%	100,0%	0,0%	14,3%	57,1%	28,6%	0,0%	100,0%
7.2 Os gestores implementam ações corretivas após a detecção da não conformidade de forma mais completa possível, sem omissão de algum fato relevante, atuando com responsabilidade pelas ações próprias ou dos outros.	5,7%	25,7%	40,0%	20,0%	8,6%	100,0%	0,0%	14,3%	57,1%	28,6%	0,0%	100,0%
7.3 Os gestores analisam criticamente as ações corretivas tomadas para predizer resultados futuros, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever.	8,6%	17,1%	48,6%	20,0%	5,7%	100,0%	0,0%	28,6%	42,9%	28,6%	0,0%	100,0%
7.4 Os resultados das análises críticas e das ações corretivas pelos gestores são registradas e mantidas mediante informações íntegras e tempestivas de acordo com as normas reguladoras internas e externas.	5,7%	34,3%	37,1%	14,3%	8,6%	100,0%	0,0%	28,6%	57,1%	14,3%	0,0%	100,0%
7.5 Os gestores relatam os resultados para as pessoas que estão efetuando a análise crítica independente, identificando as diferenças e semelhanças das informações permitindo um clima de confiança.	5,7%	31,4%	42,9%	14,3%	5,7%	100,0%	0,0%	28,6%	57,1%	14,3%	0,0%	100,0%
					Média	2,6510					Média	3,0000
					Mediana	2,8000					Mediana	3,0000
					Desvio-padrão	0,9547					Desvio-padrão	0,6733

Fonte: Dados da pesquisa.

Verifica-se na Tabela 8 um consenso de percepção para as questões relacionadas ao domínio de conformidade na identificação das causas por parte dos gestores (7.1), implementação de ações corretivas após a detecção (7.2), análise crítica dessas ações corretivas (7.3) e relato dos resultados por parte dos gestores às pessoas que efetuam a análise crítica independente (7.5). Os respondentes consideram razoável o nível de proteção, sugerindo que a empresa implementa a maioria dos controles a um nível razoável, satisfazendo os procedimentos escritos e processos. Abordam-se nestas questões os conceitos de autenticidade, comparabilidade, ética, integridade, responsabilidade, conformidade, preditiva, legitimidade, confiabilidade e transparência.

Referente ao registro dos resultados das análises críticas e ações corretivas (7.4), pode-se dizer que não há um consenso dos respondentes de nível operacional, 34,3% acreditam que o nível é mínimo e 37,1% consideram nível razoável de proteção. Já 57,1% dos respondentes de nível gerencial a consideram razoável. Nesta questão abordam-se os conceitos de disponibilidade, oportunidade e conformidade.

A média, mediana e desvio padrão deste domínio, na percepção dos respondentes de nível operacional, são de 2,65, 2,80 e 0,95, respectivamente. Para os de nível gerencial tem-se 3,00, 3,00 e 0,67. Pode-se afirmar que os níveis de proteção deste domínio estão entre 1,69 e 3,60 sob a ótica operacional e, entre 2,32 e 3,67 sob a ótica gerencial.

Na Tabela 9 apresentam-se as questões referentes à análise crítica da conformidade técnica.

Tabela 9 - Análise crítica da conformidade técnica

D8. Análise crítica da conformidade técnica	Respondentes nível operacional						Respondentes nível gerencial					
	1	2	3	4	NA	Total	1	2	3	4	NA	Total
8.1 A verificação de conformidade técnica deve ter apoio de uma ferramenta automática para a interpretação do especialista técnico, proporcionando um consenso, interpretação e avaliação de regulamentos para limitar as perdas.	**5,7%**	**22,9%**	**42,9%**	**20,0%**	**8,6%**	**100,0%**	**0,0%**	**42,9%**	**57,1%**	**0,0%**	**0,0%**	**100,0%**
8.2 Os testes de invasão ou avaliações de vulnerabilidades são planejados, documentados e repetidos quando incertezas estiverem envolvidas, para prevenir riscos, monitorando e supervisionando continuamente os processos operacionais.	**2,9%**	**34,3%**	**25,7%**	**28,6%**	**8,6%**	**100,0%**	**0,0%**	**57,1%**	**42,9%**	**0,0%**	**0,0%**	**100,0%**
8.3 A verificação de conformidade técnica somente é executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas, de forma a garantir a informação mais completa e sem omissão de algum fato relevante, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa.	**0,0%**	**11,4%**	**48,6%**	**34,3%**	**5,7%**	**100,0%**	**0,0%**	**0,0%**	**100,0%**	**0,0%**	**0,0%**	**100,0%**
					Média	**2,8770**					**Média**	**2,6570**
					Mediana	**3,0000**					**Mediana**	**2,7000**
					Desvio-padrão	**0,8875**					**Desvio-padrão**	**0,3505**

Fonte: Dados da pesquisa.

Verifica-se na Tabela 8 que há um consenso dos respondentes em todas as questões deste domínio. Para as questões sobre a verificação de conformidade técnica (8.1 e 8.3), ambos respondentes consideram a proteção razoável. Quanto aos testes de invasão e vulnerabilidades (8.2) a percepção de proteção atribuída pelos respondentes é mínima. Neste domínio abordam-se os conceitos de confiabilidade, verificabilidade, avaliação de risco, autenticidade, prudência ou conservadorismo, risco, confidencialidade, integridade e legitimidade.

Na percepção operacional, a média, mediana e desvio padrão, correspondem a 2,87, 3,00 e 0,88, respectivamente. Na percepção gerencial tem-se a média 2,6570 e a mediana que corresponde a 2,70 e 0,35 de desvio-padrão. Pode-se afirmar que os níveis de proteção estão entre 1,98 e 3,76 sob a ótica operacional e, entre 2,30 e 3,00 sob a ótica gerencial.

4.1.2.1.1 Resultados consolidados: análise descritiva

Os resultados consolidados sob a percepção dos usuários de nível operacional e gerencial são evidenciados no Quadro 12.

Quadro 12 – Resultados consolidados sob a ótica operacional e gerencial

	Nível operacional			Nível gerencial		
Domínio	**Média**	**Mediana**	**Desvio-padrão**	**Média**	**Mediana**	**Desvio-padrão**
D1	3,2000	3,0000	0,7971	3,1430	3,0000	0,3780
D2	3,5140	3,6000	0,3882	3,2000	3,4000	0,5972
D3	3,1770	3,3000	0,5151	3,0140	3,3000	0,7493
D4	3,0000	3,0000	0,8059	3,1430	3,3000	0,6604
D5	2,9570	3,0000	1,0100	3,0000	3,0000	0,6455
D6	2,7970	2,8000	0,9212	3,0000	2,7000	0,7141
D7	2,6510	2,8000	0,9547	3,0000	3,0000	0,6733
D8	2,8770	3,0000	0,8875	2,6570	2,7000	0,3505

Fonte: Dados da pesquisa.

Verifica-se no Quadro 12 que a mediana dos domínios, sob a ótica operacional, é igual ou maior do que 3,00, exceto para os domínios D6 e D7, que é de 2,80 cada. O domínio D6 refere-se à análise crítica independente da segurança da informação e o domínio D7 representa a conformidade com as políticas e procedimentos de segurança da informação. Analisando-se a percepção sob a ótica operacional, os

dados apresentados sugerem que a proteção das práticas de segurança da informação contábil encontram-se em nível razoável, a empresa implementa a maioria dos controles, satisfazendo os procedimentos escritos e processos.

O mesmo ocorre quanto à percepção dos gestores, de forma geral estes respondentes também consideram razoável o nível de proteção, exceto para os domínios D6 e D8. O domínio D6 que refere-se à análise crítica independente da segurança da informação, assim como na percepção operacional, ficou abaixo da mediana na percepção gerencial. O mesmo ocorreu para o domínio D8 que representa a análise crítica da conformidade técnica.

Analisando-se as estatísticas descritivas, conclui-se que os níveis gerenciais e operacionais possuem percepção semelhante, sugerindo que a proteção das práticas de segurança da informação contábil encontra-se em nível razoável.

Na continuação, apresenta-se o teste de normalidade dos dados desta pesquisa.

4.1.3 Teste de normalidade

Para verificar a normalidade dos dados desta pesquisa, efetuou-se os testes Kolmogorov-Smirnov e Shapiro-Wilk. A hipótese nula de ambos os testes é de que os dados seguem uma distribuição normal. Portanto, se o p-valor do teste for inferior ao nível de significância de 0.05, a hipótese nula é rejeitada, permitindo inferir que os dados não seguem uma distribuição normal. (CHAKRAVARTI; LAHA, 1967). Na Figura 3 sintetizam-se os resultados dos testes realizados.

Figura 3 – Teste de normalidade Kolmogorov-Smirnov e Shapiro-Wilk

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estatística	df	Sig.	Estatística	df	Sig.
d1	,327	42	,000	,684	42	,000
d2	,206	42	,000	,849	42	,000
d3	,131	42	,069	,958	42	,129
d4	,141	42	,035	,914	42	,004
d5	,158	42	,010	,847	42	,000
d6	,132	42	,065	,867	42	,000
d7	,153	42	,014	,886	42	,001
d8	,161	42	,008	,906	42	,002

a. Lilliefors Significance Correction

Fonte: Dados da pesquisa.

Considerando um nível de significância de 10%, verifica-se na Figura 3, que a hipótese nula de normalidade é rejeitada pelo teste Shapiro-Wilk em todos os domínios, pois os p-valores (Sig.) são inferiores a 0.10, exceto para o domínio D3 que possui um p-valor de 0,129, este domínio refere-se à proteção de registros organizacionais. Os resultados de não normalidade são corroborados pelo teste Kolmogorov-Smirnov onde, verifica-se que em todos os domínios apresentados a hipótese de normalidade é rejeitada.

Desta forma, conclui-se que os dados apresentados na Figura 3 não seguem uma distribuição normal, portanto recorre-se ao coeficiente de correlação não-paramétrico de *rho* de Spearman para calcular a correlação entre os domínios.

4.1.4 Mapa de correlação entre os domínios: rho de Spearman

As correlações das percepções dos respondentes de nível operacional e gerencial foram calculadas mediante o *software* SPSS versão 20.0 referente aos domínios evidenciados na norma ISO/IEC 27002 (2013) da seção 18 – Conformidade. No Quadro 13 apresentam-se esses domínios.

Quadro 13 – Domínios da norma ISO/IEC 27002 seção conformidade

Domínio	Descrição
D1	Identificação da legislação aplicável
D2	Direitos de propriedade intelectual
D3	Proteção de registros organizacionais
D4	Proteção e privacidade de informações de identificação pessoal
D5	Regulamentação de controles de criptografia
D6	Análise crítica independente de segurança da informação
D7	Conformidade com as políticas e procedimentos de segurança da informação
D8	Análise crítica da conformidade técnica

Fonte: Dados da pesquisa.

A correlação entre os domínios foi calculada por meio do coeficiente de correlação rho de Spearman, esse coeficiente varia de -1 a 1. O sinal indica a direção que pode ser positiva ou negativa do relacionamento das variáveis, enquanto que o valor sugere a força da relação entre as variáveis.

Para interpretar o coeficiente de rho de Spearman, utiliza-se nesta pesquisa, a classificação de Dancey e Reidy (2013), onde: ρ=0,10 até 0,30 (fraco); ρ=0,40 até 0,60 (moderado); ρ=0,70 até 1 (forte). Quanto mais próximo de 1, independente do sinal, maior é o grau de dependência estatística entre as variáveis e, quanto mais próximo de 0, menor é a força desta relação.

Na Figura 4 apresenta-se a correlação entre os domínios utilizando a correlação rho de Spearman.

Figura 4 – Correlação entre os domínios rho de Spearman

Correlações

			d1	d2	d3	d4	d5	d6	d7	d8
Rô de Spearman	d1	Correlações de coeficiente	1,000	,305*	,194	,251	,474**	,351*	,133	,200
		Sig. (2 extremidades)	.	,050	,217	,109	,002	,023	,401	,203
		N	42	42	42	42	42	42	42	42
	d2	Correlações de coeficiente	,305*	1,000	,615**	,656**	,510**	,518**	,406**	,414**
		Sig. (2 extremidades)	,050	.	,000	,000	,001	,000	,008	,006
		N	42	42	42	42	42	42	42	42
	d3	Correlações de coeficiente	,194	,615**	1,000	,682**	,585**	,437**	,544**	,387*
		Sig. (2 extremidades)	,217	,000	.	,000	,000	,004	,000	,011
		N	42	42	42	42	42	42	42	42
	d4	Correlações de coeficiente	,251	,656**	,682**	1,000	,614**	,476**	,621**	,515**
		Sig. (2 extremidades)	,109	,000	,000	.	,000	,001	,000	,000
		N	42	42	42	42	42	42	42	42
	d5	Correlações de coeficiente	,474**	,510**	,585**	,614**	1,000	,624**	,568**	,591**
		Sig. (2 extremidades)	,002	,001	,000	,000	.	,000	,000	,000
		N	42	42	42	42	42	42	42	42
	d6	Correlações de coeficiente	,351*	,518**	,437**	,476**	,624**	1,000	,521**	,395**
		Sig. (2 extremidades)	,023	,000	,004	,001	,000	.	,000	,010
		N	42	42	42	42	42	42	42	42
	d7	Correlações de coeficiente	,133	,406**	,544**	,621**	,568**	,521**	1,000	,653**
		Sig. (2 extremidades)	,401	,008	,000	,000	,000	,000	.	,000
		N	42	42	42	42	42	42	42	42
	d8	Correlações de coeficiente	,200	,414**	,387*	,515**	,591**	,395**	,653**	1,000
		Sig. (2 extremidades)	,203	,006	,011	,000	,000	,010	,000	.
		N	42	42	42	42	42	42	42	42

*. A correlação é significativa no nível 0,05 (2 extremidades).

**. A correlação é significativa no nível 0,01 (2 extremidades).

Fonte: Dados da pesquisa.

A Figura 4 evidencia o cálculo da correlação entre os domínios e também a significância dos resultados encontrados. Analisando-se os valores obtidos e, apesar da existência do nível de significância nos domínios, verifica-se que a magnitude da correlação é fraca ou moderada. Desta forma, destacam-se apenas os seguintes domínios com correlação forte:

- D3 com D4: a proteção de registros organizacionais está significativamente relacionada com a proteção e privacidade de informações de identificação pessoal;

- D4 com D2: a proteção e privacidade de informações de identificação pessoal está significativamente relacionada com os direitos de propriedade intelectual;

- D7 com o D8: a conformidade com as políticas e procedimentos de segurança da informação está significativamente relacionada com a análise crítica da conformidade técnica.

Estes domínios correspondem a 0,682; 0,656 e 0,653, respectivamente.

Com base nos resultados encontrados, conclui-se que a correlação é fraca em 5 domínios, moderada em 20 e forte em 3 domínios.

4.1.5 Percepção dos usuários: teste Kruskal-Wallis

Como procedimento adicional à análise descritiva, analisou-se estatisticamente se há diferença entre a percepção dos funcionários de nível operacional e gerencial. Utilizou-se o teste não-paramétrico de Kruskal-Wallis (KW), pois os dados desta pesquisa não seguem uma distribuição normal comprovado pelos testes Shapiro-Wilk e Kolmogorov–Smirnov realizados anteriormente.

O Kruskal-Wallis “é equivalente não paramétrico de ANOVA e uma generalização do teste Mann-Whitney”. (DANCEY; REIDY, 2013, p. 539). A fórmula do “Kruskal-Wallis baseia-se nos postos dos escores, o teste procura uma diferença significativa entre os postos médios, se não existem diferenças significativas entre os grupos, os postos médios tenderão a ser parecidos”. (DANCEY; REIDY, 2013, p. 539).

A hipótese nula do teste Kruskal-Wallis é que os grupos têm a mesma distribuição, ou seja, os respondentes de nível gerencial e operacional possuem a mesma distribuição. Utiliza-se como medida de tendência central a mediana, ao invés da média. (DANCEY; REIDY, 2013, p. 542). Apresentam-se os postos médios (*mean rank*) dos domínios na Figura 5.

Figura 5 – Postos médios Kruskal-Wallis

Ranks

	DUMMY	N	Mean Rank
d1	0	7	19,29
	1	35	21,94
	Total	42	
d2	0	7	16,00
	1	35	22,60
	Total	42	
d3	0	7	19,57
	1	35	21,89
	Total	42	
d4	0	7	22,93
	1	35	21,21
	Total	42	
d5	0	7	20,79
	1	35	21,64
	Total	42	
d6	0	7	22,00
	1	35	21,40
	Total	42	
d7	0	7	25,14
	1	35	20,77
	Total	42	
d8	0	7	17,07
	1	35	22,39
	Total	42	

Fonte: Dados da pesquisa.

Na Figura 5 apresenta-se a variável dummy a qual assume-se os valores 0 para os funcionários de nível gerencial e, 1 para os de nível operacional. Nota-se que os postos médios do nível gerencial (dummy 0) são menores que os postos médios do nível operacional (dummy 1), exceto para os domínios de proteção e privacidade de informações de identificação pessoal (D4), análise crítica independente da segurança da informação (D6), e conformidade com as políticas e procedimentos de segurança da informação (D7). Porém, para analisar se há diferença estatística entre essas médias, apresenta-se na Figura 6 o teste Kruskal-Wallis para os 8 domínios.

Figura 6 – Teste estatístico Kruskal Wallis

Test Statistics[a,b]

	d1	d2	d3	d4	d5	d6	d7	d8
Chi-quadrado	,373	1,716	,209	,117	,030	,014	,751	1,137
df	1	1	1	1	1	1	1	1
Significância Assintótica	,541	,190	,648	,732	,863	,906	,386	,286

a. Kruskal Wallis Test

b. Variável de agrupamento: DUMMY

Fonte: Dados da pesquisa.

Verifica-se na Figura 6 que o teste estatístico de Kruskal-Wallis segue uma distribuição qui-quadrada (χ^2) e, com base nos resultados evidenciados pode-se observar que em todos os domínios o grau de concordância não difere estatisticamente entre os níveis gerencial e operacional. Sendo assim, aceita-se a hipótese nula de que os grupos, gerencial e operacional, têm a mesma distribuição, pois a significância (Asymp. Sig.) é maior do que os níveis tradicionais de significância estatística de 1%, 5% e/ou 10%.

Por meio do teste estatístico KW corrobora-se a análise descritiva apresentada no capítulo anterior de que, em geral, a percepção gerencial e operacional é semelhante.

Finalmente, conclui-se os achados da pesquisa relacionando o enfoque quantitativo:

- a amostra obtida é estatisticamente significante ao nível de 95%, considerando o cálculo de tamanho da amostra;

- a percepção dos níveis gerencial e operacional é semelhante. Identificou-se que o nível de segurança da informação contábil é Razoável, isto é, a empresa analisada implementa a maioria dos controles, satisfazendo os procedimentos escritos e processos;

- os dados da pesquisa não seguem uma distribuição normal, razão pela qual utilizou-se testes não paramétricos;

- apenas nos domínios D3 com D4; D4 com D2; D7 com D8 possuem correlação forte e são estatisticamente significantes ao nível de 1%, portanto o grau de confiança é de 99%;

- a percepção dos níveis gerencial e operacional é estatisticamente igual, comprovado pelo teste não paramétrico de Kruskal-Wallis, corroborando a análise descritiva.

Com isso, conclui-se todas as análises quantitativas e, na continuação desenvolve-se as análises das entrevistas que respondem a questão problema evidenciada nesta pesquisa.

4.2 ANÁLISE QUALITATIVA - ENTREVISTAS

Essa análise qualitativa das entrevistas se compõe por: categorização dos entrevistados e; práticas de segurança da informação contábil.

As entrevistas foram realizadas com os gestores responsáveis dos seguintes setores: coordenador de contabilidade, coordenador fiscal, coordenador de custos/planejamento, supervisor de TI, gerente de TI, gerente financeiro e gerente de controladoria, totalizando 7 entrevistados. Os entrevistados são os mesmos gestores que participaram do instrumento de coleta anterior (questionário), porém desta vez, com o objetivo de aprofundar a questão de pesquisa e situação estudada.

As entrevistas foram agendadas pela informante-chave, a mesma verificou a disponibilidade dos dias e horários dos gestores. As entrevistas foram realizadas na própria empresa, nos dias 25/11/2016 e 28/11/2016. Essas entrevistas foram gravadas com o objetivo de manter a fidedignidade das respostas e tiveram duração média de 1,40 hora. As respostas foram transcritas para o *Microsoft Word*® e, após foram enviadas aos gestores para a validação da informação obtida.

Utilizou-se o protocolo de entrevista (APÊNDICE D) que contém as perguntas semiestruturadas, as questões contidas nesse protocolo também serviram como um roteiro à pesquisadora para validar se os relatos abordavam as práticas em estudo.

4.2.1 Categorização dos entrevistados

Evidencia-se na Tabela 10 a categorização dos entrevistados de nível gerencial, contemplando as áreas de atuação, tempo de trabalho, nível de escolaridade e formação acadêmica.

Tabela 10 - Categorização dos entrevistados

Variável	Resposta	Nº	Freq.
Área de atuação na empresa	Contabilidade/Controladoria	2	28,57%
	Custos	1	14,28%
	Financeiro	1	14,28%
	Fiscal	1	14,28%
	Tecnologia da Informação	2	28,57%
	Total	**7**	**100,0%**
Tempo de trabalho na empresa	Menos de 1 ano	1	14,28%
	Entre 1 e 3 anos	2	28,57%
	Mais de 5 anos	4	57,14%
	Total	**7**	**100,0%**
Nível de escolaridade	Pós-graduação	7	100,0%
	Total	**7**	**100,0%**
Área de formação acadêmica	Ciências contábeis	4	57,14%
	Administração de empresas	2	28,57%
	Tecnologia da Informação	1	14,28%
	Total	**7**	**100,0%**

Fonte: Dados da pesquisa.

Na Tabela 10 verifica-se um total de 7 entrevistados, que encontram-se nas seguintes áreas: Contabilidade, Custos, Financeiro, Fiscal e Tecnologia da Informação. O gerente de controladoria está locado no setor de contabilidade, embora seja responsável pelos setores: contabilidade, fiscal e custos.

Evidencia-se também o tempo de trabalho na empresa “X”. Verifica-se que 42,85% dos gestores possuem menos de 5 anos de empresa, sendo que 57,14% tem mais de 5 anos. A Tabela 1 apresenta também o nível de escolaridade dos gestores, com destaque para o nível de pós-graduação, que corresponde a 100% dos entrevistados.

Outra variável abordada na Tabela 1 refere-se à área de formação acadêmica. Destacam-se Ciências Contábeis com 57,14% seguida de Administração de empresas com 28,57% e Tecnologia da Informação com 14,28%.

A seguir, apresentam-se as práticas de segurança da informação contábil sob a percepção desses gestores.

4.2.2 Práticas de segurança da informação contábil

As questões de pesquisa (APÊNDICE D) referem-se aos 8 domínios da norma ISO/IEC 27002 (2013) integrados com as características qualitativas da informação contábil e com a governança corporativa no requisito de conformidade, totalizando 41 práticas. Para a análise das entrevistas utilizou-se o *software* de *Microsoft Word*®.

Apresenta-se a seguir os resultados encontrados sob a ótica dos gestores entrevistados.

- **1. Identificação da legislação aplicável (D1):**

1.1)	Esta questão verifica como são os controles específicos e as responsabilidades individuais para atender aos requisitos regulamentares, se estes são definidos e documentados, permitindo ao usuário a identificação de diferenças e semelhanças com as normas do ambiente interno e externo. Conceitos: conformidade; comparabilidade; conformidade.

De acordo com as respostas obtidas nas entrevistas, identificou-se que os setores de contabilidade e fiscal possuem um *checklist* das atividades a serem realizadas. Este *checklist* possibilita o acompanhamento dos processos, bem como a cumprimento das atividades.

Conforme a coordenadora de contabilidade "*na contabilidade temos o fechamento mensal, o controle do fechamento é feito através de checklist dos processos das empresas. O analista responsável pelo checklist verifica a efetivação do registro contábil e valida juntamente com os responsáveis dos processos*".

Sob a ótica da área fiscal, o *cheklist* é um instrumento importante para o cumprimento e atendimento das normas no ambiente interno e externo: *"Na área fiscal nós temos um cronograma, uma agenda tributária, nós temos definidos cada pessoa que é responsável e sua área. Dependemos de prazos, precisamos atender os prazos para evitar riscos. Temos as rotinas fixas [...] o checklist ajuda no cumprimento das atividades [...] a gente passa por este checklist para evitar que a gente esqueça alguma coisa*".

Outro controle evidenciado nestas áreas e que inclui a área de custos/planejamento é a conciliação. Conforme a coordenadora da contabilidade "*Temos as conciliações que são realizadas mensalmente onde controlamos saldos e pendências das contas*". O mesmo ocorre no "*fiscal também faz a conciliação contábil-fiscal e depois temos a auditoria externa da KPMG que faz a revisão também*".

Neste sentido, a coordenadora de custos/planejamento comenta sobre o envolvimento dessas áreas, especificamente para a construção do DRE "*hoje nós temos uma auditoria externa, a KPMG, que nos informa as alterações de legislação, seja contábil, fiscal, por exemplo".*

A controladoria integra as três áreas: contabilidade, fiscal e custos/ planejamento. Conforme o gerente da controladoria (contador e *controller* da empresa) o sistema SAP deve ser utilizado como o pilar básico e, o acesso às transações deve ocorrer somente por pessoas autorizadas. O *controller* afirma: "*Eu diria que hoje este deve ser o nosso principal controle é não permitir que outras áreas tenham acesso a determinadas movimentações*".

Outro processo evidenciado pelo gerente de controladoria é o controle de indicadores, este permite a identificação de diferenças e semelhanças, possibilita o monitoramento do processo, bem como a comparação de informações. O mesmo ocorre para a área de TI. Os indicadores são utilizados para medir os serviços e *links* de comunicação entre as diversas áreas da empresa.

O supervisor de TI explica como estes serviços são controlados: "*A maior parte dos controles de atendimentos que a gente faz são feitos pelo sistema de chamados [...] todas as demandas chegam por ele e, é por ele que a gente faz os atendimentos, as demandas da empresa*". Isto é corroborado pela gerente de TI: "*nós avaliamos os chamados feitos, então no nosso sistema de chamados nós temos diversos relatórios e gráficos que conseguem demonstrar se os chamados estão sendo atendidos no tempo previsto, ou se tem algo pendente [...] além disso, a gente procura fazer reuniões rápidas [...] reunião de equipe [...] isso acontece para todos ficarem atualizadas, para um ajudar o outro inclusive*".

Na área financeira, identificou-se que o controle de pagamentos é feito de forma segura. Existem alçadas diferentes para a liberação dos pagamentos. Neste sentido o gerente financeiro afirma: "*Toda e qualquer transação financeira da*

empresa tem que ser assinada por dois procuradores, isto é uma norma. Então sempre há quatro olhos para verificar as transações financeiras, isto é importante".

Questionou-se os gestores quanto ao atendimento destes controles aos requisitos estatutários, regulamentares e contratuais e, todos os gestores responderam que eles atendem, porém os gerentes de controladoria e financeiro destacaram que não são suficientes.

A coordenadora contábil afirma que "*através desses controles garantimos que os registros sejam consistentes com os processos da companhia, nos garantem demonstrações financeiras que reflitam a situação patrimonial nas datas base e que atendam a legislação vigente, essas demonstrações e nossos controles sofre auditoria independente trimestralmente*".

Na percepção da coordenadora de custos/planejamento os "*[...] controles atendem, nós temos o VSM dos nossos processos internos, conciliações, mas eu acho que a auditoria externa contribui muito hoje para este atendimento*".

Segundo o supervisor de TI *"Estes controles inclusive são registrados na qualidade, nós os controlamos mensalmente tem um mínimo que é acordado para de disponibilidade, que significa manter o sistema online".* Isto é corroborado pela gerente de TI *"esses controles que fizemos hoje atendem o nosso acordado, que é manter o sistema disponível para o usuário".*

A coordenadora do fiscal afirma: "*A gente sempre pode melhorar, mas eu diria que hoje estes controles estão bem alinhados". Já o gerente de controladoria explicita alguns controles que poderiam ser melhorados: "Eu acho que eles atendem, mas eles não são suficientes [...] falando em normas e contratos [...] o bloqueio do sistema, as conciliações são algumas ferramentas de controles, mas não são todas*".

O gerente financeiro explicita também um exemplo: "*Eu acho que atendem, mas não são suficientes ainda [...] muitas áreas conseguem efetuar esses lançamentos, pois cada área tem o seu key user para lançar. Então o que acontece, por exemplo uma FV60 para serviço deve ser anexado o documento, mas pode acontecer do pagamento ser efetuado sem o documento suporte para o pagamento*".

Indagou-se também se esses controles são definidos e documentados. Quanto à definição dos controles, estes são definidos de acordo com os processos existentes a empresa conta com um *key user* em cada área e, este é o responsável por isso.

Tratando-se especificamente sobre a documentação, a coordenadora da contabilidade respondeu: *"Nós documentamos na nossa pasta na rede [...] o checklist, as planilha Excel, as conciliações [...] outros controles como posição de clientes e fornecedores, estão dentro de SAP".* O mesmo ocorre na área de custos/planejamento: "*os controles são arquivados em uma pasta que fica disponível na rede da empresa, até por que nós reportamos à diretoria sobre estes controles".*

A coordenadora fiscal complementa que: *"Ficam na pasta do fiscal na rede e temos também um manual POP que fizemos para quase todo o processo da área fiscal, em torno de 80% das nossas tarefas tem POP*".

No que refere-se à área de TI, conforme a gerente os controles são registrados no sistema de chamados e esta informação é corroborada pelo supervisor de TI: "*[...] quando se abre um chamado fica registrado e documentado no sistema. Para os controles de disponibilidade dos sistemas, nós salvamos todo o mês o relatório que apresenta sua disponibilidade e salvamos esses documentos na rede. Hoje toda a empresa tem acesso aos indicadores da TI*". Isto é corroborado pela gerente de TI: *"[...] fica documentado via o registro no sistema de chamados".*

Quanto à identificação de diferenças e semelhanças, a percepção dos gestores também converge. Segundo a coordenadora da contabilidade "*As conciliações nos permitem analisar a evolução e movimentação das contas e validar esses saldos. O SAP possui as demonstrações parametrizadas com relatórios comparativos que também nos permite identificar distorções*".

A coordenadora fiscal afirmou "*Na conciliação se consegue verificar algum erro [...] a gente consegue verificar se há uma parametrização mal feita. Fazemos mensalmente a conciliação em mais de 20 contas contábeis-fiscais*".

Na área de TI, o supervisor de TI respondeu que essa identificação ocorre, afirmando: "*Com certeza. A ideia destes controles é aderir às normas, precisa estar alinhados com as normas para a gente atender as expectativas da empresa*". A percepção da coordenadora de custos/planejamento é de que "*[...] eu acredito que estes controles paralelos que nós fazemos hoje, nos permitem entender o que o sistema está fazendo*".

No que refere-se às responsabilidades individuais, todos os gestores acreditam que as responsabilidades individuais estão definidas. Neste sentido, O gerente de controladoria explicou que essa definição é oriunda das suas coordenadoras. Segundo o este gestor: "*A questão da divisão das responsabilidades*

individuais hoje está nas mãos dos coordenadores, dentro da minha área eu tenho [...] três coordenadores [...] eu cheguei a pouco tempo na organização, então esta estrutura já estava montada e eu não vi a necessidade de mudança, acho que as coordenadoras [...] são donas dos processos [...] elas tem que ter autonomia para gerenciar o seu processo [...] o meu papel é muito mais na orientação e algumas sugestões que eu possa dar dentro do processo".

Na contabilidade "*o analista responsável pelo checklist verifica a efetivação do registro contábil e valida juntamente com os responsáveis dos processos (gestão de pessoas, comercial financeiro, custos, etc.)*". Referente a essas responsabilidades a coordenadora fiscal comentou: "*A responsabilidade individual é definida pelo conhecimento que o funcionário tem, hoje as atividades mais complexas são feitas por um analista pleno, hoje eu não tenho analista sênior, estes fazem a entrega do compliance das obrigações [...]*".

O requisito de equipe enxuta foi comentado pela coordenadora de custos/planejamento e gerente de TI. Conforme a coordenadora de custos/planejamento: "*Dentro da nossa área, hoje nós somos cinco pessoas [...] temos uma equipe muito enxuta, fica cada uma com o seu processo, quando uma sai, a outra pessoa tem que dar o suporte*".

No mesmo pensamento, a gerente de TI relata: "*Hoje nós temos uma equipe reduzida, mas que conseguimos atender os chamados, com grandes dificuldades, mas a gente consegue [...] as responsabilidades a gente divide em negócios e infraestrutura [...] as pessoas de negócios ficam responsáveis por alguns módulos no SAP [...] a gente divide estes módulos para que eles se tornem especialistas na própria operação, [...] o mesmo ocorre para a equipe de infraestrutura, algumas pessoas têm mais acessos do que outras*".

Isto é corroborado pelo supervisor de TI: "*Hoje nós tratamos por funcionais, por que daí o funcionário de TI consegue ter maior entendimento sobre a área que ele está atuando, conhecer os processos daquele módulo na qual ele acompanha. Na parte de infraestrutura, nós temos a administração que controla os usuários da rede e tem o suporte que dá o suporte para o sistema*".

Na área financeira, de acordo com o gerente, cada funcionário tem a sua responsabilidade: "*o nível de acesso do sistema é conforme os acessos das transações de suas áreas, a única pessoa que tem acesso a tudo é a key user da área, mas mesmo a key user há uma restrição, por exemplo o acesso bancário: a*

key user do contas a receber não consegue fazer pagamento, então há sim restrições de acesso".

Analisando-se as entrevistas, conclui-se que todas as práticas apresentadas no domínio D1 são utilizadas pela empresa em estudo.

Por fim, questionou-se aos gestores quanto à contribuição destas práticas (controles; atendimento das normas, responsabilidades individuais, documentação dos controles, identificação de diferenças e semelhanças) para a conformidade. Constatou-se que todos os gestores acreditam que elas contribuem.

Segundo a coordenadora da contabilidade "*Os controles nos permitem garantir que as informações foram efetivadas e são consistentes. Esses controles, desde o checklist até a conciliação e validação dos saldos contábil, são necessários para a elaboração das demonstrações financeiras sem distorções. Os trabalhos de auditoria são conduzidos de acordo com as normas brasileiras e internacionais de auditoria e validados de acordo com as práticas contábeis adotadas no Brasil e com as normas internacionais de relatório financeiro (IFRS) emitidas pelo International Accounting Standards Board (IASB). Esses controles nos garante a conformidade das Demonstrações*".

A coordenadora fiscal também acredita na contribuição destas práticas: "*Se os controles não existirem não se tem a certeza se o processo está certo. É necessário tanto o controle fiscal quanto o controle contábil, as duas informações se completam, juntamente com o sistema. Eu acredito que desta forma a gente consiga mostrar que está tudo em conformidade*".

Na percepção da coordenadora de custos/planejamento, a contribuição destas práticas está nos controles que são feitos paralelamente ao sistema SAP: "*O que eu enxergo hoje é que a gente consegue contribuir por que a gente tem esses controles paralelos [...] na minha visão, esses controles que fazemos hoje contribuem para seguir a conformidade, eles contribuem na própria validação das informações*".

O gerente de controladoria afirma que estas práticas: "*contribuem de forma vital, porque hoje o sistema faz o que as pessoas mandam, então é muito importante que a gente tenha as pessoas treinadas, as pessoas nas suas áreas de responsabilidade, com as suas atribuições bem definidas. [...] eu acho que isso facilita muito na confiabilidade da informação [...]".*

Na perspectiva do gerente financeiro "*estas normas definem um padrão e o padrão é muito importante. A gente até pode discutir se o padrão está ou não correto, daí é uma questão de até que ponto a empresa quer assumir o risco e até que ponto a empresa quer ser mais ágil. Por exemplo, quando se tem muitas travas o processo é mais seguro, mas o processo não é tão ágil e, quando menos travas o processo é mais ágil, mas não é tão seguro. Então definir isso é muito importante para decidir o modelo que se quer.*

Sob a ótica da área de TI, o supervisor de TI afirma que as práticas contribuem para a conformidade da seguinte forma: "*Eu acredito que garantindo que as informações estarão disponíveis quando forem solicitadas, seja para o usuário interno quanto externo*". Já na percepção da gerente de TI: [...] *a regra tem que ser seguida para manter a conformidade, essa é a primeira diretriz [...] eu acho que essas práticas contribuem, mas não quer dizer que sejam suficientes, a gente sempre pode melhorar*".

Aborda-se a seguir as práticas relacionadas ao domínio D2.

- **2. Direitos de propriedade intelectual (D2):**

2.1)	Esta questão verifica como ocorre a divulgação da política de uso legal de produtos de software e de informação. Ela deve ser exposta de forma compreensível aos usuários atendendo às normas reguladoras no ambiente interno e externo. Conceitos: política de segurança; compreensibilidade; conformidade.

Verificou-se nas entrevistas que todos os gestores, exceto os gestores de contabilidade e financeiro, relataram que há uma política de uso legal de produtos e softwares e esta é divulgada no momento que o funcionário ingressa na empresa, porém eles acreditam que essa política deveria ser mais divulgada.

A coordenadora do custos/planejamento explicou: "*A empresa tem essa política e ela é divulgada quando o funcionário entra na empresa, quando ele é contratado. O novo funcionário recebe as orientações não só de software, mas dos bens da Companhia* [...] *ela não é disseminada na empresa, ocorre apenas quando o funcionário entre na empresa*".

Isto é corroborado pela coordenadora fiscal que relatou: “*Quando eu entrei na empresa eu recebi um computador e um celular, eu sou a responsável por eles. A gente assina um termo de responsabilidades, lá consta o que pode e não pode fazer. Em relação ao software, eu não tenho certeza, a gente assina também um termo de responsabilidade, tipo um código de conduta, eu só posso usar as informações do sistema de forma correta para o meu trabalho [...] eu acho que ela poderia ser mais divulgada*”. Já a coordenadora contábil acredita na existência desta política e que deve estar na área de TI, mas não forneceu mais detalhes sobre esta questão.

O gerente de controladoria explica também: *“quando eu cheguei eu tive acesso à política que me foi passada pela área de TI através de e-mail, tive também um contato pessoal com as pessoas da área de TI, onde fui informado dos procedimentos [...] “eu não tenho o conhecimento de outra forma de divulgação, até pelo pouco tempo de empresa. Eu desconheço se a área de TI a cada tanto tempo distribui ou reforça*”.

Ainda sobre esta questão, a área de TI explica em detalhes como é a política de uso legal, bem como sua divulgação. Conforme a gerente de TI: “*Nós temos uma política de TI, que ela é divulgada no momento que a pessoa entra na empresa, ela recebe uma integração onde é dito que existe esta política. Nesta integração são passadas algumas diretrizes desta política pela área de TI [...] por exemplo, na área administrativa: você vai receber um usuário de rede, senha a qual deve ser trocada periodicamente, essa senha tem que ter “X” caracteres, você não pode divulgar essa senha para ninguém, ela é de uso pessoal e intransferível se você divulgar fica sob a sua responsabilidade os acessos, a gente fala que eles serão monitorados, que tudo fica registrado no sistema, os acessos à internet também vai ser monitorado, e este monitoramento pode ser feito a qualquer momento pela TI e, em cima de qualquer pessoa [...] o funcionário assina um documento que ele tem conhecimento disso e o RH guarda esse documento*”.

O supervisor de TI acrescenta que esta política está documentada e disponível também na rede para os usuários. Em contrapartida, os gestores de contabilidade e financeiro desconhecem esta política, estes gestores responderam: “*Eu desconheço. Deve ter*”.

Outra abordagem desta questão é a compreensão destas políticas pelos os usuários, bem como o atendimento das mesmas no ambiente interno e externo.

Neste sentido todos os gestores acreditam que os usuários a compreendem, apenas os gestores contábil e financeiro que não responderam a questão anterior, pois não sabem da existência dessa política.

De acordo com a coordenadora fiscal: "*Os usuários sabem o que eles podem usar e também o que não pode. Por exemplo, no horário do expediente a utilização do sistema de forma correta, não usar a parte se sistema para outros fins. Eu acho que essas normas atendem os ambientes*".

A coordenadora de custos/planejamento tem a mesma percepção: "*Os funcionários sabem que essa política existe [...] eu acho que elas atendem as normas, mas eu acredito que vai muito da responsabilidade de cada um*".

Neste sentido, o gerente da controladoria abordou: "*Eu acho que sim [compreensão dos usuários das políticas] a gente pode ter algum desvio pontual, mas de certa forma eles têm um bom entendimento*".

A gerente de TI também acredita que eles a compreendem, porém salientou a importância de reforçar essa política: "*Eu acho que eles compreendem, mas acho que é importante de tempo em tempo a gente reforçar essa compreensão, para que eles não esqueçam, lembrem que existe a política [...] eu acho que essas normas atendem aos ambientes*".

O supervisor de TI complementa: "*Quando ela é revisada ela é publicada, toda a empresa é comunicada [...] as políticas são divulgadas na rede. Hoje estas normas atendem a empresa interna e externamente*".

2.2)	Esta questão verifica se a aquisição de software ocorre somente por meio de fontes conhecidas e de reputação para assegurar que o direito autoral não está sendo violado e, se isto ocorre de forma idêntica e uniforme prevenindo o risco por meio de monitoramento e supervisão de processos operacionais. Conceitos: confiabilidade; uniformidade; risco.

Constatou-se que a aquisição de software somente ocorre por fontes conhecidas e de reputação, porém os gestores de controladoria e custos desconhecem o processo. Conforme a coordenadora fiscal: "*Só pode ser comprada por meio de fontes conhecidas. Hoje nós utilizamos o SAP, o Mastersaf que é para os livros fiscais. São estes dois sistemas que nós utilizamos*".

A coordenadora contábil complementa: “*A empresa tem como regra adquirir softwares de fontes seguras, procura fornecedores qualificados, que tenham experiência e já estejam há algum tempo no mercado [...] o fornecedor deverá estar presente para nos dar suporte e até mesmo para atender as necessidades de crescimento da empresa*”.

O gerente financeiro explicita essa aquisição e o controle também é feito pela empresa que dispõem do software, segundo o gerente: “*Sim, com certeza [aquisição de software por meio de fontes reconhecidas] até por que o SAP controla quantos usuários estão acessando o sistema, há um número limitado de usuários, isto é auditado pela própria SAP até remotamente*”.

Referente a esta questão, a gerente de TI afirma que a aquisição de software por meio de fontes conhecidas e de reputação ocorre para todos os softwares da empresa, ela comenta também sobre o processo de compra: “[...] *se essa ferramenta nos foi apresentada por algum e-mail que recebemos, ou uma empresa que ligou, a gente faz o primeiro reconhecimento, ver se essa ferramenta é útil para a empresa, se for a gente já envolve o setor de compras [...] que faz essa análise, até para que não haja preferência, e depois se faz uma análise, um gráfico inclusive, [...] o setor de compras compara 3 propostas, mostrando a questão de valores. Aí nós da TI olhamos e dizemos em relação a aplicabilidade do software, através de uma visão técnica da nossa área*”. Neste sentido, o supervisor de TI afirma: “*nós sabemos quais as empresas que podem ou não fornecer o software*”.

Em contrapartida, o gerente de controladoria e a coordenadora de custos/planejamento, não têm conhecimento desse processo de aquisição de *software*. Conforme o gerente: “*Eu não tenho o conhecimento, não presenciei, não vivenciei. Seria muito mais um filing de achar que sim”.*

Quanto ao processo de uniformidade de compra do *software*, as coordenadoras fiscal e contábil acreditam que há, porém não sabem como ocorre. Já o gerente financeiro afirma que: “*O processo segue uma regra de compras [...] a questão das três cotações”.* Isso é corroborado pelo supervisor de TI. Segundo o supervisor de TI: “[...] o *procedimento de compra de um software segue um rito, uma uniformidade como qualquer outra aquisição. A aquisição entra como um procedimento de compras, só que como é um software a TI é envolvida isto está escrito na política de TI*”. A gerente de TI complementa: “*compras compara as 3*

propostas, mostrando a questão de valores. Aí nós da TI olhamos e dizemos em relação a aplicabilidade do software, através de uma visão técnica da nossa área".

Questionou-se também aos gestores, se estas práticas, de adquirir um *software* somente por meio de fontes conhecidas e a uniformidade do processo de compra, previnem o risco para a empresa. Todos os gestores responderam que sim, que elas previnem o risco, apenas o gerente de controladoria e a coordenadora de custos/planejamento não responderam, pois desconhecem estas práticas.

De acordo com a coordenadora contábil estas práticas reduzem o risco "[...] *precisamos de garantias de que a implantação e os objetivos serão alcançados a [...] o fornecedor deverá estar presente para nos dar suporte e até mesmo para atender as necessidades de crescimento da empresa".*

A coordenadora fiscal afirma: "*Com certeza. Por que temos a confiabilidade, dentro de um software estão todas as informações da empresa, de todas as áreas, então se você não trabalhar com uma empresa que tenha um software reconhecido, por exemplo, um software pirata, eu acredito que se tenha o risco de divergência das informações e o vazamento destas informações [...] eu entendo que eles também têm uma responsabilidade pela segurança das informações*".

Nesta mesma abordagem de segurança das informações, o gerente financeiro afirma: "*Com certeza protege, primeiro por que evita qualquer tipo de software pirata, as máquinas são todas bloqueadas, se eu por ventura quiser baixar o pdf da internet o meu computador é bloqueado para isto, por que tem uma regra para a aquisição de software e aí protege o capital intelectual da empresa, evitando multas, recolhimento de máquinas [...]".*

A gerente de TI também acredita que essas práticas reduzem os riscos: "*Sim, por que existe uma regra e esta é cumprida, consequentemente o risco é mitigado". Isto é corroborado pelo supervisor de TI: "reduz o risco de invasões, protege a empresa, pois o fornecedor tem responsabilidade também sobre a segurança da informação".*

2.3)	Esta questão verifica a conscientização das políticas para proteger os direitos de propriedade intelectual, se estas são consideradas úteis e com vistas à responsabilidade das ações próprias ou dos outros. Conceitos: política de segurança; utilidade; responsabilidade.

Verificou-se que os gestores do financeiro, controladoria, custos/planejamento, fiscal e contabilidade, não sabem se existe a conscientização dessas políticas de proteção. O supervisor de TI comenta: "*A conscientização eu não sei, eu sei que eles não tem permissão de instalar software [...] isso é bloqueado*".

A gerente de TI ressalta: "*A conscientização é que eu acho que tem que ser reforçada e, esta constantemente. É no trabalho do dia-a-dia mesmo, no atendimento, na hora que está se falando com o gestor, ressaltar lembrar. A conscientização é o mais difícil, por exemplo: o empréstimo da senha [...] essa conscientização é que tem que ser reforçada diariamente. Isso eu tenho percebido uma grande dificuldade [...] nós [TI] fazemos esse trabalho, eu digo que é um trabalho de formiguinha, um trabalho diário de conscientização [...] todos devem entender que a informação é o valor mais precioso que a empresa tem*".

2.4)	Esta questão verifica como é a manutenção e identificação dos registros de ativos para proteger os direitos de propriedade intelectual, se estes ocorrem sem omissão ou distorção, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa. Conceitos: autenticidade; materialidade; legitimidade.

Identificou-se que os gestores do financeiro, controladoria, custos/planejamento e contabilidade, não sabem como ocorre a manutenção e identificação desses registros para a proteção dos direitos intelectual. Alguns gestores explicaram que este processo é especificamente da área de TI.

A coordenadora de custos/planejamento relatou: "[...] *não sei, eu acho que isso é mais com a área de TI. O que nós sabemos é a parte de valor, agora de aquisição, como é feita a manutenção essas coisas não sei te dizer".* Já a coordenadora fiscal explicou como ocorre o registro de ativos: "*Os registros de ativos a gente faz fiscalmente, somente quando todas as etapas do processo estão em conformidade. Por exemplo: a compra de um ativo é feita somente mediante uma análise viabilidade que depois de aprovada gera uma ordem de compra e é enviada ao fornecedor e depois se faz o recebimento fiscal".*

Quanto à omissão ou distorção mediante essa manutenção, bem como a percepção dos *stakeholders* sobre isso, o supervisor de TI afirma: "*É praticamente*

impossível pelo fato das pessoas não poderem instalar o software. Hoje para que o usuário consiga instalar um software tem que ter permissão de administrador. Internamente a gente sabe quando um usuário quer instalar algo indevido, mas externamente eu acho que eles não têm como saber".

Neste sentido, a gerente de TI relata: "*Distorções no sentido do usuário entregar a sua senha ao colega [...] isso é um trabalho de conscientização [...] é uma coisa que nos incomoda bastante, nós da área de TI queremos que tudo seja feito de acordo com as regras para ninguém distorcer ou burlar algo no sistema [...] Isso a gente internamente consegue visualizar em infraestrutura [...] mas externamente eu acho que não é percebido pelos stakeholders.*

A coordenadora fiscal também acredita que não há omissão ou distorção em relação à manutenção e afirma que: "[...] a área de TI tem procedimentos que consegue verificar esta questão das manutenções e instalações de software, mas eu acho que os stakeholders não conseguem perceber isso, pois é interno".

2.5)	Esta questão verifica se manter provas e evidências de propriedade evita a omissão ou distorção nas decisões dos usuários, mediante a responsabilidade sobre as ações próprias ou dos outros. Conceitos: integridade; materialidade; responsabilidade.

Constatou-se que todos os gestores acreditam que manter as provas e evidências de propriedade evita a omissão ou distorção nas decisões dos usuários.

Conforme a coordenadora contábil explica: "*a senha de acesso ao sistema é uma evidência de propriedade, cada usuário tem a sua, os registros consultados e lançados no software pelo usuário ficam registrados".* Ainda no que tange ao sistema, o gerente financeiro relata: "*Eu acho que é uma questão de segurança por que ter um usuário ligado a uma pessoa é sempre mais seguro por que se consegue rastrear tudo o que aquela pessoa faz".*

Alinhada à estes gestores, a coordenadora fiscal relata: "*O usuário assina um termo de responsabilidade e o fato da empresa manter uma evidência de que o funcionário sabe que deve usar o sistema adequadamente isso reduz o risco do usuário agir indevidamente*".

O termo de responsabilidade também é citado pelo supervisor de TI: "*No momento que a pessoa assina o termo de responsabilidade, eu acredito que ela vai*

pensar duas vezes antes de tomar qualquer ação que seja contra a norma. Eu acho também que é um respaldo que a empresa tem de que o usuário que infringir algo da norma pode ser penalizado por isso e até mesmo ser demitido".

O gerente de controladoria também evidencia que o documento de responsabilidade é importante afirmando que: "[...] *ajuda na formalização [...] acho que ter essa evidência é importante por que isso pode ajudar em futuras demandas*".

No entanto, as gestoras de coordenadora de custos/planejamento e TI afirmam que a omissão ou distorção depende também da responsabilidade de cada usuário em seguir a política. A coordenadora de custos/planejamento relata: "*Existe uma política conforme te falei, eu acho que quando o funcionário assina o conhecimento desta política [...] é uma segurança para a empresa, mas eu acho que se o usuário quiser fazer algo errado depende da responsabilidade dele e não apenas da norma propriamente assinada [...]*".

No mesmo pensamento, a gerente de TI relata: "*Eu acho que pode evitar, mas vai também do comprometimento do usuário em seguir o procedimento a ser seguido*".

2.6)	Esta questão objetiva verificar se os controles neutralizam os vieses e asseguram que o número de usuários permitidos não exceda o número de licenças adquiridas, cumprindo as normas do ambiente interno. Conceitos: conformidade; neutralidade; conformidade.

Constatou-se que todos os gestores sabem que existe um número de licenças adquiridas, mas apenas a área de TI sabe que número é este. Conforme a coordenadora de custos/planejamento: "*No SAP tem, mas eu não sei o número. Eu sei que tem inclusive licenças conforme os níveis, por exemplo, só para consulta, manutenção*".

A coordenadora fiscal utiliza-se de exemplos para evidenciar esta questão: "*Existe, a empresa contratou um X números de licenças, mas eu não sei quantas são. Acontecia muito no inicio do usuário tentar entrar no sistema e não conseguir, mas agora já está normalizada essa situação. Outra questão, se você ficar mais de 10 minutos sem mexer nele ele cai, acaba liberando o acesso para outra pessoa*".

Neste sentido, o gerente financeiro complementa: "*quando o número máximo de licenças está sendo utilizado, o SAP bloqueia, não se consegue mais nenhum acesso até que algum usuário saia do sistema".*

Já os gestores de TI, têm conhecimento das quantidades de licenças adquiridas. Segundo o supervisor de TI: "*Hoje estamos utilizando 200 licenças, se entrar uma pessoa a mais esta fica sem licença, pois a empresa não está autorizando mais a compra de licenças*".

A gerente de TI explica como funciona este processo de licenças: *[...] falando do SAP são 200 licenças permitidas. Todos os anos a SAP faz uma auditoria, eles avisam que vai ter a auditoria e entram no ambiente monitorando [...] o SAP tem ferramentas bem evoluídas de auditoria, então eles olham as licenças permitidas: por exemplo: nós temos 200 licenças, mas eles verificaram que usamos 220, então a empresa tem que pagar o excedente das 20 licenças. Depois que excedeu o número de licença adquirida não adianta apenas pagar [...] se paga o excesso e fica-se com as 20 licenças a mais [...] o usuário não consegue entrar caso o limite tenha excedido, mas a TI consegue liberar esse acesso. O controle de licenças é da TI [...] nós fizemos essa análise porque cada licença do SAP é muito cara [...] nós reportamos os valores ao vice-presidente financeiro e chegamos nas 200 licenças [...] hoje se entrar um usuário a mais na área, não se tem disponível, o gestor deve fazer uma análise interna e redistribuir as atividades para não gerar mais custo*".

2.7)	Esta questão identifica se as verificações de aquisição e instalação de softwares e licenciados ocorrem de forma mais completa possível, sem omissão de algum fato relevante, permitindo um clima de confiança. Conceitos: autenticidade; integridade; transparência.

Nesta questão apenas os gestores do TI e da contabilidade explicaram como as verificações de aquisição e instalações de software ocorrem, os demais gestores desconhecem como é este procedimento.

O supervisor de TI relata que o SAP foi recentemente adquirido pela empresa, e que a instalação pode ocorrer quantas vezes for necessário, porém há um controle de licenças que não pode ser ultrapassado. Segundo este gestor: "*Essa verificação de disponibilidade de usuários versus licença é feita, e hoje não temos nenhuma licença disponível. O controle de usuários ativos é feito pelo TI*".

A gerente de TI também explica esta verificação: "*A gente faz um acompanhamento inicial e também depois, se surgir algum problema nesta instalação [...] nós da TI na época ajudamos na aquisição, auxiliamos na instalação junto com o fornecedor e é estabilizado o processo, [...] se sentir a necessidade de ajuda, eles abrem um chamado para o TI e a gente auxilia".*

A coordenadora contábil explica que as verificações e monitoramentos são feitos pela área de TI: "*Os sistemas utilizados na empresa são instalados na rede, as manutenções e liberação de acesso são feitas pela TI de acordo com o perfil de cada usuário. Alguns programas específicos instalados nas máquinas de alguns usuários [...] são monitorados pelos profissionais da TI de forma remota".*

2.8)	Esta questão verifica se a política para a manutenção das condições de licenças é exposta de forma compreensível ao usuário, contribuindo para uma boa imagem perante *os stakeholders*. Conceitos: política de segurança; compreensibilidade; criação de valor.

Identificou-se que todos os gestores, exceto a área de TI, não têm conhecimento sobre a política de manutenção de licenças e sua exposição. Como exemplo, destaca-se a afirmação da coordenadora contábil: "*Não tenho conhecimento se existe esta política, mas acho que o TI deve ter uma política interna que controla este processo de manutenção*".

De acordo com as informações dos gestores de TI, existe uma política sobre as condições de licenças. Neste sentido o supervisor de TI relata: "*Existe uma política do SAP, quando aderimos a este sistema nós aderimos automaticamente à política do SAP. Esta política está disponível também para o usuário via rede*". Isso é corroborado pela gerente de TI: "em uma política específica para o SAP, tem uma política da TI que é a visão geral de TI da empresa e tem a política corporativa SAP". Questionou-se sobre a percepção dos *stakeholders* em relação a estas políticas e, verificou-se divergência de opinião entre o supervisor e a gerente de TI. Segundo o supervisor de TI: *"[...] eu acho que eles nem precisam ter acesso a estas informações de política".* Já a gerente de TI *"Eu acho que eles [stakeholders] não têm a visão da política, acho que isso não chega para eles. Acho que seria interessante eles enxergarem isso.*

2.9)	Esta questão verifica se a política para disposição ou transferência de software é exposta de forma compreensível ao usuário contribuindo na prevenção de risco, monitoramento e supervisão contínua dos processos. Conceitos: política de segurança; compreensibilidade; risco.

Identificou-se que não há uma política para disposição ou transferência de software. Segundo o supervisor de TI: "*Não existe uma política que diga como fazer e o que fazer quando se transfere um software, não tem nada escrito, acho que nenhuma empresa trata isso, até por que não é comum uma empresa ficar mudando de sistema para sistema, geralmente a transferência de software se faz uma ou duas vezes durante a existência da empresa e não em cada ano*".

Isso é corroborado pela gerente de TI: "*Não fizemos uma política para transferir o software antigo para o novo, o que foi feito um treinamento para que todos entendessem qual era a metodologia que seria utilizada*".

Quanto aos demais gestores, eles desconhecem a existência dessa política. A coordenadora contábil relata: "*Eu não sei se existe uma política de disposição ou transferência de software, acredito que os usuários também não têm conhecimento".* Já a coordenadora de custos/planejamento afirma: *Recentemente nós trocamos o software, mas eu não sei se existe uma política sobre essa transferência, nunca ouvi falar"*.

2.10)	Esta questão verifica o cumprimento de termos e condições para software e informação obtidas a partir de redes públicas e, se isso pode ser verificável, prevenindo o risco, monitoramento e supervisão contínua dos processos. Conceitos: conformidade; verificabilidade; risco.

Constatou-se que existe o cumprimento de termos e condições para software e informações obtidas a partir de redes públicas. Isso ocorre em função do bloqueio de determinados sites, bem como da própria restrição de acesso ao usuário à internet, apenas tem acesso àqueles usuários que possuem autorização dos gestores. Sendo assim, a coordenadora de custos/planejamento afirma: "*Depende do nível do usuário se dá o acesso a ele, mas redes sociais por exemplo o facebook, não*".

Neste sentido a coordenadora fiscal relata: "*Somente os funcionários autorizados tem esse acesso. Nós temos acesso a vários sites na internet, mas por exemplo, o facebook é bloqueado se alguém tentar não vai conseguir acessar. Eu particularmente uso muito o goolge, para procurar uma decisão, verificar alguma questão específica fiscal [...] hoje temos um controle de acesso, se eu quiser saber o que um funcionário está acessando durante o dia eu consigo rastrear. Eu nunca cheguei ao ponto de pedir este relatório ao TI, os funcionários não acessam durante o horário de expediente*".

Outros exemplos de sites são citados pela coordenadora contábil: *"alguns sites são bloqueados, por exemplo: sites de compras, e-mails externos e particulares".* Segundo os gerentes de controladoria e financeiro, a internet é utilizada como uma ferramenta de informação.

Conforme o gerente de controladoria: "*tem acesso, eu não sei dizer e termos de redes sociais, mas a internet temos acesso até por que a usamos como ferramenta de informação*".

Quanto ao uso de redes sociais, apenas as áreas de Marketing e RH possuem esse acesso. O supervisor de TI explica: "*[...] algumas áreas da empresa que precisam ter acesso [...] a área de RH tem acesso ao LinkedIn e Facebook para pesquisar o perfil dos funcionários [...] a TI é uma área que não tem acesso a estas redes sociais. Quanto ao uso da internet, quando se cria um usuário o gestor informa à TI se o usuário precisa ou não o acesso à internet e também justifica este acesso, informando os sites de uso, a TI verifica essa justificativa e libera o acesso".*

Ainda sobre as redes sociais, a gerente de TI complementa: "*O Marketing tem acesso as redes sociais, mas são acessos controlados, são para algumas pessoas e isso também é monitorado, mesmo que eles tenham essa permissão vinda do gerente ou diretor da área também é monitorado*".

Questionou-se também os gestores quanto ao acesso à rede pública com a rede da organização ao mesmo tempo. De forma unânime os gestores acreditam que não há problemas de acessar essas duas redes ao mesmo tempo.

De acordo com a coordenadora fiscal, vários sites podem ser abertos juntamente com o software da empresa: *"É só minimizar o SAP e abrir a internet. Várias coisas podem ser usadas ao mesmo tempo, o e-mail, o sistema, a internet*". Neste sentido a coordenadora contábil afirma: "*Consegue acessar ambos ao mesmo tempo. Não vejo isso como um problema para a segurança da informação, se há a*

possibilidade de acessar dois canais no mesmo equipamento deve ser seguro, eu acho que não interfere na rede da empresa, pois são redes independentes".

Sobre esta questão, a coordenadora de custos/planejamento relata: "*Eu não vejo problema em acessar as duas juntas, por que a gente usa muito, até para consultar a legislação e consulta de tradução. Nós usamos também o acesso online do SAP, a gente às vezes está dentro do sistema SAP e temos uma dúvida e daí entramos no Google para procurar. Eu vejo assim, se for em nível de trabalho não vejo problema nenhum".*

O gerente financeiro possui a mesma percepção: "*Eu não vejo problema de acesso de ambos ao mesmo tempo, por que temos que utilizar justamente a rede pública para obter a informação, a empresa não é nada mais do que um grande conglomerado de informações. Eu acho que isso é essencial hoje em dia*".

A explicação sobre a segurança das informações advém da área de TI. Conforme o supervisor de TI: "*Nós temos hoje um firewall que toda e qualquer conexão que sai e entra na empresa passa por este firewall. Este firewall atende políticas de segurança, ele consegue barrar possíveis entradas indevidas, ninguém de fora consegue entrar na máquina do usuário, o firewall barra. Hoje temos o firewall Next Generation Firewall, ele verifica ameaças na internet conhecidas e ele nos manda atualizações e, desta forma a gente sabe de todas as ameaças que podem estar ocorrendo na internet, qualquer tipo de ataque que possa tentar entrar na nossa rede*". A instalação deste antivírus ocorre em todas as máquinas, conforme informação da gerente de TI.

2.11)	Esta questão aborda o não copiar no todo ou em partes documentos em geral, além daqueles permitidos pela lei de direito autoral. Este procedimento evita as manipulações e deve considerar o comportamento ético e moral. Conceitos: autenticidade; representação fidedigna; ética.

Todos os gestores responderam que apenas os usuários de suas respectivas áreas possuem acesso à pasta na rede e, desta forma podem copiar os documentos que ali estão disponíveis.

Sobre isto, o gerente de controladoria explica: "*A proteção que existe é o acesso. Hoje a rede bloqueia se você não for uma pessoa daquela área, a não ser que se tenha essa permissão. É protegido no acesso, o usuário que tem o acesso*

consegue copiar as informações". A coordenadora contábil corrobora: *"os usuários da contabilidade possuem acesso a todas as informações do departamento".*

Neste sentido, a coordenadora de custos/planejamento sobre o monitoramento destes acessos: "*o TI tem esse monitoramento, de cópia, de transferência de arquivo por exemplo. Toda a movimentação do usuário fica registrada. O acesso das pastas na rede depende do acordo do gestor da área com os outros gestores. Eu posso pedir acesso à pasta da contabilidade, mas o gestor precisa autorizar isso. Se interferir no trabalho, se solicita o acesso ao gestor, mas a princípio não se tem o acesso às outras pastas*".

A coordenadora fiscal cita um exemplo de como funciona o acesso aos dados na rede: "*A pasta do setor fiscal fica na rede, todos do setor fiscal têm acesso por que não tem informações confidenciais, o controller também tem esse acesso, mas, por exemplo, eu não consigo acessar a pasta da contabilidade e a contabilidade não consegue ter acesso a do fiscal. Os funcionários conseguem fazer a cópia de qualquer documento que esteja nesta pasta e, eu tenho uma pasta separada na rede que se trata de assuntos gerenciais*".

A área de TI também corrobora estas afirmações. Segundo o supervisor de TI: "*Na área de TI as pastas que estão na rede da TI estão bloqueadas para as demais áreas e vice versa também. Existem duas pessoas que são os administradores que têm acesso às pastas de outras áreas, mas eles entram nestas pastas quando necessário, a pedido do gestor via chamado e também entram com o acesso de administrador".*

Ainda sobre esta questão, a gerente de TI detalha como funciona o processo de proteção dos dados: "[...] *Por exemplo: um usuário do setor fiscal, só tem acesso a rede fiscal, ele pode gravar e copiar os documentos. Ah, mas se ele quiser copiar o documento e salvar na máquina dele ele pode? Pode, mas na política está escrito que os arquivos devem ser salvos na rede para que entre numa rotina de backup, isso também é segurança da informação. Outra questão, eu quero copiar para dentro de um pendrive. Se o USB da máquina estiver liberado ele vai conseguir copiar, mas todos os USBs das máquinas são bloqueados para que não se consiga espetar um pendrive e copiar e, vamos dizer que a pessoa conseguiu copiar, a pessoa só vai conseguir sair da empresa se tiver uma autorização para sair com aquele pendrive. Vai ser uma autorização do gestor, ele vai se responsabilizar por aquilo e, caso o gestor não esteja o TI é acionado para efetuar tal autorização,*

verificando o material que está no pendrive. Isso tudo a gente procura controlar! Ah, mas eu tenho acesso a um e-mail externo, daí realmente ele consegue, vai do comprometimento da ética profissional de não mandar arquivos para fora.

Das práticas apresentadas no domínio D2 conclui-se que apenas a política para disposição ou transferência de software não é utilizada e, não houve consenso dos gestores quanto à conscientização destas políticas e à compreensão da política de manutenção das condições e licenças pelos usuários.

Por fim, questionou-se aos gestores quanto à contribuição destas práticas (política e divulgação de uso legal de softwares; aquisição de software por fontes reconhecidas; verificações de aquisição e instalação de software; manutenção e identificação de registros de ativos; manutenção de provas e evidências de propriedade; controle de licenças adquiridas; acesso a redes públicas juntamente com a rede da empresa; proteção contra cópia de documentos) para a conformidade.

Constatou-se que todos os gestores acreditam que elas contribuem. Segundo a coordenadora fiscal: "*Eu acho que seguindo essas regras, comprar o software de fontes conhecidas mitiga o risco de divergência e vazamento das informações, eu acho também que as limitações de acesso de determinados sites pode impedir a entrada de alguns vírus. Eu acho que tudo isso garante que a empresa está cumprindo as normas, para divulgar um número que condiz com a realidade da empresa".*

Sobre a divulgação do resultado da empresa, a coordenadora contábil afirma: "[...] *são práticas que evitam perda e atraso na entrega das informações e nos garante resultados mais seguros o que contribui para conformidade*".

O gerente financeiro acredita que "[...] *evitar se ter softwares que não tenham licenças dentro da empresa, acho que isso é muito importante, mitigar os riscos de uma multa de estar usando os usuários acima do exigido por exemplo pela SAP, da gente ter uma política de utilização dos softwares da empresa elas mitigar bastante o risco, saber o que cada usuário está fazendo é muito importante. O momento que estamos nos permite saber que tudo que é feito pelo usuário se tem rastreabilidade, não há pontos obscuros, se tem monitoramento da informação [...]".*

Sob a percepção do gerente de controladoria as práticas contribuem porque *"limita o acesso, deixa restrito às pessoas nas suas áreas de atuação, tu proteges os documentos de alterações indevidas [...] se protege em relação a alguém que não*

tem o conhecimento de trabalhar em cima dos documentos e aí sim, perder informações. Eu entendo que isso traz uma confiança para o processo, [...] há uma importância e ajuda sim na conformidade". Isso é corroborado também pela coordenadora de custos/planejamento: "*Eu acho que a contribuição é a limitação, a própria limitação da informação de cada setor, por exemplo, imagina ter acesso a toda a rede de RH, no que refere à folha. Eu acho que a própria limitação, essas barreiras contribuem para a conformidade*".

As respostas obtidas pelos gestores de TI também são semelhantes aos demais gestores. A gerente de TI afirma: "*[...] eu acho que elas contribuem para mitigar ao máximo o risco, para que a gente mantenha a segurança da informação*".

O supervisor de TI complementa: "*Nós utilizamos todas estas práticas para garantir a segurança das informações, eu acredito que elas conseguem garantir informações sejam íntegras e que ninguém possa manipular ou lesar a empresa, por exemplo, num software por multas, que pode acontecer. Nós já sofremos auditorias de empresas como a Microsoft, Autodesk e diversas outras empresas [...] e em todas estas auditorias a nossa empresa nunca teve problema de conformidade, justamente por que a gente segue as normas e procedimentos".*

A seguir, abordam-se as questões referentes ao domínio D3.

- **3. Proteção de registros organizacionais (D3):**

3.1)	Esta questão verifica como são categorizados os registros (ex: registros contábeis, registros de bases de dados, de transações), e também se estes são disponibilizados em tempo hábil para a tomada de decisão, permitindo um clima de confiança e transparência. Conceitos: disponibilidade; tempestividade; transparência.

Nesta questão, todos os gestores possuem a mesma percepção, exceto a coordenadora de custos/planejamento.

Quanto à categorização dos registros o gerente de controladoria afirma: "*O sistema SAP deixa tudo vinculado, se tem acesso a todas as informações, qualquer movimentação que é feita no sistema se tem um rastro [...] o SAP permite esse check, a confiabilidade, tem uma rastreabilidade de buscar, entender como as coisas foram feitas*". No que refere-se à disponibilidade desses registros para a tomada de

decisão este gerente afirma: "*Eu acredito que sim, porque a informação está disponível no sistema, depende muito da habilidade dos usuários de coletar a informação e da clareza da própria gestão em saber o que quer. Eu não vejo problema neste sentido, ela está sempre disponível para ser usada*".

Quanto à confiança e transparência nas informações obtidas, o gerente de controladoria respondeu: "*[...] eu acredito na confiança dos números porque nós temos profissionais capacitados aqui na empresa [...] a própria questão da conciliação ajuda nisso, nós trabalhamos muito forte no garantir que estes processos aconteçam, por exemplo: registros de documentos, registros de notas fiscais, tanto a entrada quanto a saída, lançamentos no setor financeiro, apontamentos de fábrica, apontamentos de produtos. Nós temos uma complexidade bem grande dento do nosso processo fabril principalmente, então é necessário [...] dentro do sistema amarrações necessárias, a informação que hoje está no sistema ela é disponível e confiável*".

Já o gestor financeiro explica como funciona a categorização dos registros na área financeira: *"[...] nós temos tipos de transações que são de diferentes áreas da empresa, por exemplo temos as transações F que são transações financeira, V que são transações de venda, então dentro do sistema isso é bem segmentado".* Esse gestor também acredita que as informações estão disponíveis em tempo hábil para a tomada de decisão: *"Com certeza. Por que essa é a grande vantagem do sistema, ele está todo online, se consegue tirar a informação agora, é tudo integrado. Se entrou uma nota agora no fiscal ela já está no contas a pagar. Há também relatórios gerenciais que facilitam a análise".*

O gerente financeiro completou que há a confiança e transparência nas informações: "*Com certeza [...] ele é um sistema todo online a gente não tem diferenças de informação. A informação que se tem no contábil, em vendas, no financeiro é a mesma, pois a transação vem toda de uma mesma base. É uma informação única não se tem questionamento, por exemplo, eu tenho 10 milhões no contas a pagar eu tenho 10 milhões no balanço, então a confiabilidade é 100%*".

A coordenadora fiscal também aborda sobre as transações e destaca a integração do sistema SAP. Ela acredita que a disponibilidade das informações para a tomada de decisão está relacionada com a integração das informações no sistema de forma online. Conforme esta gestora: "*[...] As informações para a tomada de decisão sempre estão em dia, é tudo integrado, por exemplo, se eu quiser saber*

quanto de faturamento teve ontem é só acessar o sistema". O mesmo exemplo foi citado pela coordenadora contábil.

Quanto à confiança e transparências das informações, a coordenadora fiscal afirma: *"o registro é feito conforme o documento físico e se alguma informação não estiver correta alguma área vai conseguir identificar. As áreas contábil, financeira e fiscal fazem suas conciliações, qualquer diferença pode ser identificada, isso permite a confiança e transparência das informações*". Neste sentido, a coordenadora contábil explica: "*é confiável [...] a medida que a informação é registrada no sistema acontece também o registro contábil , podendo também gerar relatórios gerenciais com essas informações*".

Na área de TI a explicação é mais sobre a categorização dos dados. Segundo o supervisor de TI: "*Os registos ficam no sistema do SAP, somente os usuários daquela área têm acesso àquelas informações, no módulo da contabilidade por exemplo. O gestor daquela área libera as informações para os seus funcionários, é o gestor que dá permissão para os usuários. Os registros são dados e estão categorizados por transação*". Este gestor também acredita que os registros são disponibilizados em tempo hábil para a tomada de decisão, ele afirma: "*Com certeza. Por que os registros estão presentes no sistema e, com base nos relatórios que podem ser executados no sistema o gestor consegue gerar a informação online e tomar a decisão".*

Sobre a confiança de transparência das informações, esse o supervisor de TI é enfático: "*[...] eu tenho hoje um sistema onde é possível colocar as informações, lá dentro eu sei que ninguém vai alterar e, se alterar isso fica registrado quem alterou. Eu digo que os registros estão seguros e disponíveis para quem precisar acessar e obviamente para quem tem acesso a eles, mas se estão certos ou não depende da área de contabilidade*".

Já a gerente de TI, utiliza-se de uma nomenclatura específica do SAP, ela explica: "*Os registros dentro do SAP são categorizados por módulo, por frente, a gente fala muito em frente dentro do SAP [...] por exemplo: frente SD (vendas), frente MM (compras), frente PP (produção), então primeiro por grandes módulos e, depois dentro de cada módulo desses as tabelas transacionais. [...] todas essas tabelas são integradas uma na outra, a informação tem um link*".

Quanto à disponibilidade das informações em tempo hábil para a toma de decisão, a gerente de TI responde: "*Sim, porque é tudo online. Todo o registro*

ocorre de forma online, se eu fiz a movimentação de estoque e tirei um material de um depósito e enviei a outro, isso ocorre no mesmo momento, o que permite a tomada de decisão naquele momento, no caso do estoque já é possível identificar o saldo de estoque. A tempestividade e a disponibilidade são essenciais para a tomada de decisão". No que se refere à confiança e à transparência das informações, a gestora afirma: "*[...] Hoje ela é online, a transação acontecendo, a gente consegue ter a confiança do que se tem no físico e no sistema".*

Em contrapartida, a coordenadora de custos/planejamento acredita que os registros não são disponibilizados em tempo hábil para a tomada de decisão, ela relata: *"Eu acho que não. Hoje ainda não, por que a gente tem algumas preocupações ainda com o sistema SAP, então eu acho que muitas áreas ainda estão amadurecendo esse processo, então as informações demoram muito ainda. A gente tem o fechamento contábil no décimo dia útil hoje, é uma coisa que não adianta mais [...] demora por que a gente depende de outros setores [...]".*

Quanto à confiança e transparência das informações, essa gestora explica: *"O que dificultou muito pra gente, é que foi liberado o lançamento contábil para todos os setores. Cada setor registra a sua despesa, cada setor lança a sua nota, então a gente tem muito problema com isso, porque não são todos que entendem o que é um débito, um crédito, uma despesa, um gasto. Isso é bem complicado, pois a pessoa pode lançar em uma conta errada ou no centro de custo que não é o dele por exemplo. Às vezes a gente perde mais tempo verificando o que foi feito do que gerando a informação [...] a gente não tem braço suficiente para conferir todo o dia o que estão fazendo [...]. No sistema antigo estes lançamentos eram centralizados em um setor, o que na minha visão reduzia os problemas de lançamentos, hoje com a expansão de agilizar o processo eu acho prejudicou um pouco, não se tem muita confiança do que está lá dentro. Eu acho que em certos casos os registros não permitem a confiança e transparência das informações.*

3.2)	Esta questão verifica se os registros armazenados possuem detalhes de proteção ao longo do tempo e estão disponíveis em local adequado. Conceitos: integridade; disponibilidade; locais funcionais.

Identificou-se, pelas explicações dos gestores de TI, que os registros são armazenados em servidores, tanto internamente quanto externamente. Porém os

demais gestores não souberam explicar como são protegidos, bem como o local que é armazenado.

Segundo a coordenadora fiscal os registros são armazenados "*[...] em servidores [...] eu acho que deve ter um interno e para garantir deve ter outro externo. Quando a empresa estava localizada em Porto Alegre eu sei que havia até uma sala contra incêndio.* Indagou-se também sobre a disponibilidade e acessibilidade destes registros, desta forma a gestora responde: *[...] estão disponíveis, por exemplo, se eu quiser algo de 2016 está tudo no SAP e se eu quiser algo anterior a 2016 eu preciso entrar no sistema Sapiens*".

Já o gerente financeiro acrescenta: "*Eu acho que o servidor está aqui, mas eu não tenho nem ideia de onde fica, mas se ele estiver aqui eu acho que não é o local mais adequado*". Sobre a acessibilidade e disponibilidade dos registros, a gerente contábil afirma: "*O registro está em rede, qualquer usuário pode acessá-lo".* Conforme o gerente de controladoria: "*Eu acho que a gente tem uma estrutura de TI de backoffice bastante forte, para armazenagem de dados e backups*".

Os gestores de TI explicam como funciona a questão de proteção dos registros armazenados. Segundo o supervisor de TI: "*O SAP fica hospedado em um servidor num Datacenter de outra empresa a Uol em São Paulo, de forma muito segura, há redundância de gerador, de energia elétrica, de nobreak, de gerador. A redundância quer dizer que são duas entradas, se uma falha se tem outra para garantir a segurança. As informações da empresa não são compartilhadas com outra [...] o acesso a esses registros [SAP] ocorre de forma normal, como se estivessem na nossa rede interna [...] dentro da empresa temos um servidor interno que ficam os arquivos de Excel, rede interna, documentos da empresa, por exemplo.*

Quanto ao local onde são armazenados, este o supervisor de TI respondeu: "*Sim [estão em local adequado] por haver toda a questão de segurança que comentei anteriormente e também da disponibilidade deles*". A gerente de TI cita a rotina de *backup* como uma prática de proteção dos registros, sendo assim: *"rotina de backup vai permitir o acesso aos registros caso necessário [...] o acesso às informações ocorre da seguinte forma: por meio de um login para ter acesso aos arquivos da rede e, através de um usuário e senha para acessar o SAP*".

3.3)	Esta questão verifica como as chaves de criptografia ou assinaturas digitais são armazenadas, bem como se elas estão livres de erros, vieses e manipulações, auxiliando na prevenção de riscos, monitoramento e supervisão contínua dos processos. Conceitos: disponibilidade; representação fidedigna; risco.

Constatou-se que apenas as áreas fiscal, controladoria e financeira utilizam as assinaturas digitais. Conforme a coordenadora de custos/planejamento: "*No nosso setor não fazemos uso de assinatura digital, porque não temos acesso aos bancos, órgãos públicos, por exemplo*".

Já a área fiscal faz o uso da assinatura digital, de acordo com a coordenadora fiscal: *"A gente usa a assinatura digital para a entrega das obrigações. Utilizamos o token do vice-presidente, a gente só consegue enviar para os órgãos com esse token. Este token não é meu, é da empresa, do vice-presidente, mas ele fica conosco por que ele é o representante legal perante a Receita e demais órgãos. Eu não tenho nenhum token".*

Sobre o local onde são armazenadas as assinaturas digitais essa coordenadora respondeu: *"A gente tem uma caixinha com todos os tokens (um de pessoa jurídica e outro de pessoa física) que ficam em uma gaveta. Nós controlamos quem pega o token de pessoa jurídica, quem usa somos nós aqui do fiscal, o RH e a segurança patrimonial. O uso não é exclusivo de gestores, no RH tem um funcionário que utiliza o token para enviar as informações trabalhistas. Para o token de pessoa física, só o fiscal usa. A senha dos tokens é compartilhada com todos estes setores".*

Neste sentido, questionou-se a gestora fiscal quanto a erros, manipulações ou vieses, ela afirma: "*Apesar dele ser utilizado por vários setores eu não acho que pode haver erro ou manipulação por que se eles utilizarem de forma errada em algum momento a Receita não vai acatar essa informação e o setor que mandou a informação receberá uma inconsistência [...] sem o token e a senha não se consegue enviar informações, antigamente se transmitia a informação sem essa segurança. Hoje o certificado digital existe e ajuda a prevenir os riscos*".

Conforme a coordenadora contábil, quem possui a assinatura digital é o gerente de controladoria e, na percepção desta gestora *"[...] a segurança da assinatura digital está no usuário, dependendo de como ele guarda é um risco*".

O gerente de controladoria explica como funciona o processo de assinatura digital na controladoria, bem como a divulgação das demonstrações para o mercado: "*eu faço a entrega dos Speds das informações através da minha assinatura digital [...] A assinatura digital é pessoal, através do token, quando eu entrei na companhia por ser o responsável pelas demonstrações eu tive que fazer a assinatura pela empresa, então é um processo que funciona normalmente durante os momentos de entrega de declarações. Eu não tenho, por exemplo, liberações a bancos, esse tipo de informação é da área financeira. A entrega de divulgação de balanço é feita pela área de RI, relacionamento com investidores, o que nós fazemos é o fechamento do balanço, que é o processo contábil propriamente dito, nós não fazemos através de assinatura digital nenhuma entrega de resultados para a bolsa de valores ou para a CVM. A área de RI é quem faz esta divulgação e este link com estes órgãos*".

Ao responder se as assinaturas digitais estão livres de erros, vieses e manipulações, o gerente de controladoria afirma: "*Eu acho que não. Eu acho que são coisas diferentes, não tem relação. Se eu fizer alguma coisa mal feita e transmitir, não é a assinatura digital que vai bloquear ou não, a assinatura digital é um meio para fazer a declaração, mas todo o processo de confiabilidade dos números, de confiança, de integridade da informação tem que ser feito dentro do sistema. Então eu acho que não tá relacionado. Hoje a gente tem as conciliações que nos ajudam a verificar se os saldos estão corretos, as próprias análises. As evidências que temos são da equipe, do dia-a-dia da equipe que trabalha com a informação, a equipe analisa, concilia, checa, valida e aí sim se faz o processo de declaração*".

Na área financeira, identificou-se que o uso do *token* e senha ocorre apenas pelo gestor da área. Explica o gerente financeiro: "*todas as assinaturas que a gente faz aqui na empresa a gente tem um token que é individual, se tem um usuário, uma senha e um token e para assinar contrato se tem usuário, senha, token e cpf. Então por exemplo se alguém hackeou a minha senha ele não consegue fazer nenhuma operação por que ele precisa do meu token. O token fica comigo, ele é individual. Outra questão importante é que sempre se precisa de dois, por exemplo o meu token e o de outro procurador, pois são sempre duas pessoas que aprovam a transação bancária*".

O gestor financeiro acredita que as assinaturas digitais estão livres de erros, vieses e manipulações, pois *"Existe todo um compliance, a informação vem do*

sistema e este é integrado". Ele acredita que essas assinaturas auxiliam na prevenção de risco. Segundo o gestor: *"Sim, com certeza. Justamente por apenas as pessoas autorizadas conseguem fazer as transações, não se tem outra maneira de fazer".*

A área de TI explica de forma mais consistente essa questão que envolve as assinaturas digitais e criptografia. Conforme o supervisor de TI: *"Nós temos algumas chaves de criptografia para determinados sistemas aqui dentro, que utilizam HTTPS, que é a porta de comunicação segura. Tudo que trafegar ali, fica criptografado, mas o usuário não enxerga isso. Quanto as assinaturas digitais são apoiadas pelo TI, na instalação destes certificados que são emitidos diretamente pelos bancos. Os bancos emitem o certificado, fornecem os tokens e a TI apoia na instalação deste certificado para a área que fará uso da assinatura. A TI hoje não utiliza assinatura digital [...] Elas ficam em posse da área que utiliza a assinatura digital".*

A gerente de TI acrescenta: "*A criptografia a gente está iniciando o uso da criptografia para notebooks, para algumas pessoas que acabam expondo isso ao sair da empresa, viajar com o notebook e expõe a informação, há um risco dessa informação da empresa fora. Hoje tem um risco muito grande de roubo de notebook e, esse notebook vai estar com o ambiente dele todo criptografado*". Quanto às assinaturas digitais, a gerente de TI corrobora as informações apresentadas pelo supervisor de TI: "*quem usa são as áreas fiscal e financeira, não sei como eles guardam isso*".

No que tange se as assinaturas digitais estão livres de erros, vieses e manipulações, ambos os gestores de TI acreditam que sim. Conforme o supervisor de TI: "*Eu acredito que sim, pois as assinaturas digitais são fornecidas diretamente pela empresa que solicita que a gente as utilizem. Se tem algum erro ou manipulação fica na responsabilidade destas empresas e não da aqui da empresa*". Já a gerente de TI afirma: "*a assinatura tem segurança, ela é certificada*".

Referente a prevenção de risco, utilizando-se das assinaturas digitais e chaves de criptografia, o supervisor de TI responde: "*[...] a empresa hoje tem chaves de criptografia para portais de acesso, por exemplo: as pessoas que utilizam o e-mail fora da empresa, existem uma chave de criptografia que é utilizada para abrir os e-mails, ela não vai acessar num formato de qualquer pessoa que possa visualizar as informações contidas no e-mail, há uma segurança no tráfego da*

informação. Também fazemos uso da criptografia interna, hoje o servidor qualquer conexão que chega nele precisa estar criptografada".

Na percepção da gerente de TI: "*ajuda na segurança, porque ela já é uma assinatura certificada, isso já está intrínseco a ela e, para o uso dela é necessário um usuário e senha*".

3.4)	Esta questão verifica como são os cuidados quanto à possibilidade de deterioração das mídias armazenadas e, se isso ocorre de forma semelhante para itens afins dentro da estrutura organizacional. Conceitos: política de segurança; consistência; locais funcionais.

Constatou-se que apenas os gestores de TI possuem o conhecimento sobre a deterioração das mídias armazenadas. A gerente de TI explica como funciona este procedimento: "*A gente entra em contato com a equipe de meio ambiente para fazer o descarte adequado com a empresa autorizada, para que não vá para um lixo comum [...] não faça contaminação de solo. Nós chegamos a fazer descarte de equipamentos, computadores muito velhos, com HD junto, principalmente na época da mudança da empresa para cá, mas atualmente não tem acontecido mais*".

3.5)	Esta questão verifica como são procedimentos para assegurar a capacidade de acesso aos dados contra perdas ocasionadas pelas futuras mudanças na tecnologia, permitindo aos usuários identificar diferenças e semelhanças, interpretando e avaliando os regulamentos para limitar as perdas. Conceitos: integridade; comparabilidade; avaliação de risco.

Identificou-se que os gestores das áreas financeira, contabilidade e controladoria não têm o conhecimento dos procedimentos para assegurar a capacidade de acesso aos dados contra perdas ocasionadas pelas futuras mudanças tecnológicas. Apenas os gestores das áreas fiscal, custos/planejamento e TI explicaram tal procedimento.

A coordenadora fiscal explica esse processo utilizando-se de um exemplo prático que ocorreu recentemente na empresa, a troca de sistema. Conforme a gestora: "*Eu posso te dizer que no sistema antigo nós não perdemos o acesso aos dados, quando precisamos consultar algo anterior a 2016 acessamos o sistema*

Sapiens, eles estão disponível, por exemplo eu gero a base e exporto para o excel. Eu imagino que se a empresa futuramente mudar de sistema ou alguma mudança tecnológica ocorrer o SAP também ficará disponível".

Já a coordenadora de custos/planejamento relata o procedimento de backup para garantir o acesso aos dados. Segundo essa gestora: "*O que eu sei é que o TI faz backup de toda a rede, do sistema. Eu sei que eles têm esse processo de backup que é feito em fitas*".

Isto é corroborado pelos gestores de TI, a gerente de TI relata: "*O procedimento é o backup da informação. Se faz o backup da base e revisamos a informação para imputar isso para o novo sistema, nós fizemos isso quando mudamos o sistema Sapiens para o SAP.*

Neste sentido, o supervisor de TI explica este procedimento: "*A única forma de se fazer isto é com backup, na minha opinião, pois é a única forma de se ter uma posição anterior e isso vale também para uma possível mudança tecnológica. Quando nós trocamos o sistema, nós ficamos com uma base do sistema antigo que fica disponível para consulta ao usuário, que ficará disponível até que a empresa julgue necessário, eu acredito que sempre. Muitas informações foram migradas para o SAP, pois era necessário ter as informações em um único ambiente, mas tiveram informação que não eram necessárias migrar, estas ficaram disponíveis para consulta no sistema antigo, hoje nós pagamos esse sistema para ter a informação disponível mediante consulta ao usuário*".

Questionou-se aos gestores sobre a comparabilidade das informações e se os procedimentos conseguem limitar as perdas. Constatou-se que os gestores das áreas fiscal, custos/planejamento e TI possuem a mesma percepção, os demais gestores não responderam, pois não têm o conhecimento do procedimento de acesso aos dados contra perdas ocasionadas por futuras mudanças tecnológicas.

A coordenadora fiscal afirma: "*os processos acabam mudando, mas o resultado final é comparável [...] hoje com a mudança do SAP o sistema está mais completo se tem uma visão do início ao final do processo, eu acho que isso limita as perdas sim*". Quanto ao procedimento de backup destacado pela coordenadora de custos/planejamento, ela relata que os *"arquivos de Excel por exemplo, eu acho que sim [limitar as perdas], pois se tem o acesso da informação".*

Neste sentido a gerente de TI explica a comparabilidade das informações: *"são comparáveis sim. Talvez elas não estejam no mesmo formato uma da outra,*

porque cada sistema tem um formato de armazenar o dado [...]". No que tange a limitação de perdas, a gerente afirma: "*Acho que sim, até porque se mantém um histórico daquele que era o antigo, se mantém inclusive por motivos legais [...] hoje se consegue comparar os dados. Se por acaso seja necessário recuperar a informação, se consegue através do histórico do sistema antigo [...] isso ajuda a limitar as perdas*". Isso também é corroborado pelo supervisor de TI: "*eles praticamente anulam as perdas, por que nós sempre vamos ter a informação guardada em uma posição anterior, se for necessária alguma informação o acesso e disponibilidade a essa informação será dado via backup*".

3.6)	Esta questão verifica como o dado pode ser recuperado de forma aceitável, mais completa possível e sem omissão, por meio de monitoramento e supervisão contínua dos processos. Conceitos: autenticidade; integridade; risco.

Verificou-se nesta questão que todos os gestores acreditam que o dado pode ser recuperado de forma aceitável, mais completa possível e sem omissão, isto ocorre por meio do backup dos dados. Porém, nenhum dos gestores, exceto os da área de TI, soube explicar como ocorre o monitoramento e supervisão dos processos de recuperação.

A coordenadora contábil afirma: "*[...] Ele pode ser recuperado através de backup. Mas não sei qual a periodicidade deste backup*".

O gestor financeiro também acredita que o dado pode ser recuperado de forma mais completa possível, ele afirma: "*há um histórico que fica dentro do SAP. Existe um backup destas informações eu só não sei qual a regularidade do backup, mas eu sei que ele existe. O backup copia tudo, então permite que a informação seja mais completa possível, o máximo que pode acontecer é o usuário perder algo do dia em que executou alguma coisa*".

A coordenadora fiscal também relata sobre a recuperação dos dados: "*Ele pode ser recuperado hoje eu consigo recuperar qualquer informação antiga".* A coordenadora de custos/planejamento cita alguns exemplos de arquivos que podem ser recuperados: "*arquivos que te comentei [...] Word e Excel, eu acho que sim. Agora via sistema eu já não sei. Quando a gente perde um arquivo a gente pede o*

backup via chamado para a área de TI e informa a última data de alteração do arquivo, daí eles recuperam esta informação".

Quanto ao monitoramento e supervisão do processo de recuperação dos dados, todos os gestores, exceto os de TI, afirmaram não ter conhecimento de como ocorre. Esse detalhamento é feito pela gerente de TI: "*[...] diariamente a gente armazena os dados transacionais, só o que movimentou naquele dia, não se faz o backup completo todos os dias. O backup full, é feito semanalmente e também temos outro mensal. A gente trabalha assim por que [...] o volume é muito grande dos dados para armazenar backup. Hoje o nosso backup ainda é em fita [...] é um meio muito caro, [...] a gente procura garantir dessa forma que tudo está dentro da rotina de backup e da melhor maneira possível, mas mais enxuta possível. A TI tem que garantir que a informação esteja disponível quando o usuário precisar. Hoje tenho uma pessoa para fazer este processo, não é uma coisa muito demorada, mas tem uma ação de retirar e colocar a fita para gravar o backup. A gente disponibiliza [o arquivo reparado] na rede no local onde estava o arquivo*".

Outra forma de monitorar evidenciada pelo supervisor de TI *é "pela busca no helpdesk, através dos chamados".*

3.7)	Esta questão verifica se a destruição dos registros, caso não sejam mais necessários à organização, ocorre com cautela cumprindo normas reguladoras no ambiente interno e externo. Conceitos: política de segurança; prudência ou conservadorismo; conformidade.

Constatou-se que os gestores de controladoria, financeiro, fiscal e custos/planejamento não possuem o conhecimento da destruição dos registros. A coordenadora contábil explica como ocorre: "*Para os arquivos físicos existem alguns documentos que são eternos, não podem ser destruídos [...] para os arquivos digitais, são os registros contábeis que possuem backup*".

Neste sentido a gerente de TI afirma: "*[...] a TI não faz o descarte de arquivo de outras áreas [...] essa limpa, essa manutenção é de responsabilidade de cada área. A TI entra muitas vezes orientando, a gente tem um monitoramento diário de espaço nos nossos servidores, temos uma tv dentro da TI que apresenta as cores, verde, amarelo e vermelho, tem todos os servidores nossos estampados ali, quando*

começa a ficar vermelho significa que o espaço começou a bater no limite, então a gente tem que entrar monitorar e ver o que está estourando o espaço".

3.8)	Esta questão verifica se a emissão de diretrizes gerais para retenção, armazenamento, tratamento e disposição de registro de informações é capaz de predizer resultados futuros por meio de normas reguladoras no ambiente interno e externo. Conceitos: política de segurança; preditiva; conformidade.

Identificou-se que todos os gestores não sabem da existência destas diretrizes, exceto os gestores da área de TI. A coordenadora de custos/planejamento justificou a sua resposta: "*Não sei, mas eu acredito que tenha alguma coisa interna para armazenar a informação sim, até porque são informações que podem ser utilizadas durante muito tempo. Eu acho que deve ter na área de TI algum regramento*".

Neste sentido o supervisor de TI explica essa diretriz: *"A política fala que o Datacenter deve ficar armazenado em cofre, em local seguro e distante do local onde elas estão. O Datacenter que contem as informações do SAP está em São Paulo, o Datacenter que envolve arquivos de redes, acessos internos, documentos, e Excel, por exemplo, fica num prédio aqui. Hoje por uma definição da empresa estão dentro, mas praticamente 500 metros de distância da empresa está em um prédio separado e dentro de um cofre contra incêndio, o acesso a ele é limitado a área de TI".*

3.9)	Esta questão verifica como é a programação para retenção, de forma a identificar os registros essenciais e o período que cada um deve ser mantido de forma disponível e acessível aos usuários. Conceitos: confiabilidade; disponibilidade; acessibilidade.

Nesta questão, diversas foram as respostas dos entrevistados. Os gerentes de controladoria, financeiro e coordenadora de custos/planejamento não souberam responder. Já a coordenadora contábil comenta que a retenção ocorre meio do SAP e a guarda dos registros está dentro do sistema, incluindo o backup feito pela área de TI. A coordenadora fiscal afirma que a guarda dos registros ocorre por transação,

ela explica: "*os registros são por transações, se tem várias opções de consultar a informação, pode ser, por exemplo, pelo número da nota fiscal, nome do fornecedor, número do fornecedor, por data, por código*".

Conforme a gerente de TI "a *guarda dos registros é feita em várias tabelas diferentes, falando de SAP. O dado é armazenado em vários lugares, dependendo da informação que ser quer, busca-se essa informação*". O supervisor do TI complementa: "*a guarda destes registros é feita no Datacenter em São Paulo*".

3.10) Esta questão verifica como as informações-chaves de diferentes sistemas são mantidas/armazenadas e transportadas a uma base de dados gerencial. Conceitos: disponibilidade; transparência; acessibilidade.

O gerente de controladoria explica como as informações-chaves são utilizadas: *"nós temos o processo de gestão da empresa como um todo, a nossa base de indicadores, a nossa base de demonstrativo gerencial, que hoje a gente trabalha não dentro do sistema, mas sim em planilhas Excel, depois em formato de divulgação em Powerpoint., mas toda a nossa base de informações, gestão de estoques, gestão de margem, receita, tudo isso faz parte do processo diário de gestão [...] compartilhamos informações com outras áreas, nós temos reuniões específicas [...] temos as reuniões de diretoria [...] nós temos o processo de fechamento do balanço do mês, fechamento das informações, divulgação do demonstrativo, análise sobre o fechamento do mês, mas hoje a gente não precisa esperar só no final do mês para estar analisando estas questões. Por exemplo: o estoque, que hoje para nós é um item importante, diariamente a gente verifica como está o nosso estoque, e assim sucessivamente como as outras questões de despesas, de vendas. Todas estas informações são extraídas do sistema SAP, não temos outro sistema paralelo para transportar essas informações, usamos o Excel apenas como ferramenta para alguma formatação*".

Quanto ao transporte dessas informações-chaves, as áreas de custos/planejamento, financeira e contábil fazem uso apenas do sistema SAP.

A coordenadora de custos/planejamento relata: "*gerarmos as informações na base SAP e exportamos estas informações para o Excel, para trabalhar com a informação principalmente na área gerencial*".

O mesmo ocorre na área financeira *“Na minha área toda a informação que eu tenho está centralizada dentro do sistema SAP. O SAP fornece vários relatórios, posso te dizer que 99% eu consigo dentro do sistema e 1% eu transporto a base do SAP para o Excel e monto o relatório que eu quero, às vezes é só uma questão de layout da informação”.*

A gerente contábil também explica como ocorre na contabilidade: *“As informações estão dentro do sistema SAP e este sistema já disponibiliza alguns relatórios gerenciais, algum outro relatório que se deseja e que o sistema não disponibilize, é feito em planilhas Excel”.*

No entanto, na área fiscal utilizam-se dois sistemas, o SAP e o Mastersaf. A coordenadora fiscal explica: “*Os arquivos são transportados em formato txt, se gera a base no SAP e se transporta (importo) para o Mastersaf, depois de importar as informações eu consigo gerar um relatório no Mastersaf e aquilo que não importou aparece um erro, uma mensagem*”.

A explicação sobre os diversos sistemas utilizados pela empresa em estudo é feita pela área de TI. A gerente de TI relata: “*O SAP é uma base única, tanto operacional quanto gerencial. Alguns setores usam outros sistemas e o transporte dessas informações ocorre pela integração que existe entre os sistemas. Eles podem ser integrados por arquivos texto, ou diretos por uma RFC, é como se fosse um canal direto desse sistema especialista com o SAP [...] essas informações-chaves estão disponíveis via relatórios diversos que tem no SAP, claro que é necessário algumas análises da área específica, pode inclusive ser exportada para o excel, permitindo o uso de filtros, de gráficos por exemplo*”.

Conclui-se que todas as práticas apresentadas no domínio D3 são utilizadas pela empresa, porém em uma não há um consenso dos entrevistados. Esta questão refere-se à disponibilidade dos registros para a tomada de decisão e a confiança/transparência nestes registros, a coordenadora de custos/planejamento divergiu dos demais entrevistados.

Por fim, questionou-se aos gestores quanto à contribuição destas práticas (proteção dos registros; assinaturas digitais; deterioração das mídias armazenadas; procedimentos contra perdas por futuras mudanças tecnológicas; recuperação de dados; destruição dos registros; diretrizes gerais para guarda dos registros; programação para a guarda dos registros; única base para as informações-chaves) para a conformidade.

De acordo com o gerente de controladoria: “*Eu acho que contribuem, porque temos em uma base de dados toda a informação [...] uma única base nos ajuda a ter a conformidade. Acho que a assinatura digital é muito mais um processo de entrega das informações, do que propriamente garantir que os números sejam confiáveis, eu acho que o que garante que os números sejam confiáveis é a nossa equipe, o nosso trabalho e não a assinatura, porque se for feito errado a assinatura só transmite, ela não mitiga o risco [...] os demais processos que temos hoje mitigam, a gente pode dizer que temos uma confiabilidade grande neles, temos uma recuperação de informações, backup do sistema, confiabilidade de como o sistema opera. Qualquer problema que se possa ter é muito mais em relação a erro humano ou equívocos que acontecem no dia-a-dia, do que efetivamente um problema de sistema [...] a gente tem um suporte bem grande que nos dá essa segurança*”.

Na percepção da coordenadora de custos/planejamento essas práticas “*ajudam no controle, no próprio registro da informação porque a gente não está livre de ter algum problema. Eu acho também que a confiabilidade que o usuário tem que a informação está armazenada e que estará disponível quando ele precisar*”.

Sob a ótica do gerente financeiro: *“Contribuem sim. Eu acho que aquela questão da segurança das assinaturas é muito importante, saber que é a pessoa que está fazendo a operação é a mesma pessoa que possui a responsabilidade de fazê-la e que tem poderes para tal, se tem a garantia não só de sistema mas de segurança. Todos os procuradores que têm autorização para as transações bancárias há um procedimento de responsabilidade, há o registro em cartório”.*

A coordenadora fiscal afirma: “*Cada setor só tem acesso as suas transações, então aí se tem uma garantia de acesso aos dados que são permitidos, as pessoas têm o conhecimento e treinamento para imputar os dados no sistema, cada área tem a sua responsabilidade e isso com certeza contribui*”.

A coordenadora contábil explica a importância destas práticas para a empresa, ela afirma: *“Os registros contábeis são de grande importância para empresa, através deles se dá a tomada de decisões, eles devem ser confiáveis e claros, devem estar protegidos e arquivados em locais seguros, livres de riscos, devem estar disponíveis a qualquer momento. É importante seguir essas práticas para garantir a integridade das informações contábeis*”.

Para a gerente de TI essas práticas “*proporcionam a disponibilidade e a integridade dos dados, no momento que se faz uma recuperação de algum dado*

esse dado tem que vir por completo, íntegro". Neste mesmo pensamento, o supervisor de TI afirma: *"elas contribuem justamente por conseguir disponibilizar a informação, tanto internamente, para a diretoria e também externamente caso solicitem ela. É sempre buscando a segurança da informação e a disponibilidade dela".*

Abordam-se a seguir as questões que envolvem o domínio D4.

- **4. Proteção e privacidade de informações de identificação pessoal (D4):**

4.1)	Esta questão verifica como é política de privacidade e proteção de dados da organização, bem como sua relevância permitindo interpretar e avaliar os regulamentos para limitar as perdas. Conceitos: confidencialidade; relevância; avaliação de risco.

Identificou-se que os gestores das áreas financeira, controladoria e contabilidade não tem o conhecimento sobre a política de privacidade e proteção de dados da organização. Já a coordenadora fiscal comenta sobre um termo de responsabilidade, que é assinado no momento da contratação do funcionário, ela relata: "*Quando a gente é contratada a gente assina alguns termos e, se não me engano, tem um que trata sobre a questão das informações confidenciais da empresa".*

A coordenadora de custos/planejamento também corrobora a explicação da coordenadora fiscal: "*Quando a gente ingressa na empresa [...] a gente recebe toda uma política interna e também nós gestores assinamos outro termo porque temos acesso as informações fora da empresa, temos acesso ao sistema fora da empresa*".

Os gestores da área de TI afirmam que existe uma política de privacidade e proteção de dados. A gerente de TI relata: *"a política de privacidade a gente lida com esses perfis de acessos dos usuários. Se consegue privar determinados acessos, isso está escrito está documentado na política. Eu considero essa política hoje muito boa [...].*

O supervisor de TI complementa: *"a pessoa não poder transmitir e violar informações e também ir contra os princípios da organização. Não se pode fornecer*

informações confidenciais da empresa para alguém externamente. Estas recomendações estão na política de TI e documentada".

4.2)	Esta questão verifica como ocorre a comunicação da política de privacidade e proteção de dados da organização para todas as pessoas envolvidas no processo. Recomenda-se que seja exposta de forma mais compreensível possível ao usuário, possibilitando a construção de uma boa imagem perante seus *stakeholders*. Conceitos: disponibilidade; compreensibilidade; reputação corporativa.

Questionou-se aos gestores sobre como ocorre a divulgação da política de privacidade e proteção de dados e, como os gestores das áreas financeira, controladoria e contabilidade não tem o conhecimento dessa política, os mesmos também não sabem como ocorre essa divulgação.

A coordenadora de custos/planejamento afirma que essa política é pouco divulgada, ela explica: "*Eu acho que ela é pouco divulgada, ocorre uma única vez de forma presencial e depois não mais"*. O mesmo ocorre sob a percepção da coordenadora fiscal, ela explica: "*Ela [a política] é pouco divulgada, mas no departamento fiscal a gente tem um acordo, pode se dizer assim, uma ética profissional de não ficar comentando coisas que acontecem dentro da empresa para o ambiente de fora da empresa*".

Em contrapartida, os gestores de TI afirmam que essa política é exposta de forma mais compreensível possível ao usuário. Segundo a gerente de TI*: "primeira divulgação ela é dada no momento que alguém solicita o acesso para um novo colaborador [...] Fazemos também um comunicado [via e-mail] estes comunicados ficam expostos em painéis para que todos leiam essa nova política [...] esse ano nós fizemos uma revisão dela e se publicou ela recentemente totalmente redesenhada, revisada inclusive junto com a diretoria, ela está completa. Essa política estava há quatro anos sem ser atualizada e este ano nós a atualizamos".*

O supervisor de TI confirma o relato da gerente de TI: "*Sempre que essa política é atualiza é disparado um e-mail, um comunicado para toda a empresa e [...] sempre que uma pessoa entra na empresa ela é informada desta política e assina o termo de responsabilidade*".

Questionou-se também aos gestores sobre a percepção dos *stakeholders* quanto à política de privacidade e proteção de dados da organização. Neste sentido, os gestores de controladoria, contabilidade, fiscal e financeiro acreditam que os *stakeholders* não percebem. De acordo com o gerente financeiro: "*Eu acho que não por que eu que sou funcionário não consigo perceber, imagino que eles não devem perceber*". Já a coordenadora de custos/planejamento respondeu: *"No site da empresa tem, consta lá que a empresa segue as políticas, mas eu não sei se eles percebem algo sobre atuação propriamente desta política".*

O supervisor de TI acredita que essa política não precisa ser percebida pelos *stakeholders*, conforme esse gestor: "*na minha opinião não tem que chegar até eles*". Em contrapartida, a gestora de TI acredita que essa divulgação aos stakeholders é importante, ela afirma: "*Eu acho que essa divulgação para os stakeholders é importante, justamente para eles saberem da segurança que é feita na empresa. Sempre se tem as reuniões do conselho também, de repente isso foi divulgado para eles*".

4.3)	Esta questão verifica se existe uma pessoa responsável (*privacy officer*) que tem a função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos a serem seguidos. Essas orientações devem ser expostas de forma compreensível ao usuário, possibilitando um padrão de excelência percebida pelos *stakeholders*. Conceitos: política de segurança; compreensibilidade; criação de valor.

Constatou-se que não existe uma pessoa responsável pela função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos a serem seguidos.

Neste sentido, a coordenadora contábil afirma: "*Hoje não existe esta pessoa. Quanto se tem alguma dificuldade técnica sobre sistema a gente consulta a área de TI [...] procuramos buscar ajuda*". Isso é corroborado pela coordenadora fiscal: *"Se eu precisar de alguma questão eu abro um chamado e alguém do TI vai me atender*". O gerente financeiro complementa: *"eu acho que tem uma pessoa do TI que faz vários papéis, mas não exclusiva para a segurança".*

Já a coordenadora de custos/planejamento afirma: “*quando for alguma dúvida relacionada à segurança eu faço um chamado e alguém me atende*”. Isso é corroborado pelo supervisor de TI: *“Se o gestor quiser alguma informação sobre segurança da informação ele vai solicitar via chamado e alguém vai ajuda-lo, mas não tem uma pessoa específica. O que posso te garantir é que existem pessoas que entendem sobre segurança da informação, eu sou uma delas, eu conheço toda a parte se segurança de informação da empresa [...] não vejo necessidade de colocar uma pessoa para isso, é uma responsabilidade da área de TI e não de uma pessoa apenas*”.

Conforme a gerente de TI: *“[...] hoje essa pessoa seria eu ou o supervisor de TI. A nossa equipe é bem enxuta, ela deveria ser maior até para a gente segregar melhor as tarefas. Isso é uma cobrança que a gente tem praticamente de todas as auditorias que passam na empresa, são as segregações de atividades dentro do setor*”.

Quanto ao perfil laboral da pessoa para cuidar da segurança da informação, a gerente de TI revela: “*Essa pessoa tem que conhecer toda a política de TI, conhecer toda a organização de infraestrutura e negócio, tem que entender detalhes do negócio relacionados ao SAP e, na parte de infraestrutura pelo menos a parte básica de servidores, como isso está organizado fisicamente, para conseguir orientar de forma adequada os usuários. Hoje a gente faz isso, comigo mesma, se a gente observa que alguém não está respeitando parte da política já envia um e-mail ao gestor, orientando o procedimento correto e alertando os riscos para a empresa*”.

Conclui-se que apenas a prática de política de privacidade e proteção de dados é utilizada, porém esta política deveria ser mais divulgada aos usuários.

Por fim, questionou-se aos gestores quanto à contribuição desta prática (política de privacidade e proteção dos dados) para a conformidade.

Os gestores de controladoria, contabilidade e financeiro não sabem como estas práticas podem contribuir, pois ele desconhece o uso delas. Segundo o gerente financeiro: “*Estas práticas não são claras, podem até serem aplicadas, mas não é de domínio de todos. Eu não sei como elas podem contribuir para a conformidade*”.

Já a coordenadora de custos/planejamento acredita que estas práticas devem ser melhoradas, ela afirma: “*Eu acho que falta ainda nós nos adequarmos a estas práticas, não temos essa pessoa específica sobre segurança e a divulgação da*

política poderia ser melhorada. Essas práticas poderiam contribuir se fossem mais bem implantadas".

Já a coordenadora fiscal acredita que a política de privacidade e proteção de dados pode contribuir para a conformidade, ela afirma: *"Eu acho que contribui os funcionários não podem expor a empresa e evitam boatos no mercado".*

O supervisor de TI acrescenta a responsabilidade do funcionário para a contribuição da conformidade. Ele explica: *"[...] no momento que o funcionário toma ciência da sua responsabilidade, isso vai garantir a segurança, vai reduzir riscos para a empresa".*

Na percepção da gerente de TI a política de privacidade e proteção de dados e sua divulgação, contribuem para a conformidade. Ela afirma: "*no momento que o funcionário entra na empresa e assina o termo aquele, ele tem a responsabilidade pela confidencialidade das informações. E assim como quando um gestor é desligado da empresa, a gente segue todos os trâmites de segurança para que não exista vazamento de informação, mesmo sendo um gestor. Quando alguém é demitido o RH já informa a TI para retirar o acesso às informações dessa pessoa [...] tudo para mitigar ao máximo o vazamento da informação*".

Na sequencia, apresentam-se as práticas relacionadas ao domínio D5.

- **5. Regulamentação de controles de criptografia (D5):**

5.1)	Esta questão verifica como é o uso de criptografia, se ocorrem com cautela de acordo com o cumprimento de normas reguladoras internas. Conceitos: confidencialidade; prudência ou conservadorismo; conformidade.

Identificou-se que apenas os gestores da área de TI têm conhecimento sobre o uso da criptografia.

O supervisor de TI explica como funciona os níveis de criptografia: *"Para que o usuário possa acessar o sistema de SAP hoje ele precisa ter um usuário, então no momento que ele tem um usuário e uma senha se tem um nível de segurança. É obrigado que o usuário tenha uma senha complexa, de pelo menos oito caracteres contendo letras maiúsculas, minúsculas, símbolos e números e ter no mínimo oito caracteres. Isso vai garantir uma segurança de que somente aquela pessoa vai ter acesso a informação que está no sistema".* A gerente de TI complementa: "*estamos*

implantando um projeto para criptografar todas as informações que constam nos notebooks dos gestores".

5.2)	Esta questão verifica como a assessoria jurídica garante a conformidade com as legislações e regulamentações, de forma a possibilitar a informação livre de erros, vieses e manipulações, por meio do cumprimento de normas internas e externas. Conceitos: conformidade; representação fidedigna; conformidade.

Constatou-se que todos os gestores utilizam-se da assessoria jurídica para garantir a conformidade com as legislações e regulamentações, principalmente no que envolve os contratos.

Neste sentido, o gerente de controladoria afirma: "*Nós temos um departamento jurídico e temos pessoas especializadas em cada uma das áreas do direito. Tudo aquilo que dentro do nosso escopo de área de jurídico não engloba, ou não tem o conhecimento, ou precisa de alguém mais especialista, se busca as pessoas mais especialistas externamente*". O gerente financeiro acrescenta uma informação importante: "*[...] toda e qualquer mudança que se tenha, por exemplo, em contrato [...] existe a aprovação jurídica. Todo o contrato tem que passar pela assessoria jurídica*".

Conforme a coordenadora contábil: "*Para a contabilidade a assessoria jurídica nos auxilia muito na parte de contratos, como por exemplo: contratos de aluguéis, com clientes, fornecedores, transações entre as empresas*". Já na parte fiscal, a assessoria jurídica participa de assuntos focados na área de impostos "*[...] na parte fiscal a gente busca serviços de consultoria externa mais focada na área de impostos. O nosso departamento jurídico não atua muito na questão tributária, geralmente buscamos serviços mais especializados na área tributária*".

As declarações das coordenadoras de contabilidade e fiscal são corroboradas pela coordenadora de custos/planejamento: "*[...] eu acredito que a área fiscal utilize este departamento bem mais em função das legislações que tem. Nós aqui utilizamos em nível de contrato [...] a gente sempre aciona o jurídico para elaborar e revisar contratos*".

Na área de TI a assessoria jurídica é destacada pelo supervisor de TI: *"setor jurídico [...] sempre nos auxilia nas demandas de TI. Vou explicar esta questão com*

um exemplo: nós criamos internamente uma área de convivência na empresa e que disponibiliza acesso a internet para todos os funcionários [...] Cada pessoa tem o seu usuário e senha, que é diferente do login do sistema de trabalho dele, é outra rede é tudo separado, não se tem acesso aos dados da empresa. A gente criou um termo de responsabilidade que a pessoa aceita quando ela vai acessar aquela rede, ali tem informações que essa pessoa não pode distribuir conteúdo pornográfico, pedofilia, a empresa é contra ameaças na internet, por exemplo. O setor jurídico ajudou a TI na confecção deste termo de responsabilidade. Outras ajudas que temos do setor jurídico são na aquisição de softwares, contratos de prestação de serviços".

Outros exemplos são citados pela gerente de TI, no que refere-se a assessoria jurídica: "*[...] a gente sempre os aciona para nos auxiliar na parte contratual. Por exemplo, no projeto de rollout do SAP [...] a empresa contratou consultores independentes, a gente fez vários contratos individuais com diversos consultores para cada frente daquelas comentadas anteriormente [...] a parte jurídica nos ajudou muito nesse sentido tivemos que ter um contrato para cada um destes consultores, depois nós tivemos que rescindir cada um destes contratos [...]. A assessoria jurídica nos ajuda também caso a gente tenha algum incidente desagradável com algum fornecedor, nós tivemos um caso assim. O jurídico entrou para nos apoiar e foi elaborado um contrato de segurança, para que o fornecedor concluísse o trabalho dele e, se ele não terminasse, nós não pagaríamos aquilo tudo [...] Em outro momento que o jurídico nos apoiou foi quando nós monitoramos um colaborador [...] este colaborador fez mal uso de um usuário e senha que não era de uma pessoa e sim de um portal. A TI entrou evidenciando que a política não estava sendo cumprida que o usuário estava agindo de forma indevida, o RH acompanhou esse processo e a área jurídica também*".

Investigou-se também se a assessoria jurídica possibilita que a informação seja livre de erros, vieses e manipulações. Os gestores acreditam que a assessoria contribui. Segundo a coordenadora contábil: *"Acredito que [...] a assessoria jurídica tem o conhecimento da legislação, garantindo que as transações estejam de acordo, ela garante que a informação seja mais confiável devido a seu conhecimento jurídico".* Neste sentido, a coordenadora fiscal afirma: "*Sim, pois selecionando o profissional, contratando um especialista da área, é uma forma de evitar esses riscos*".

Ainda confirmando a importância da assessoria jurídica, a coordenadora de custos/planejamento explica: "*[...] dá mais segurança, porque se tem o aval, a maioria das áreas da empresa são leigas nesta questão jurídica. Dá mais segurança para o gestor [...]*", isto é corroborado pelo supervisor de TI: "*Com certeza. [a assessoria jurídica] têm o conhecimento da área jurídica e reduz o risco de algum problema acontecer, pois eles têm um conhecimento específico desta área*".

Das práticas apresentadas no domínio D5, conclui-se que há a utilização de todas as práticas pela empresa. Por fim, questionou-se aos gestores quanto à contribuição destas práticas (uso de criptografia; assessoria jurídica) para a conformidade.

Constatou-se que a prática de criptografia foi evidenciada apenas a área de TI. Segundo o supervisor de TI: *"com a criptogradia a empresa disponibiliza segurança para o uso de seus colaboradores seja um software, internet ou qualquer outra coisa [...] a governança trabalha neste sentido, de que as informações estarão disponíveis e seguras".* No entanto, a gerente de TI afirma que a contribuição pode ser melhorada: *"Pode contribuir ao efetivarmos o uso da criptografia, colocar a criptografia internamente nos dados críticos [...] sobre a parte contábil, dados contábeis são dados críticos, então trabalhar nessa parte seria positivo".*

No que se refere à assessoria jurídica todos os gestores acreditam que ela contribui para a conformidade. Conforme a coordenadora de contabilidade: "*As assessorias jurídicas garantem que as informações estejam em conformidade com legislação*". Já a coordenadora fiscal afirma que: "[...] *contribui, pois há um conhecimento mais específico da área tributária, contribui de forma preventiva minimizando os riscos.*

A coordenadora de custos/planejamento complementa: "*[...] contribui porque nos dá segurança, por seguir a legislação, as normas de forma correta. Temos um respaldo de pessoas específicas sobre o assunto*". Já o gerente financeiro diz que a assessoria jurídica é essencial, ele afirma: *"A questão jurídica contribui, pois se tem o embasamento técnico e legal de que aqueles contratos que estão sendo firmados são amparados judicialmente, para evitar colocar em risco a saúde da companhia. Eu acho que é essencial a passagem pela área jurídica".* Neste sentido o gerente de controladoria afirma: *"a questão jurídica é importante por que nós não somos especialista nessa área".*

Sob a perspectiva da gerente de TI, a assessoria jurídica contribui *"[...] com as ações de acompanhamento contratual ou acompanhamento de ações irregulares internas dos usuários, nesse sentido eles nos apoiam para a gente ter sempre a conformidade dos processos e manter a segurança da informação".*

Evidenciam-se a seguir as práticas relacionadas ao domínio D6.

- **6. Análise crítica independente da segurança da informação (D6):**

6.1)	Esta questão verifica se a análise crítica da segurança da informação é iniciada pela direção de forma confiável para que o usuário aceite a informação e a utilize, construindo uma boa imagem perante os *stakeholders.* Conceitos: política de segurança; confiabilidade; reputação corporativa.

Obteve-se diferentes percepções quanto a análise crítica iniciada pela direção. As coordenadoras da contabilidade, fiscal e gerente de TI acreditam que a análise crítica da segurança da informação não é iniciada pela direção, ela é iniciada pelos gestores.

Já o supervisor de TI e a coordenadora de custos/planejamento afirmam que essa análise crítica pode ser iniciada por todos os funcionários, gestores e diretoria. No entanto, o gerente de financeiro considera que esta análise é iniciada pela direção e, o gerente de controladoria desconhece como ocorre este procedimento.

Respondendo a questão, a coordenadora contábil relata: *"[...] pode haver a análise critica pela direção, mas nem sempre ela é iniciada lá. Geralmente ela é iniciada dentro da contabilidade, quando se tem evidências de algum processo que não está correto é corrigido*". Neste pensamento, a gerente fiscal afirma: "*Eu acho que é mais iniciada pelos gestores, conforme a necessidade dos gestores é reportada à direção*".

O mesmo ocorre no discurso da gerente de TI: "*Eu acho que não é iniciada pela direção, atualmente eu vejo que ela está sendo iniciada mais pela TI mesmo. Nos últimos meses, a gente tem presenciado umas diferenças de pensamentos e cuidados vindas principalmente do nosso presidente [...] e desta forma nos trás sugestões. Muitas vezes essas sugestões são ligadas mais a produção dentro do SAP, se olhar a parte segurança na área de produção e SAP ele nos trás várias*

sugestões, em função do conhecimento dele, de grande envolvimento dele na produção".

Já o supervisor de TI afirma que a análise crítica "*[...] tem que ser iniciada por qualquer pessoa da empresa, não necessariamente pela direção. Eu acho que pode ser iniciada pela direção, mas não necessariamente [...] eu acredito que os funcionários conseguem perceber essa segurança, por que quando eles tentam utilizar uma senha que, por exemplo, seja igual as últimas 10 senhas, ou que seja com menos de 8 caracteres, ou quando eles tentam acessar um site que está bloqueado [...] São nestes momentos que eles percebem que existe uma segurança aplicada ao negócio. Eu acho que os stakeholders não sabem desta análise crítica.*

Alinhada à percepção do supervisor de TI, a coordenadora de custos/planejamento afirma: "*[...] eu acho que é o conjunto todos os funcionários, gestores e com o apoio da direção. Eu acho que a percepção é mais interna do que externa, para fora da organização a gente só consegue saber se vasar a informação [...]*".

Em contrapartida, o gerente financeiro acredita que a análise crítica é iniciada pela direção, ele relata: "*[...] temos algumas regras de compliance de demonstrações financeiras e vem da direção e também da parte de relação com investidores. Eu acho que os stakeholders percebem com certeza, primeiro por que a empresa nunca teve nenhum tipo de informação que foi vasada ao mercado antes do período. A própria questão da auditoria externa é uma garantia da segurança da informação".*

Já o gerente de controladoria explica: "*Não sei te responder se inicia por eles. Eu não sei te dizer como é este processo. Acho que eles são o principal cliente da informação digamos assim para a tomada de decisão, mas que começa por eles, sem dúvida é uma preocupação deles, não saberia te responder*".

6.2)	Esta questão verifica como a análise crítica inclui a avaliação de oportunidades para melhoria e necessidade de mudanças para o enfoque da segurança da informação evidenciando suas diferenças e semelhanças para a busca de excelência operacional percebida pelos *stakeholders*. Conceitos: política de segurança; comparabilidade; criação de valor.

Constataram-se diversas percepções quanto à avaliação de oportunidades para melhoria da segurança da informação.

A coordenadora fiscal relata que a auditoria externa evidencia as oportunidades de melhoria, ela explica: "*A auditoria externa também coloca no relatório as sugestões de melhoria que geralmente nós as aderimos, geralmente essas oportunidades não tem um impacto financeiro*".

Já a gestora contábil afirma que oportunidades de melhorias são feitas pela área contábil, após o levantamento feito pela análise crítica independente. A gestora afirma: "*Quando a contabilidade recebe as não conformidades levantados pela auditoria, a própria contabilidade avalia e traça as metas de correção oportunidades, após responde para à direção".*

De acordo com a coordenadora de custos/planejamento não se tem uma avaliação contínua de melhoria, ela explica: *"*Eu acredito que hoje não se tem um processo contínuo de revisões de melhoria, eu acho que só quando surge o problema é que se verifica a oportunidade de melhoria*".*

O gerente financeiro acredita que a análise crítica executada pela auditoria externa não inclui a avaliação de oportunidades, ele explica: "*Eu acho que a segurança da informação não, eu acho que eles avaliam a qualidade da informação e não a segurança dela. Eu acho que a segurança é muito voltada para a TI*".

Alinhada à percepção do gerente financeiro, o gerente de controladoria afirma: *"[...] Eu acho que a oportunidade está na própria área de TI em estar preocupada em trazer isso para a direção avaliar [...]".*

Ainda sobre a avaliação de oportunidades de melhoria na segurança da informação, a gerente de TI exemplifica: *"Eu vejo que essa questão está partindo muito da área de TI [...] nós sabemos que tem uma oportunidade de melhoria, que é trocar a ferramenta de backup para que ele não seja mais em fita, que ele seja feito em nuvem ou em disco [...] a oportunidade está em investir em uma ferramenta que é um pouco mais cara agora, mas que vai trazer uma segurança e agilidade de busca da informação muito maior e melhor, o retorno deste investimento será em breve. A gente consegue identificar essas e outras oportunidades de melhoria participando e indo a eventos de TI ou por e-mails que a gente recebe das empresas. A auditoria externa também faz algumas sugestões".*

Isto é corroborado pelo supervisor de TI: "*Hoje eu tenho participado de várias palestras externamente, congressos propriamente sobre segurança da informação.*

Como a gente conhece tecnologia, a gente consegue saber o que pode ser aplicado na empresa, algumas a gente consegue aplicar, mas outras não. Sempre que a gente pode aplicar algo para melhorar a segurança da informação a gente faz. A gente sabe que existem hoje diversas ameaças na internet e sob todas as formas, as ameaças digitais, a gente sempre tenta trazer o melhor para a empresa".

Quanto à percepção dos *stakeholders*, o gerente de controladoria acredita que eles percebem as oportunidades de melhoria na segurança da informação, ele explica: *"Eu acho que os stakeholders percebem, até pelos investimentos que são feitos na área, a própria mudança de sistema, o investimento que é feito em tecnologia por parte da companhia, sem dúvida os stakeholders percebem isso".*

Já o supervisor de TI acredita que os stakeholders não percebem, ele afirma: "*Os stakeholders não conseguem perceber, eu não sei se eles precisariam saber disso. Eu acho que essa questão está na área de TI, verificando oportunidades de melhoria sem divulgar aos stakeholders*".

6.3)	Esta questão verifica se a análise crítica inclui políticas e objetivos de controle relevantes, capazes de fazer a diferença na gestão preventiva de riscos, monitoramento e supervisão contínua dos processos. Conceitos: política de segurança; relevância; risco.

Identificou-se que a percepção dos gestores das áreas financeira, fiscal, contábil e TI diverge dos gestores de controladoria e custos/planejamento.

O gerente financeiro acredita que a análise crítica executada pela auditoria externa é capaz de fazer a diferença na gestão preventiva de risco, ele afirma: "*A auditoria externa vem trimestralmente na empresa, é feita uma auditoria das nossas demonstrações financeiras e processos, então somos auditados quatro vezes ao ano. A auditoria tem um checklist do processo, por exemplo, eles pegam um processo do contas a pagar. Exemplo a nota fiscal de número 2, verificam quem lançou a nota fiscal 2, quem aprovou a nota fiscal 2, quem pagou a nota fiscal 2 e pedem a evidência física, para verificar a se ela realmente existe e se está lançada corretamente no sistema*".

A coordenadora fiscal explica como essa auditoria pode mitigar o risco: "*havendo uma revisão do trabalho, principalmente por uma empresa independente, ajuda a reduzir o risco e de expor a empresa".* A coordenadora contábil afirma que

"*Qualquer evidência de erros, de análises que não esteja adequada, a auditoria informa a contabilidade e os ajustes são efetuados*".

Conforme o supervisor de TI a auditoria faz a diferença, pois "*[...] são verificados todos os processos que existem na área e se eles estão sendo cumpridos ou não. Se eles não estiverem sendo cumpridos obviamente vai gerar um ponto de auditoria para que seja corrigido. E se ninguém fizer essa verificação, tem coisas que são básicas e importantes que podem não ser vistas*". Nesta mesma perspectiva, a gerente de TI afirma: "*[...] com essa avaliação da auditoria, se tiver algum risco exposto, a gente tem que trabalhar em relação a este ponto, fazer um plano de ação com prazo e cumprimento desta ação*".

Em contrapartida, a coordenadora de custos/planejamento acredita que a análise crítica da auditoria externa não é capaz de fazer a diferença na gestão preventiva de riscos. Esta gestora explica: "*Eu acho que ela não é focada em prevenção, ela é focada na análise do resultado que já ocorreu ela analisa o resultado que já foi efetivado, mas na prevenção de possíveis riscos ou prever algo que possa acontecer eu acho que não".*

Já o gerente de controladoria afirma que a auditoria externa ajuda, mas fazer a diferença na prevenção de riscos está voltada à equipe: "*Eu acho que ajuda, mas o fato de fazer a diferença está muito mais em fazer com a nossa equipe do que com a propriamente com os consultores externos. Eu acho que eles são apoiadores, são facilitadores, mas em termos de processo do dia-a-dia é a nossa equipe que tem que garantir isso*".

6.4)	Esta questão verifica como é executada a análise crítica e, se esta reflete de fato o que ocorreu independente de um contrato. Deve fornecer evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever. Conceitos: política de segurança; primazia da essência sobre a forma; legitimidade.

Identificou-se que a auditoria crítica é realizada por uma auditoria externa. Segundo o gerente de controladoria essa auditoria atesta os números da empresa, ele afirma: "*Nós temos a auditoria externa, temos uma auditoria interna hoje que está realizando outro trabalho, mas hoje nós temos a auditoria externa que atesta os*

nossos números, faz a devida auditoria trimestralmente e depois no final do ano um pente fino mais apurado em cima dos nossos números, que é a KPMG [...] Na confiabilidade das informações e evidencias de conciliações de análises, eles auditam processos também, tanto o contábil o balanço quanto os nossos processos internos também". O gerente financeiro complementa: "*A KPMG faz auditoria contábil, financeira e de processos*".

A coordenadora fiscal relata um exemplo desta auditoria externa: "*agora em dezembro nós vamos receber a auditoria externa, eles vão auditar todos os impostos de janeiro a setembro, nós vamos entregar todos os registros de entradas e saídas, todas as obrigações entregues ao fisco, e eles cruzam estas informações com o balanço. Quando eles possuem alguma dúvida há o questionamento para a área fiscal*".

A coordenadora de custos/planejamento acrescenta que há também uma análise crítica interna, ele explica: *"Internamente [...] gente analisa os lançamentos contábeis, passa por uma criticidade interna. Como a gente conhece os números da organização, quando há alguma distorção a gente atua também, mas o aval final até pela empresa ser uma companhia de capital aberto é feito pela auditoria externa*".

Na visão da coordenadora contábil, a análise crítica inclui as análises feitas pela própria área de contabilidade, contador e diretoria, bem como a auditoria externa. Essa gestora explica: "*A análise crítica começa a ser feita a partir das conciliações. Nós fazemos a análise das conciliações, o contador também efetua a análise crítica em relação às demonstrações contábeis, através de relatórios gerados pelo sistema SAP. A auditoria externa, através dos trabalhos que são realizados trimestralmente na empresa, existe uma validação das informações, registros e processos, pela auditoria externa [...] a diretoria que também faz análise crítica nos relatórios que são enviados a eles*".

Na área de TI, o supervisor comenta: *"Essa auditoria [externa] audita a área contábil, fiscal, e TI por exemplo".* Já a gerente de TI explica em detalhes como funciona esta questão: "*Não temos hoje uma auditoria específica para a TI, temos na empresa a KPMG que é uma auditoria externa. Eles nos auditam, mas sempre vinculado na questão na contabilidade, até mesmo processos voltados à contabilidade. Até hoje nós sempre participamos dessas auditorias no quesito de processo contábil, eles entram bem detalhado, eles querem ver se o usuário teve formulário, cadastramento, perfil de acesso dentro do ERP, segregação de tarefas e*

ambientes, eles querem ver como é feita a movimentação dos dados para a produção, se existe controle disso. É uma auditoria bem completa, eles dizem para nós da TI que isso é para ter segurança da informação dos dados contábeis, é sempre nesse foco. Essa auditoria nos ajuda, porque eles levantam alguns pontos que eles consideram importantes para a segurança. A gente padroniza e coloca procedimentos, desta forma a gente atende a todos não só a parte contábil inclusive ao meu próprio processo de TI.O SAP nos audita anualmente, mas é só para aquela questão das licenças, para verificar se estamos utilizando o que compramos e se tem algo a mais para pagar".

Questionou-se de que forma a análise crítica fornece evidências aos *stakeholders* que está cumprindo com o seu dever. Todos os gestores acreditam que a auditoria externa consegue fornecer estas evidências.

De acordo com o gerente de controladoria: "*Eu acho que sim, eu acho que uma das funções da auditoria é exatamente isso. Eles dão conformidade aos números que estão ali, eles avaliam os principais números que estão nas demonstrações, eles dão confiabilidade nas informações da companhia*".

Neste sentido, o gerente financeiro afirma: "*Se tem a garantia de todo e qualquer processo e demonstrações financeiras foi verificado por um terceiro que garante que as informações tão corretas*".

Na visão da coordenadora de custos/planejamento, a auditoria externa cumpre com o seu dever "*Até porque a auditoria externa tem que seguir uma legislação, ela segue parâmetros, leis. Ela é um suporte para os acionistas*". Esta visão é compartilhada também pela coordenadora fiscal: "*é uma segurança para os stakeholders de que o que está sendo feito está de acordo com a legislação, ou seja, o fiscal está cumprindo com a obrigações, o mesmo ocorre para o contábil, os dois setores devem estar alinhados*".

A forma de como essa informação é evidenciada pela auditoria externa aos *stakeholders* é abordada pela coordenadora contábil: "*A auditoria externa emite um parecer de auditoria sobre as demonstrações contábeis e estes pareceres ficam disponíveis aos stakeholderes*".

Esta forma de evidenciação é desconhecida pela supervisor de TI: "*Nós fornecemos as informações à auditoria externa, na verdade tudo o que envolve o sistema da empresa, é verificada a questão da segurança e processos. Elas fornecem um parecer sobre estas questões, mas como ela evidencia isso aos*

stakeholders eu não sei". Já a gerente de TI sabe como ocorre a evidenciação aos *stakeholders*: "*Eles fazem sempre um relatório e é bem completo para nós internamente, para os stakeholders eles fazem um mais gerencial ou macro*".

6.5)	Esta questão verifica como os resultados da análise crítica independente são registrados e relatados à direção. Isto ocorre de forma neutra, não havendo viés de resultado por meio de informações úteis aos usuários, permitindo um clima de confiança.
	Conceitos: integridade; neutralidade; transparência.

Verificou-se que os resultados da análise crítica independente são registrados e relatados à direção, todos os gestores explicaram que esses resultados ocorrem por meio de um relatório, um parecer de auditoria.

Sendo assim, o gerente financeiro afirma: "*Eles têm um relatório de auditoria que é feito trimestralmente, e não só para diretoria da empresa, vai para o conselho e todo o mercado. Há um relatório formal de tudo o que está acontecendo na empresa. São publicadas, vai para a CVM e segue um rito bem rigoroso*".

O gerente de controladoria explica como isto ocorre: *"[...] é feito um relatório, o nosso balanço divulgado ele exige que seja auditado e exige-se que a própria auditoria emita um parecer, para que estes números possam ser divulgados e a própria auditoria faz a aprovação destes números*".

Já a coordenadora de custos/planejamento explica este procedimento, focando a área interna: *"eles chamam de relatórios internos de controles da KPMG, todo o final de ITR eles entregam esse relatório informando o que eles enxergaram, números que eles não concordam por exemplo. Todo o trimestre tem o report da auditoria externa para a diretoria*". Isto é corroborado pela coordenadora fiscal: "*[...] É feito um relatório de auditoria e é entregue à direção [...]*".

Neste sentido, a coordenadora contábil explica sobre os pontos levantados pela auditoria: "*No final do trabalho da auditoria externa eles fazem um relatório com todos os pontos, sejam eles de correção ou melhoria de processos que são levados à diretoria e são trabalhados prazos para a correção".*

Os gestores da área de TI relatam sobre um software utilizado pela auditoria para evidenciar os pontos a serem tratados. O supervisor de TI explica: "*A empresa tem um software chamado Teammate onde qualquer ponto de auditoria que foi*

gerado durante a auditoria é escrito no software. O gestor da área terá conhecimento que houve um ponto de auditoria na área dele e estas informações são reportadas para a diretoria. A KPMG que é a auditoria externa gera os relatórios e a interna abastece as informações. Cada gestor consegue visualizar a sua área, eles tem um usuário e uma senha, eu não consigo visualizar a área fiscal, por exemplo, só a diretoria consegue visualizar todas as áreas. Eu não sei se a auditoria entrega também uma via em papel sobre as questões de não conformidade".

A gerente de TI complementa a informação prestada pelo supervisor de TI: "*Os pontos de auditoria são colocados nessa ferramenta e semanalmente é enviado um e-mail com cópia para a diretoria contendo os pontos que estão em aberto, daí nesta ferramenta a gente coloca o plano de ação tomado e eles acompanham*".

Questionou-se também aos gestores se os resultados da análise crítica refletem/proporcionam a transparência das informações e, constatou-se que todos os gestores acreditam que sim.

Neste sentido, gerente financeiro afirma: "*Com certeza. Por que a auditoria auditou todo o processo e demonstrações da empresa e passou isso ao mercado, ela está dizendo que tudo que está sendo feito aqui dentro está ok e que essas informações podem ser divulgadas e que os próprios acionistas da empresa podem confiar nos números. A auditoria externa tem responsabilidade também, ela não pode divulgar nada que não seja correto*".

Alinhada à percepção do gerente financeiro, a coordenadora fiscal relata: "*Eu acredito que a empresa consegue demonstrar de forma transparente ao mercado o que de fato ocorre na empresa, pois é auditada por uma empresa independente que também tem uma responsabilidade. Essa auditoria externa valida os dados, eles fazem uma análise do processo por amostragem, isto é uma garantia de que estamos em conformidade*".

A coordenadora contábil relata de que forma a análise crítica proporciona a transparência dessas informações: "*Através do relatório de auditoria, que relata os pontos de forma detalhada e com recomendações".* A coordenadora de custos/planejamento complementa: "*Eu acho que sim. Porque isso mostra que a auditoria externa está enxergando as coisas, não é porque o número está fechado que está certo, eles criticam os números".*

A gerente de TI justifica sua resposta: "*[...] eles montarem este relatório e divulgarem para a diretoria e para os stakeholders isso reflete sim a transparência.*

Eles evidenciam o que está acontecendo [...] acho que proporciona sim, até pelo fato deles serem uma auditoria independente, eles fazem este parecer imparcial, isso fica totalmente transparente sem manipulação". Isto também é justificado pelo supervisor de TI: "*[...] no momento que se é auditado por uma empresa externa vai aparecer se existe algo não conforme [...]*".

Corroborando com os demais gestores, o gerente de controladoria afirma: *"[...] temos um público importante, conselho, acionistas e eu acho que sim, é um processo transparente, evidenciado pelos relatórios de auditoria e relatórios de controles internos".*

6.6)	Esta questão verifica como a direção efetua ações corretivas quando os resultados da análise crítica forem inadequados ou não conforme pela segurança da informação. De forma a garantir a confiança da informação e cumprir com obrigações de suas responsabilidades. Conceitos: conformidade; confiabilidade; responsabilidade.

Sob a percepção dos gestores das áreas fiscal, contabilidade, TI, constatou-se que as ações corretivas são executadas por meio de um plano de ação que é desenvolvido pelo gestor da área não conforme. Já a coordenadora de custos/planejamento relata que estas ações ocorrem por meio de reuniões com a diretoria. No entanto, o gerente de controladoria diz não haver um único processo de ação corretiva e, por fim, observou-se que o supervisor de TI desconhece como ocorrem estas ações corretivas.

Quanto a questão de pesquisa evidenciada, a coordenadora fiscal afirma: "*Normalmente não chega na diretoria, a gente recebe o relatório com a divergência e já efetuamos os comentários e um plano de ação para resolvê-la. Somente após o plano de ação que vai para a diretoria. A própria auditoria interna controla esse tipo de ocorrência, eles nos cobram um prazo e uma ação de correção*".

Na área contábil, a coordenadora explica: *"Os pontos de auditoria que são levantados são respondidos pela contabilidade e possuem um prazo de correção. A contabilidade é quem determina o prazo para as ações corretivas*".

A gerente de TI concorda com as coordenadoras das áreas fiscal e contabilidade. Ela acrescenta o software onde são colocados os pontos de não

conformidade: "*[...] Eu vejo que isso ocorre pela ferramenta que temos hoje, Team Central [...]*".

Já a coordenadora de custos/planejamento mencionou a reunião como uma ação corretiva. Ela explica: "*Quando é um problema interno, a diretoria faz reuniões para tentar realinhar o processo que está causando a não conformidade. Quando é mais da auditoria externa, daí é um pouco mais forte, por exemplo: isso aqui está fora da lei, fora da legislação [...] O foco é reunir as pessoas responsáveis para corrigir a informação [...]*".

No entanto, o gerente de controladoria diz não haver um único processo de ação corretiva, ele explica: "*[...] eu não acho que tenha um remédio igual para todos, depende [...] acho que a atuação é em cada um dos processos, com os lideres de áreas entendendo qual a não conformidade, entendendo o que levou a ter a não conformidade, e aí a atuação vai desde a correção do processo, troca de pessoas, enfim depende muito de qual é a não conformidade para se fazer a ação*".

Ainda sobre a questão apresentada, o supervisor de TI diz não ter conhecimento sobre como a direção efetua as ações corretivas: "*Eu não tenho conhecimento exatamente de como funciona esta cobrança. Eu sei que ela existe, se caso a área tiver pontos de auditoria isso vai aparecer em reuniões da diretoria, mas como ela é feita eu não tenho conhecimento*".

Das práticas apresentadas no domínio D6, conclui-se que apenas duas são utilizadas pela empresa: (i) análise crítica reflete de fato o que ocorreu, fornecendo evidências aos *stakeholders*; (ii) os resultados da análise crítica são relatados à direção, proporcionam a transparência das informações. Constatou-se também que a análise crítica não é iniciada pela direção e sim pelos gestores e funcionários das áreas.

Por fim, questionou-se aos gestores quanto à contribuição destas práticas (análise crítica reflete de fato o que ocorreu; os resultados das análises críticas são relatados à direção) para a conformidade.

De acordo com a coordenadora fiscal "*[...] estas práticas são uma forma de garantir que o que estamos fazendo está dentro das normas e de forma transparente. [...] cumprir a legislação e ter uma revisão de uma auditoria independente isso garante que não há sonegação e contribui para reduzir os riscos*".

A coordenadora contábil explica também como estas práticas contribuem para a conformidade: "*A análise crítica dos registros, relatórios, processos e das*

demonstrações são de grande importância para validação das informações geradas pela contabilidade, através dessas análises são sinalizadas e identificados erros que são trabalhados e corrigidos para que as informações finais sejam divulgadas em conformidade com as exigências dos órgãos reguladores".

Neste sentido o gerente financeiro afirma que a visão trazida por uma empresa independente contribui para a melhoria dos processos e sua conformidade. Ele explica: "*[...] quando a gente tá envolvido no processo muitas vezes não se vê as falhas, se está tão envolvido, muitas vezes foi até a pessoa que criou o processo e pode não se ter uma visão imparcial daquilo [...] Eu acho que isso contribui muito, ter um olhar da auditoria independente que faz este processo em clientes grandes, ela traz um benchmarking de mercado também. Eu acho que ela ajuda muito a gente a melhor os processos através de sugestões de melhorias, se tem um feedback*".

A grande contribuição, na percepção da coordenadora de custos/planejamento é a garantia da auditoria externa. Segundo essa gestora: "*Eu acho que a prática mais forte que nós temos é a auditoria externa, por ser uma empresa de capital aberto nós temos que seguir leis da CVM, do IFRS [...] Eu acho que essa é a maior garantia que a gente tem, quando a auditoria externa dá o aval eles se comprometem também com a informação divulgada. Eu acho que o cumprimento das obrigações legais ajuda na conformidade*".

Na percepção dos gestores de TI estas práticas contribuem, segundo a gerente de TI: *"Eu acho que estas práticas contribuem sim, principalmente na redução do risco pois a auditoria externa valida as informações e também checa os processos internos*". O supervisor de TI complementa: *"a área de TI é uma área que muda muito e se você não for atrás de novas tecnologias de segurança você pode ficar vulnerável, desta forma eu acho que ela contribui".*

Para o gerente de controladoria essas práticas contribuem para a conformidade da seguinte forma: "*contribui muito para garantir as conformidades e mitigar os riscos, a gente tem um processo que está bem desenhado, se tem o processo interno e, depois um processo de validação que é feito pela auditoria externa. Eu entendo que isso dá a segurança para que os clientes externos, stakeholders, acionistas, eles confiem no número da companhia. Eu acho que é processo importante, é um processo que precisa estar sempre sendo aperfeiçoado e que sim, garantem a conformidade. Acho que possíveis falhas ou erros que podem*

acontecer, mas não são coisas que comprometam o negócio, a operação ou mesmo a tomada de decisão".

A seguir abordam-se as práticas relacionadas ao domínio D7.

- **7. Conformidade com as políticas e procedimentos de segurança da informação (D7):**

7.1)	Esta questão verifica como os gestores identificam as causas quando há qualquer não conformidade, evidenciando as diferenças e semelhanças, por meio do comportamento ético e moral. Conceitos: autenticidade; comparabilidade; ética.

Constatou-se que os gestores de contabilidade, fiscal, custos/planejamento, controladoria, financeiro afirmam que conseguem identificar as causas de não conformidade. Porém a gerente de TI acredita que eles têm dificuldades de identifica-las.

A coordenadora contábil explica como faz essa identificação: "*Nós implantamos o sistema este ano e alguns processos não estão, ainda, totalmente alinhados, são revisados e ajustados manualmente. Por exemplo, o estoque: o processo de estoque está com problemas que não conseguimos corrigir automaticamente, o ajuste é feito manual. Outro exemplo é o imobilizado que na mudança de sistema algumas informações entre contas contábeis deram entrada no SAP incorretamente então há ajustes manuais também*".

Na área fiscal, a coordenadora afirma que a análise é feita principalmente quanto aos impostos apurados, ela relata: "*faço uma análise principalmente quanto aos impostos, e não tem um caminho específico*". O mesmo ocorre na área de custos/planejamento, a coordenadora explica: "*Na minha área eu acho que eu consigo identificar, pode até não ser de forma imediata, mas a gente vai atrás e identifica. Muitas vezes quando se faz essa identificação a origem da não conformidade está em outro setor [...]*".

Essas percepções são corroboradas pelo gerente das áreas de contabilidade, fiscal e custos/planejamento. Neste sentido, o gerente de controladoria afirma: "[...] *acho que conseguem identificar, enfim eu falo da minha própria área, a gente tem possíveis problemas que possam acontecer, possíveis problemas de conciliação de*

alguns números que nós controlamos, eu acho que sim que isso está na mão do gestor sim. Eu acho que os gestores ou sua própria equipe conseguem identificar e aí vai da forma como cada um trata isso [...]".

Ainda segundo o gerente de controladoria, ele explica como ele efetua a identificação de não conformidade: "*[...] Como controller, a gente consegue identifica muito mais processos não conformes, correções de rotas que precisam ser feitas, a gente consegue identificar através dos números, através dos indicadores, obviamente que não a nível de 100%. Os indicadores são importantes sem dúvida, tanto para a correção de rumo para o atingimento de metas, bem como para saber se o processo está funcionando da maneira correta. Obviamente a gente não se atrela somente a isso, a gente tem que olhar o processo como um todo. Eu acho que este é o caminho [...]*".

Já o gerente financeiro acrescenta o sistema como um facilitador na identificação de não conformidade, ele relata: *"[...] Na maioria dos casos sim [identificação da não conformidade], até por que o sistema possui uma boa rastreabilidade. Então se tiver um pouco de entendimento do sistema e boa vontade para procurar é bem fácil".*

Na área de TI, o supervisor explica como identifica as causas quando há qualquer não conformidade: "*[...] vou te responder dando um exemplo: um usuário na rede que por ventura o gestor não abriu o chamado, não fez o formulário eletrônico. Neste momento que eu vejo que existe um usuário que não tem o chamado, eu identifiquei uma falha [...] Eu tenho que instruir a minha equipe para que ela não crie usuário sem chamado e comunicar o gestor sobre o procedimento correto que deve ser adotado [...]*".

No entanto a gerente de TI afirma que os gestores têm dificuldade de identificar as causas de não conformidade. Ela explica: "*Eu acho que eles têm dificuldades para identificar as causas. Dependendo da não conformidade eles conseguem identificar de maneira fácil, mas tem não conformidades que eles têm dificuldades de identificar".* A gestora justifica a sua resposta da seguinte forma: "[...] *nós temos dentro do SAP hoje um nível de automação muito grande lá na produção, hoje se sabe que há falhas em relação ao saldo de alguns componentes do produto [...] isso acaba atrapalhando a automação, porque onde eu tenho falta de saldo a ferramenta automática já não funciona mais, alguém tem que entrar e identificar o porquê faltou saldo. Essa identificação no sistema, de falta de saldo, o porquê está*

ocorrendo isso, o motivo, os gestores tem muita dificuldade em identificar isso, e isso é uma não conformidade [...] têm causas que não se consegue identificar a causa, pois podem ser várias causas que justificam essa falha. Outras falhas mais simples eu acho que eles identificam facilmente".

Quanto à área de TI a gerente afirma que consegue efetuar a identificação de não conformidades por meio de indicadores, ela relata como isso é feito: *"[...] eu tenho os meus indicadores dentro da TI, quando um desses indicadores não for atingido, a gente consegue identificar a causa. Por exemplo, eu tenho um indicador que visualiza se os meus links estão disponíveis, essa meta é de 99% e, se não atingiu a meta, a gente volta no histórico e no registro e se chega ao motivo que não consegui atingir o indicador [...]*".

Questionou-se também aos gestores quanto às não conformidades do tipo comportamental e, todos responderam que conseguem identificar este tipo de não conformidade. Neste sentido a coordenadora fiscal afirma: "*Se for comportamental a gente chama o funcionário para uma conversa, utilizando o relatório do TI como suporte. Quanto aos processos, o treinamento é a melhor opção, treinar o pessoal, informando o correto para que a falha não ocorra mais e, é claro efetuar o devido ajuste".*

A coordenadora de custos/planejamento também relata sobre a rastreabilidade do sistema, porém atribui a essa rastreabilidade a insegurança do usuário: "*[...] a gente consegue identificar em função da insegurança do funcionário. Eu percebo que tem funcionários ainda muito inseguros, por exemplo, com o processo, o novo sistema. Às vezes eu vejo o usuário comentar que não vai mexer porque não sabe o que vai acontecer. Durante muito tempo nós tivemos com a presença de consultores externos, então tu libertar as pessoas desse convívio com os consultores externos causa a insegurança. Eu acho que em muitos casos esse comportamento de insegurança do funcionário sobrepõe o conhecimento técnico dele. No caso do funcionário fazer algo indevido, nós temos tudo mapeado, fica registrado no sistema e, é por isso que eu digo as pessoas se bloqueiam muito para não fazer a coisa errada e acabam sendo inseguras".*

A rastreabilidade do sistema também é comentada pelo gerente financeiro: "*[...] tudo fica registrado no sistema e se tem rastreabilidade como eu já disse. Se houver uma transação que não esteja conforme se consegue visualizar isso muito fácil no sistema, através do acesso do usuário*".

Além da rastreabilidade o supervisor de TI afirma que é necessário estar atento ao comportamento do usuário: *"eu sempre procuro estar atento ao comportamento das pessoas [...] fica tudo registrado no sistema, temos diversos relatórios, por exemplo: os de acesso a internet, acesso da rede, conversas pelo Skype é possível ter acesso as conversas dos funcionários. Inclusive tivemos recentemente um caso de demissão, o uso indevido do recurso de TI. Essa pessoa estava acessando uma rede que não era para ter acesso ela conseguiu acesso a senha, a gente descobriu e o funcionário foi demitido*". Isto é corroborado pela gerente de TI: "*[...] a não conformidade comportamental eu também consigo, e já identifiquei isso e tive que tomar ações disciplinares, quanto a isso [...]*".

Na opinião do gerente de controladoria os gestores identificam as causas de não conformidade do tipo comportamental por estarem envolvidos no processo, porém afirma não ter presenciado esse tipo de não conformidade. Ele explica: "*[...] eu acho que depende de cada gestor [...] particularmente aqui eu ainda não vivenciei isso, não participei, mas tenho o conhecimento que sim, em algumas áreas isso foi identificado pelo gestor e tratado. Eu acho que é um processo que acontece e que está na mão do gestor e ele tem como identificar, os nossos gestores são gestores operacionais estão dentro do processo, então eles tem condições para isso*".

7.2)	Esta questão verifica como os gestores implementam ações corretivas após a detecção da não conformidade. Se isto ocorre de forma mais completa possível, sem omissão de algum fato relevante, atuando com responsabilidade pelas ações próprias ou dos outros. Conceitos: integridade; integridade; legitimidade.

Verificou-se que os gestores efetuam as ações corretivas após a detecção de não conformidade por meio de manuais, desenhos do processo, chamados via TI e conversas com os funcionários.

De acordo com o gerente financeiro: "*[...] se tem pouca não conformidade dentro do sistema [...] Eu acho que o principal é ir atrás do processo, verificar o manual VSM de processo de cada área, a gente tem esse material, dá para consultá-lo e comparar com o que foi feito [...]*".

A coordenadora de custos/planejamento explica como efetua as ações corretivas: "*A gente mapeia todo o processo para ver a origem da não conformidade*

e reunimos todos os envolvidos, porque às vezes isso ocorre por falta de entendimento do processo e não pelo desenho do processo [...] então mapeia o processo, reúne todas as áreas envolvidas e revisa processo [...] Eu vejo que a parte comportamental é mais relacionada à conversa mesmo com a pessoa envolvida".

Na contabilidade, a ação de implementação de ações corretivas ocorre da seguinte forma: "*Quando se identifica um problema, a contabilidade abre um chamado para a área de TI nos auxiliar quando se tratar de problema de sistema. Quando forem problemas de lançamentos, por exemplo: o registro ocorreu em conta errada, nós vamos até o departamento que deu entrada da informação e damos a devida orientação. O ajuste ocorre no sistema SAP de forma manual*". Já a área de TI envolve a área de RH quanto aos aspectos comportamentais, a gerente de TI explica: "*Eu sempre procuro envolver o RH no caso comportamental e, no caso não comportamental eu verifico os acessos, os logs, consigo resgatar o histórico de algo não conforme, no caso dos indicadores*".

7.3)	Esta questão verifica se as ações corretivas tomadas são capazes de predizer resultados futuros, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever. Conceitos: conformidade; preditiva; legitimidade.

Constatou-se que os gestores das áreas fiscal, custos/planejamento, financeiro e TI acreditam que as ações corretivas são capazes de predizer resultados futuros, fornecendo evidências aos *stakeholders.*

Sendo assim, a coordenadora fiscal afirma: "*Efetuando a análise crítica e tomando as ações corretivas vai efetuar o processo correto, você vai evitar qualquer auto de infração, vai evitar problemas para a companhia. Um problema tributário pode gerar valores financeiros e também prejudicar a imagem da empresa no mercado".*

Com esta mesma percepção, a coordenadora de custos/planejamento relata: "*[...] se há muitas ressalvas ou não, no relatório da auditoria é uma comunicação com os stakeholders. Isso vai transmitir a confiança que os investidores. Se houver muitas ressalvas pode haver problemas no processo ou até mesmo falhas e, se tudo correr bem eu acho que eles pensam assim, que tudo está*

dentro da legislação, os processos estão corretos. Eu acho que sim, que consegue predizer".

Neste sentido, o gerente financeiro acrescenta: "*Elas evitam que se tenham problemas nos resultados futuros. Existe um processo de análises para garantir a qualidade da informação que está publicada ao mercado, eu acho que o stakeholders conseguem perceber, por que eles têm uma segurança de que está sendo feito corretamente, pois se tem uma auditoria externa que sustenta isso também*".

A gerente de TI também explica como a análise crítica pode predizer resultados futuros: "*[...] se algum dado não foi imputado pelo usuário para dentro do sistema isso vai ter um reflexo lá na frente. Eu acho que os stakeholders têm a visão que temos uma auditoria externa a qual significa que estamos garantindo que os procedimentos internos estão sendo seguidos, e que isso garante a integridade da informação divulgada*".

O supervisor de TI corrobora com a percepção dos demais gestores: *"[...] são efetuadas ações para corrigir os pontos identificados [...] reduz a probabilidade de acontecer novamente, mitiga o risco".* Em contrapartida, a coordenadora contábil acredita que as análises críticas não conseguem predizer resultados futuros: "*Eu acho que não por que quando a gente percebe a não conformidade nós já corrigimos [...] então elimina-se o problema e, desta forma os stakeholders não conseguem perceber*".

Já o gerente de controladoria, não deixou claro se as análises críticas podem predizer resultados futuros: "*Eu acho que é complicado, predizer ou antever alguma coisa em termos de resultados futuros [...] Eu acho que pode acontecer se for algo muito grave que afete o futuro da companhia, acho que depende muito da gravidade da não conformidade. As ações de gestão levam a ter uma visão de curto, médio ou longo prazo do que propriamente as conformidades ou não conformidades*".

7.4)	Esta questão verifica se os resultados das análises críticas e das ações corretivas pelos gestores são registradas e mantidas mediante informações íntegras e tempestivas de acordo com as normas reguladoras internas e externas. Conceitos: disponibilidade; oportunidade; conformidade.

Verificou-se que os resultados das análises críticas e das ações corretivas ficam registrados em pastas localizadas na rede de cada área específica, em manuais de processos (VSM), bem como no próprio sistema SAP através dos registros feitos.

Conforme a coordenadora fiscal: *"a gente deixa uma evidência dentro da nossa pasta que fica na rede. No mês que ocorreu alguma não conformidade a gente deixa uma planilha suporte dentro da pasta, para que depois de alguns anos a gente consiga saber o porquê e como se fez determinada alteração".*

Quanto ao registro por meio do sistema, a coordenadora contábil explica: "*Quando efetuamos as correções, os registros não se apagam, ou seja, consta no sistema o registro anterior e o posterior ao ajuste. Uma vez corrigidas elas estão prontas para o uso da informação*".

As percepções das gestoras contábil e fiscal são corroboradas pela coordenadora de custos/planejamento: *"Elas ficam arquivadas em nossas pastas na rede e tudo o que for de sistema fica registrado lá dentro do SAP". Neste sentido, a* gerente de TI também responde: *"Fica tudo registrado em pastas e no sistema".*

Já o gerente financeiro acrescenta outro exemplo de registro das ações corretivas: "*são registradas e mantidas nos manuais de processos VSM*".

O supervisor de TI sintetiza o processo de registro destas análises críticas: "*Elas são registradas e mantidas no sistema. Qualquer pessoa que quiser buscar os pontos de auditorias tem acesso a estas informações, elas estão disponíveis, tempestivas e integras sim. Fazemos também o backup deste sistema, ela uma vez por semana em função de limitações do sistema*".

No entanto, o gerente de controladoria não tem conhecimento sobre como estas análises críticas são registradas e mantidas. Ele explica: "*[...] na parte de processos, eu não sei se fica registrado, eu acho que não. Dependendo do processo da gravidade do processo pode ser que tenha algum registro, mas eu acho que isso está muito mais no dia-a-dia, correção. Pode ser que um e-mail seja o registro, vai depender muito do gestor, tem aqueles que guardam tudo e tem outros que já não guardam, então vai depender muito do modus operandi de cada um*".

7.5)	Esta questão verifica se os gestores relatam os resultados para as pessoas que estão efetuando a análise crítica independente, identificando as diferenças e semelhanças das informações permitindo um clima de confiança. Conceitos: confiabilidade; comparabilidade; transparência.

Constatou-se que os gestores não relatam os resultados para a as pessoas que estão efetuando a análise crítica independente, no caso, a auditoria externa. Os gestores argumentaram que quando um registro de não conformidade ocorre, este fica registrado no sistema, desta forma não há necessidade de relatar à auditoria.

Neste sentido, o gerente financeiro explica: "*[...] quando a gente detecta a não conformidade ela tem que ser consertada dentro do sistema. Nós fazemos os ajustes e isso fica registrado no sistema, a auditoria externa consegue rastrear a informação do início ao fim da operação*".

O mesmo é relatado pela coordenadora contábil: "*[...] quando há um lançamento errado, nós corrigimos este lançamento e a auditoria externa tem condições para visualizar determinada alteração, pois eles têm toda a base. Estas alterações constam no razão das contas contábeis, não tem o porquê informarmos a auditoria externa eles conseguem visualizá-los*". A coordenadora fiscal também relata: *"as questões de não conformidade foram arrumadas e não tiveram impacto financeiro para a empresa".*

A gerente de TI compartilha também deste pensamento: "*[...] a auditoria externa tem acesso a todas as informações, inclusões, alterações e exclusões eles iriam evidenciar isso, caso tivesse ocorrido*".

A coordenadora de custos/planejamento afirma que o relato de não conformidade parte na maioria das vezes da auditoria externa para o gestor, ela relata: "*[...] eu acho que é o contrário. Se a auditoria aponta alguma coisa aí ela vai no gestor, mas partir do gestor para a auditoria eu acho que não [...]".*

Já o gerente de controladoria aborda que a auditoria externa ainda é vista como um órgão fiscalizador, mas mesmo assim ele acredita que seus gestores relatam os resultados a auditoria externa. Ele explica: "*Não sei se todos [relatam]. Por que a auditoria ela ainda ela é vista, não no viés de alguém que vem ajudar a companhia, mas muito mais para fazer uma inspeção. Dentro da área administrativa eu acredito que sim, até por ser uma orientação de passar as informações, de*

comunicar, de inclusive pedir ajuda para a área de auditoria, mas eu não sei se isso acontece em todas as áreas".

Das práticas apresentadas no domínio D7, conclui-se que a empresa utiliza-se das práticas: (i) os gestores implementam as ações corretivas após a detecção da não conformidade e; (ii) os resultados das análises críticas e das ações corretivas são registrados e mantidos de forma íntegra.

Por fim, questionou-se aos gestores quanto à contribuição destas práticas (implementação das ações corretivas pelos gestores; registro e manutenção dos resultados das análises críticas de forma íntegra) para a conformidade.

Neste sentido o gerente financeiro afirma: "[...] *eu acho que elas contribuem na medida em que todas as informações divulgadas ao mercado estão alinhadas, não só com as normas contábeis, mas as normas de compliance também. Esta é a grande garantia. É a informação estar íntegra, tem um terceiro validando a informação prestada. A própria questão da empresa estar no nível 2 da governança corporativa já possibilita essa integridade".*

A coordenadora de contabilidade também relata: "*A importância da segurança das senhas de acesso é de responsabilidade dos usuários e deve ser obedecida para garantir a segurança das informações. As correções e ajustes das informações são necessários para obtermos os resultados em conformidade com situação real da empresa*".

Esta percepção é corroborada pela gerente de TI: "*Eu acho que o cumprimento destas práticas e o melhoramento delas também contribui, para mitigar o risco de segurança*". O supervisor de TI complementa: *"[...] Eu acho que essas práticas só beneficiam a empresa [...]*".

A coordenadora de custos/planejamento também explica como estas práticas contribuem para a conformidade: "*[...] eu acho que ter a segurança da auditoria independente, no sentido dela apontar ou não alguma falha, que são as ressalvas, e o próprio vinculo de confiança com a equipe de trabalho, eu acho que isso tudo contribui*" e, segundo a coordenadora fiscal: "[*...] desta forma a gente evita de expor a empresa, de causar algum risco de imagem e também financeiro para a empresa*".

Sob a ótica do gerente de controladoria estas práticas "*contribuem porque elas trazem melhorias ao processo, elas fazem com que os processos sejam criticados em cada tempo, trazem as correções de rotas que são necessárias, e qualquer problema grave que se possa ter são identificados e consequentemente*

corrigidos, então eu acho que contribuem por isso, por garantir a acuracidade da informação, por garantir que os processos efetivamente aconteçam isso internamente e externamente, pois se tem o processo de auditoria validando tudo isso".

A seguir apresentam-se as práticas evidenciadas no domínio D8.

- **8. Análise crítica da conformidade técnica (D8):**

8.1)	Esta questão identifica se a verificação de conformidade técnica possui apoio de uma ferramenta automática para a interpretação do especialista técnico. De forma a proporcionar um consenso, interpretação e avaliação de regulamentos para limitar as perdas. Conceitos: confiabilidade; verificabilidade; avaliação de risco.

Identificou-se que os gestores da contabilidade e controladoria consideram o próprio SAP uma ferramenta de apoio para ajudar na interpretação do especialista técnico. Os gestores das áreas fiscal e TI possuem outras ferramentas específicas. Já o gerente financeiro e a coordenadora de custos/planejamento acreditam que o SAP não proporciona a interpretação das informações, isso depende do especialista técnico.

Conforme a coordenadora contábil "*Eu considero que o próprio sistema SAP é uma ferramenta que ajuda nossa interpretação, pois existe no sistema vários relatórios gerenciais e transações que auxiliam na interpretação do especialista. Esses relatórios gerenciais e as transações disponíveis no SAP permitem aos gestores um monitoramento em tempo real dos processos que estão acontecendo na empresa, auxiliando no processo de tomada de decisão desses especialistas*".

Alinhado a esta percepção, o gerente de controladoria afirma: "*O próprio sistema o SAP nos dá muitas das informações que a gente precisa, de relatórios, o sistema auxilia o usuário nas análises. Alguns relatórios já vêm prontos, ai vai muito da atitude e do conhecimento do usuário em fazer este trabalho [...] o SAP hoje é uma ferramenta muito grande e poderosa por estar tudo integrado, todas as informações vem deste sistema [...]*".

Identificou-se também que há ferramentas específicas que ajudam na interpretação do especialista técnico nas áreas fiscal e TI. A coordenadora fiscal

explica: "*Hoje temos uma ferramenta que a gente usa no recebimento fiscal, ela busca pelo xml que o fornecedor gerou para importar os dados da nota [...]a ferramenta valida com as informações da nossa ordem de compra. Se tiver alguma diferença é verificado o que está errado, se é o fornecedor ou a nossa ordem de compra. É uma conferência que a ferramenta faz, ela ajuda a validar [...]*".

A gerente de TI exemplifica também algumas ferramentas de apoio na interpretação técnica: "*Hoje na TI nós temos um sistema de chamados, quando esse chamado é concluído pelo funcionário de TI ele é avaliado pelo usuário que efetuou o chamado, eu acho que isso seria uma ferramenta de avaliação do nosso funcionário de TI. Hoje nós temos um suporte técnico do SAP, que são X horas mensais e que os meus colaboradores podem consultar estes técnicos do SAP, eu acho que isso também é uma ferramenta que nos auxilia na interpretação. O RH possui também uma ferramenta que auxilia na avaliação de competências".*

Outros exemplos são citados pelo supervisor de TI: "*[...] eu tenho um relatório que roda semanalmente e me envia a informação de quem acessou o Datacenter, isso é automático que me ajuda na interpretação. Eu verifico no relatório se alguém que não deveria ter acesso conseguiu acessar o Datacenter. Em muitos casos a interpretação ocorre pelos relatórios existentes do sistema, a gente procura automatizar os sistemas para que ele nos auxilie a evitar problemas*".

Em contrapartida, o gerente financeiro afirma que não há uma ferramenta que ajude na interpretação do especialista: *"Não temos uma ferramenta específica. Podemos nos apoiar no SAP, ele nos dá a informação, mas não ajuda na interpretação [...]".* Esta percepção é compartilhada pela coordenadora de custos/planejamento: *"[...] eu acho que ele [SAP] ajuda é na visualização do processo, mas eu acho ele ajuda mais na entrega dos dados, pois a interpretação é do usuário, do conhecimento técnico do usuário*".

8.2)	Esta questão identifica como ocorrem os testes de invasão ou avaliações de vulnerabilidades e se estes são planejados, documentados e repetidos quando incertezas estiverem envolvidas. De forma a prevenir riscos, monitorando e supervisionando continuamente os processos operacionais. Conceitos: autenticidade; prudência ou conservadorismo; risco.

Constatou-se que todos os gestores não sabem como são efetuados os testes de invasão ou avaliações de vulnerabilidades, exceto a área de TI que possui este conhecimento.

O gerente de controladoria sintetiza as respostas dos demais gestores: "*Eu não sei como é este processo, eu imagino que tenha pela importância do produto, pela importância da companhia, mas eu não tenho o conhecimento de como é este processo*".

No entanto, a gerente de TI explica como ocorre este procedimento: "*Hoje nós temos um firewall ativado, existem várias regras que bloqueiam as entradas indevidas e invasões, isso está sempre constante e em operação [...] nós não temos casos de invasão e vulnerabilidades, temos vários sites da internet que são bloqueados, justamente para limitar o acesso e reduzir essas vulnerabilidades*".

O supervisor de TI complementa: "*nós acessamos um relatório que informa se alguém tentou acessar as nossas informações. A verificação deste relatório é feita via um painel que fica na área de TI, nós visualizamos isso diariamente. Neste painel contem as verificações de ameaças que podem tentar entrar na nossa rede, essa informação fica online diariamente, por isso não realizamos um teste específico*. *Essas informações ficam registradas no próprio equipamento que coleta as informações, são feitos backups também*".

8.3)	Esta questão identifica se a verificação de conformidade técnica somente é executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas. De forma a fornecer evidências aos *stakeholders* sobre o atendimento de uma expectativa. Conceitos: confidencialidade; integridade; legitimidade.

Identificou-se que as respostas dos gestores de contabilidade, fiscal, controladoria e financeiro convergiram. Estes gestores acreditam que a verificação técnica é executada por todas as pessoas competentes envolvidas no processo, independente de serem gestores.

Neste sentido, a coordenadora de contabilidade relata sobre a formação e competências de seus funcionários: "*Hoje todos os analistas contábeis são formados em ciências contábeis e todos eles validam as informações*". O mesmo ocorre na

área fiscal: “*As pessoas do recebimento fiscal e elas são treinadas para usar estas ferramentas*”.

Alinhado a estas percepções, o gerente de controladoria afirma: “*Nas áreas de planejamento, contabilidade e fiscal, todos os processos desembocam nestas áreas, então hoje nós temos pessoas especialistas para fazer este tipo de trabalho, através da validação e análise*”.

Corroborando com os demais gestores, o gerente financeiro explica: “*Eu acho que ocorre por todos. Até a própria contabilidade faz isso, por que se a gente tem algum erro vai aparecer na contabilidade, quando eles conciliar as contas, quando efetuarem as demonstrações contábeis. Eu digo que isso passa também muito pela contabilidade, que fica a critério de um especialista técnico e não de uma ferramenta*”.

Sob a ótica da coordenadora de custos/planejamento essa verificação ocorre em nível gerencial: “*Eu acho que é sob a supervisão, de nível mais gerencial e não operacional. Eu acho que isso faz parte da companhia mesmo, uma questão hierárquica em solicitar o aval do gestor*”. Esta percepção é compartilhada pelos gestores de TI. Segundo a gerente de TI: “*[...] essa verificação ocorre por mim e pelo supervisor de TI*”. Isto é corroborado pelo supervisor de TI: “*[...] O acompanhamento é feito pela gestão da área, não são os funcionários que executam*”.

Das práticas apresentadas no domínio D8, conclui-se que a empresa utiliza-se das práticas: (i) testes de invasão e vulnerabilidades; (ii) verificação de conformidade técnica somente é executada por pessoas competentes ou sob a supervisão dela.

Por fim, questionou-se aos gestores quanto à contribuição destas práticas (testes de invasão e vulnerabilidades; verificação da conformidade técnica somente por pessoas competentes ou sob supervisão delas) para a conformidade.

A coordenadora contábil afirma: “*Uma boa ferramenta de gestão contribui para a tomada de decisão, auxilia na gestão da empresa com informações integras, seguras e em tempo real. A qualidade das informações também é garantida com profissionais qualificados no quadro funcional da empresa. Essas práticas mantêm e contribuem com a conformidade das informações*”.

Sob a ótica da coordenadora fiscal: *“O controle de invasão assegura que não é qualquer informação que se traz para dentro da empresa, o bloqueio de*

determinados sites. As pessoas qualificadas e treinadas minimizam o risco de imputar uma informação errada".

Neste sentido, o gerente de controladoria afirma: "*Contribuem no sentido de ter especialistas tratando [...] eles garantem um nível de acuracidade muito bom, principalmente porque parte disso não tem um acesso humano, porque está dentro do SAP o próprio sistema faz. Cabe aos colaboradores analisar e interpretar [...] então eu acho que contribui no momento que se limitam as vulnerabilidades no sentido de não ter sistemas paralelos com integração de dados, com troca de interface, hoje isso tudo está centralizado dentro do sistema e acho que isso traz um ponto muito importante para a conformidade*".

Alinhada a estas percepções a gerente de TI explica: "*Eu acho que elas contribuem. A gente mantém a segurança da informação em função dos acessos, da confiança de ter desse firewall. Eu acho que essas práticas ajudam a mitigar o risco de segurança*". O supervisor de TI complementa, afirmando que estas práticas "*mantém a integridade e a segurança das informações*".

Já a coordenadora de custos/planejamento acredita que estas práticas devem ser melhoradas. Segundo esta gestora: "*Eu acho que o próprio sistema deveria fazer a análise crítica e não a pessoa. Eu acho que essas práticas tem que ser mais aplicadas no sentido do sistema ajudar na interpretação".* Isto também é percebido pelo gerente financeiro: "*Como nós não temos uma ferramenta, eu acho que vai muito da percepção da contabilidade garantir que as informações estejam de acordo com os padrões contábeis atuais, então vai muito da interpretação dos responsáveis pela contabilidade*".

Apresenta-se no capítulo a seguir a análise documental para corroborar os relatos dos entrevistados.

4.3 ANÁLISE DOCUMENTAL

Essa análise documental tem como objetivo verificar as evidências documentais a fim de corroborar com as entrevistas executadas. Ela compõe-se por analisar os seguintes documentos: (i) Política de segurança da informação; (ii) Políticas de tecnologia da informação; (iii) Política corporativa de segurança SAP;

(iv) Manual de conduta sobre uso, divulgação e manutenção de sigilo acerca de informações; (v) Código de conduta.

A seguir apresentam-se os objetivos destes documentos e, na sequência destacam-se as palavras-chave contidas.

- **Política de segurança da informação (PSI):** essa política tem como objetivo estabelecer princípios e diretrizes para a proteção dos ativos de informação e a responsabilidade dos usuários;

- **Política de tecnologia da informação (PTI):** essa política tem como objetivo assegurar que os recursos da tecnologia da informação sejam utilizados de maneira ponderada e adequada aos propósitos de negócio da empresa;

- **Política corporativa de segurança SAP (PSAP):** essa política tem como objetivo definir como as informações e sistema SAP deve ser gerido e utilizado, além das responsabilidades dos membros das organizações;

- **Manual de conduta sobre uso, divulgação e manutenção de sigilo acerca de informações (MC):** esse manual baseia-se nas normas expedidas pela CVM, tem como objetivo estabelecer padrões de conduta a serem observados pelos *stakeholders* e funcionários referente ao conhecimento de informações de ato ou fato relevante sobre a companhia;

- **Código de conduta (CC):** esse código de conduta tem como objetivo emitir um conjunto de valores que reflete os padrões éticos e morais, buscando a credibilidade e preservar a imagem da empresa no curto e longo prazos, junto aos mercados de atuação;

Analisou-se também os Relatórios dos Auditores Independentes sobre as Demonstrações Financeiras - 2015 e 2014 (RAI) e o Relatório sobre a Revisão de Informações Trimestrais - 2016. A seguir apresentam-se os objetivos destes documentos.

- **Relatório dos auditores independentes sobre as demonstrações financeiras 2015 e 2014 (RAI):** tem como objetivo emitir um parecer sobre a adequação das demonstrações financeiras e aplicações de recursos da entidade auditada em consoante as práticas adotadas no Brasil e de acordo com as normas IFRS.

- **Relatório sobre a revisão de informações trimestrais - 2016 (RIT):** tem como objetivo revisar as informações contábeis trimestralmente, esta revisão consiste na realização de indagações, principalmente às pessoas responsáveis pelos assuntos financeiros e contábeis e procedimentos adotados.

Os relatórios analisados não possuem ressalvas pela auditoria independente, isto sugere que as demonstrações financeiras estão em conformidade com as práticas adotadas no Brasil e de acordo com as normas internacionais IFRS.

Analisando-se os documentos da empresa em estudo conclui-se que ela possui as políticas de segurança da informação documentadas. Verificou-se que estas políticas estão disponíveis na intranet da empresa, porém constatou-se pelos relatos dos gestores, exceto os de TI, que essas políticas são pouco divulgadas. Por fim, constatou-se também que a empresa não possui ressalvas da auditoria independente nas demonstrações financeiras evidenciadas no período analisado.

Na sequência, identificam-se as práticas utilizadas e a contribuição destas para a conformidade.

4.4 CONTRIBUIÇÃO PARA A CONFORMIDADE

De acordo com as entrevistas e análise documental constatou-se que as práticas evidenciadas na Tabela 11 são utilizadas pela empresa em estudo e contribuem para a conformidade.

Tabela 11 – Práticas utilizadas pela empresa “X”

Domínio	**Questão**
D1	1.1
D2	2.1
	2.2
	2.4
	2.5
	2.6
	2.7
	2.10
	2.11
D3	3.2
	3.3
	3.4
	3.5
	3.6
	3.7
	3.8
	3.9
	3.10
D4	4.1
D5	5.1
	5.2
D6	6.4
	6.5
D7	7.2
	7.4
D8	8.2
	8.3

Fonte: Dados da pesquisa.

Verifica-se na Tabela 11 as questões que envolvem as práticas de segurança da informação contábil. Constata-se que das 41 práticas, a empresa utiliza-se de 27. Apresenta-se no Quadro 24 a contribuição destas práticas por meio das palavras-chave relatadas pelos gestores.

Quadro 14 – Contribuição das práticas para a conformidade

CONTÁBIL	FISCAL	CUSTOS	CONTROL.	FINANC.	TI (G)	TI (S)
acesso	acesso	acesso	acesso	ágil	acessos	conformidade
análise crítica	auditoria	armazenada	acuracidade	alinhadas	assina	conhecimento
arquivados	independente	auditoria	alterações	assinaturas	*backup*	criptografia
auditoria	bloqueio	independente	atribuições	digitais	checa	disponibilidade
independente	conformidade	aval	auditoria	auditoria	confiança	governança
checklist	conhecimento	barreiras	*backup*	independente	confidencialidade	informação
conciliação	contábil	comprometem	centralizado	autorização	conformidade	integridade
confiáveis	controle	confiabilidade	confiabilidade	*benchmarking*	contábil	mitigar os riscos
conformidade	cumprir	confiança	confiança	*compliance*	contratos	responsabilidade
consistente	divergência	conformidade	conformidade	conformidade	criptografia	segurança da
controles	evitar boatos	controle	documentos	contratos	cumprimento	informação
demonstrações	evitar exposição	cumprimento	equipe	divulgadas	disponível	sem lesar
disponíveis	fiscal	CVM	especialista	embasamento	*firewall*	sem manipular
exigências	fontes	disponível	identificação	técnico	informações	tecnologia
informação	conhecidas	divulgar	informação	evitar risco	integridade	usuários
integridade	impedir	equipe	integração	*feedback*	melhorar	vulnerável
legislação	informações	IFRS	interpretação	imparcialidade	processos	
locais seguros	legislação	informação	limita as perdas	informação	mitiga o risco	
normas	expor a empresa	legislação	melhoria	integridade	processos	
internacionais	normas	limitar perdas	processo	licença	regras	
obediência	mitiga o risco	melhorar	mitiga os riscos	melhoria	responsabilidade	
órgãos	preventiva	processos	processo	processo	seguir	
reguladores	processo	obrigações	protege	mitigar riscos	segurança da	
práticas	profissionais	legais	responsabilidade	monitoramento	informação	
contábeis	qualificados	registro	restrito	normas	termo	
processos	mitiga o risco	respaldo	sistema	contábeis	valida	
profissionais	regras	ressalvas	*stakeholders*	padrão	vazamento	
qualificados	responsabilidade	validação	suporte	processo		
protegidos	risco de imagem		treinadas	rastreabilidade		
qualidade das	risco financeiro		validação	responsabilidade		
informações	sites		vital	seguro		
responsabilidade	sonegação		vulnerabilidades	utilização		
segurança da	transparente			validação		
informação	treinamento					
senhas	vazamento					
tempestividade	vírus					
tomada de						
decisão						
validação						

Fonte: Dados da pesquisa.

Destacam-se no Quadro 14 as seguintes palavras-chave: informação, acesso, conformidade, melhoria de processo, processo, controle, cumprimento, legislação, auditoria independente, confiança, disponível, integridade, responsabilidade, validação, segurança da informação, mitigar os riscos.

A palavra “informação” destacada pelos gestores está presente em todos os domínios evidenciados nesta pesquisa, refere-se às informações internas e externas da organização. Está alinhada ao conceito de Zeman (1979) que significa uma forma de representar, de apresentar ou de criar uma ideia aos usuários. Ela foi destacada pela gerente de TI como “o valor mais precioso que a empresa tem”, portanto está alinhada também com Ribeiro Filho, Lopes e Perdeneiras (2009) quando abordam

que a informação é essencial, bem como com a abordagem de Sêmola (2014) que considera a informação um dos ativos mais relevantes de uma organização.

A “informação” foi atrelada a diversas características qualitativas, como: acessibilidade, conformidade, confiança, disponibilidade, integridade, segurança da informação, validação e responsabilidade.

O “acesso” citado pelos gestores está presente nos domínios: Direito de propriedade intelectual (D2); Proteção de registros organizacionais (D3); Conformidade com as políticas de segurança da informação (D7) e; Análise crítica da conformidade técnica (D8). A palavra “acesso” relatada pelos gestores refere-se ao acesso da informação e também às limitações de acesso.

Sobre o acesso da informação os gestores relataram os acessos dos usuários internos e externos. O acesso interno refere-se a determinados sites da internet, bem como o uso de um sistema integrado que proporciona o acesso aos relatórios gerenciais. Já no acesso aos usuários externos, abordou-se o acesso às demonstrações contábeis pelos *stakeholders*. Esses acessos às informações possibilitam a tomada de decisão e abordam o conceito de acessibilidade evidenciado por Ferreira *et al.* (2015); Gerard e Weber (2015); Mateescu (2015); Oliveira *et al.* (2015).

Quanto às limitações de acesso, os gestores relataram a importância da restrição, ou seja, somente tem permissão de acesso às transações e pastas de rede o usuário com o perfil autorizado pelo gestor. Este procedimento segundo os gestores protege a informação contra acessos não autorizados. As limitações de acesso convergem com as recomendações da ISO/IEC 27002 (2013) e também com as obras de Albertin e Pinochet (2010) e Sêmola (2014).

A “conformidade” palavra-chave destacada por todos os gestores e presente em todos os domínios, exceto no domínio - Proteção e privacidade de informações de identificação pessoal (D4) foi evidenciada no intuito de cumprir os vários requisitos internos e externos da organização. Os gestores relataram que os controles, as responsabilidades individuais, as melhorias de processo, as políticas internas, o cumprimento de legislações e a auditoria independente são requisitos fundamentais para a conformidade. De acordo com o gerente de controladoria elas contribuem “de forma vital” para a empresa.

O conceito de conformidade abordado pelos gestores converge com Ferreira *et al.* (2015), Mateescu (2015), Griffith *et al.* (2016). Estes autores conceituam a

conformidade como o cumprimento de normas reguladoras, tanto no ambiente interno quanto externo da organização. A percepção dos gestores está alinhada também com o estudo de Turrent e Ariza (2016) o qual indica que a conformidade da governança corporativa propicia maior controle e manutenção da reputação no mercado.

No entanto esta pesquisa diverge do estudo de Darounco (2013). Este autor evidenciou a falta de processos, sistemas e controles padronizados e sistematizados, sendo determinantes para a manutenção da conformidade. Constatou-se nesta pesquisa que os controles e processos são padronizados e sistematizados contribuindo para a conformidade das informações.

Outra palavra destacada pelos gestores refere-se à confiança, ela está presente em todos os domínios, exceto nos domínios - Proteção e privacidade de informações de identificação pessoal (D4); Regulamentação de controles de criptografia (D5).

A palavra “confiança” remete ao conceito de confiabilidade. Os gestores explicaram que a confiança das informações está atrelada ao treinamento dos usuários, suas responsabilidades, as atribuições, a proteção dos registros organizacionais, ao desenho do processo interno e a validação da auditoria externa. A auditoria externa, na percepção dos gestores, contribui para a confiabilidade das informações, pois é um órgão independente que valida as informações possibilitando confiança aos *stakeholders*.

Neste sentido, a “confiabilidade” evidenciada pelos gestores significa que o usuário aceita a informação e a utiliza como base de decisão (HENDRIKSEN; VAN BREDA, 1999; RIBEIRO FILHO; LOPES; PERDENEIRAS, 2009; IUDÍCIBUS (2010); CPC 00 R1 (2011); SOUZA *et al.* (2015); JORISSEN (2015); AZAD *et al.* (2016), bem como a atuação do sistema ocorre conforme o esperado. (ALBERTIN; PINOCHET, 2010).

A palavra “disponível” remete a palavra “disponibilidade” que foi evidenciada pelos gestores nos domínios: Identificação da legislação aplicável (D1); Proteção de registros organizacionais (D3) e; Regulamentação de controles de criptografia (D5). Os gestores relataram que o sistema disponibiliza as informações aos usuários internos e externos, bem como existe a recuperação dos dados permitindo sua a disponibilidade de forma completa e íntegra via *backup*. A criptografia também foi evidenciada no sentido de disponibilizar a informação segura.

Os relatos dos gestores quanto à disponibilidade estão alinhados com os conceitos de Hendriksen e Van Breda (1999), Dhillon e Backhouse (2000), Ribeiro Filho, Lopes e Perdeneiras (2009), Iudícibus (2010), Albertin e Pinochet (2010), CPC 00 R1 (2011), Souza *et al.* (2015); Safa *et al.* (2015), Jorissen (2015) e Azad *et al.* (2016).

A palavra “integridade” também foi abordada pelos gestores, ela está presente nos domínios: Direitos de propriedade intelectual (D2); Proteção de registros organizacionais (D3); Conformidade com as políticas de segurança da informação (D7) e; Análise crítica da conformidade técnica (D8). As práticas evidenciadas nestes domínios, abordam a “integridade” como a garantia de que ninguém possa manipular a informação ou lesar a empresa. Os registros contábeis, recuperação dos dados (backup), divulgação dos dados ao mercado, validação pela auditoria externa, nível 2 da governança corporativa, sistema integrado, profissionais qualificados, limitações de acessos, são exemplos citados pelos gestores.

A “integridade” relatada pelos gestores converge com a proteção contra alterações indevidas de Dhillon e Backhouse (2000); Albertin e Pinochet (2010); Sêmola (2014); Uddin e Preston (2015); Safa *et al.* (2015), bem como com a informação mais completa possível sem omissão de algum fato relevante. (HENDRIKSEN; VAN BREDA, 1999; RIBEIRO FILHO; LOPES; PERDENEIRAS, 2009; IUDÍCIBUS (2010); CPC 00 R1 (2011); SOUZA *et al.* (2015); JORISSEN (2015); AZAD *et al.* (2016).

Quanto a palavra “responsabilidade” foi evidenciada pelos gestores nos domínios: Identificação da legislação aplicável (D1); Proteção de registros organizacionais (D3); Proteção e privacidade de informações de identificação pessoal (D4); Conformidade com as políticas e procedimentos de segurança da informação (D7). Ela foi abordada na questão que envolve a responsabilidade do funcionário, da área de atuação, da auditoria externa (independente), assinaturas digitais, autorização para transações. Desta forma, a “responsabilidade” significa responder pelas ações próprias ou dos outros. (FERREIRA *et al.*, 2015; GERARD; WEBER, 2015; MATEESCU, 2015; OLIVEIRA *et al.* 2015).

A palavra “validação” foi abordada pelos gestores nos domínios: Identificação da legislação aplicável (D1); Análise crítica independente da segurança da informação (D6) e; Conformidade com as políticas e procedimentos de segurança da informação (D7). Os gestores responderam que a validação da informação ocorre

por meio de análises críticas internas, dentro do setor de atuação do gestor. Já a validação externa ocorre por um órgão independente, sendo este destacado constantemente pelos gestores. A palavra “validação” remete ao conceito de “autencidade” que significa a garantia que a informação não foi alterada após o envio ou validação. (SÊMOLA, 2014).

A palavra “segurança da informação” foi relatada nos domínios: Direitos de propriedade intelectual (D2); Proteção de registros organizacionais (D3); Regulamentação de controles de criptografia (D5); Conformidade com as políticas e procedimentos de segurança da informação (D7) e; Análise crítica da conformidade técnica (D8). Os gestores acreditam que as práticas evidenciadas nestes domínios contribuem para a conformidade.

A segurança da informação foi relacionada pelos gestores aos conceitos de integridade, disponibilidade, políticas de segurança, conformidade, confiabilidade, confidencialidade e autenticidade, convergindo com o os conceitos de Dhillon e Backhouse (2000); Albertin e Pinochet (2010); Bulgurcu, Cavusoglu e Benbasat (2010); Fontes (2012); Sêmola (2014); Uddin e Preston (2015); Safa *et al.* (2015). No entanto, os gestores atribuíram também à segurança da informação os conceitos de responsabilidade e acessibilidade.

Quanto a palavra “mitigar os riscos” foi abordada pelos gestores em todos os domínios, exceto no domínio Identificação da legislação aplicável (D1). Alguns exemplos citados pelos gestores referem-se à: licenças, políticas de utilização dos softwares, rastreabilidade das informações, integridade das informações, base única dos dados, backup, confiança no sistema, termo de responsabilidade assinado pelo funcionário, assessoria jurídica, auditoria externa na validação da informação e verificação dos processos internos, processos desenhados. De acordo com a coordenadora fiscal, essas normas e procedimentos mitigam também o risco de divergência e vazamento de informações.

Os exemplos acima citados pelos gestores estão alinhados ao conceito de avaliação de risco, que significa a gestão preventiva de riscos, monitoramento e supervisão contínua dos processos (GRIFFITH *et al.,* 2016).

Com base na análise qualitativa das entrevistas observou-se que as práticas de segurança da informação evidenciadas na ISO/IEC 27002 (2013) integradas aos conceitos de qualidade da informação contábil contribuem para a conformidade da governança corporativa, no sentido de proporcionar a informação acessível,

disponível, conforme, confiável, íntegra, autentica, responsável e segura para mitigar os possíveis riscos à organização.

Na sequencia, efetuam-se as considerações finais desta pesquisa.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa teve como objetivo geral analisar como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade.

As contribuições decorrentes da utilização de práticas de segurança da informação contábil foram analisadas em uma indústria metalúrgica localizada no Estado do Rio Grande do Sul.

O primeiro objetivo específico desta pesquisa foi identificar as recomendações teóricas de governança corporativa no requisito de conformidade, características qualitativas da informação contábil e segurança da informação. Para este objetivo efetuou-se um construto de pesquisa evidenciado no Quadro 9, o qual foi utilizado na elaboração dos instrumentos de coleta deste estudo.

O segundo objetivo específico foi verificar o nível de controle das práticas de segurança da informação dispostas na ISO/IEC 27002 (2013) no requisito de conformidade, relacionadas às características qualitativas da informação contábil e à conformidade da governança corporativa. Este objetivo pode ser atingido a partir do retorno dos questionários aplicados aos funcionários de nível operacional e gerencial das áreas de contabilidade, fiscal, custos/planejamento, controladoria, financeiro e TI da empresa “X”. Tabulou-se os dados e concluiu-se por meio da análise descritiva que os níveis gerenciais e operacionais possuem percepção semelhante, sugerindo que a proteção das práticas de segurança da informação contábil encontra-se em nível razoável, isto é, a empresa implementa a maioria dos controles a um nível razoável satisfazendo os procedimentos escritos e processos.

O terceiro objetivo específico foi identificar as diferenças de percepção dos grupos operacional e gerencial. Atingiu-se este objetivo a partir do teste de normalidade de Kolmorogov-Smirnov e Shapiro-Wilk, identificou-se que os dados não seguem uma distribuição normal. Após, calculou-se o coeficiente de correlação *rho* de Spearman entre os domínios e constatou-se que apenas os domínios D3 com D4; D4 com D2; e D7 com D8 possuem correlação forte e são estatisticamente significantes ao nível de 1%, portanto o grau de confiança é de 99%. Por fim, ainda sob a perspectiva quantitativa, efetuou-se o teste de Kruskal-Wallis e verificou-se que a percepção dos níveis gerencial e operacional é estatisticamente igual, corroborando com a análise descritiva.

O quarto objetivo específico foi avaliar qualitativamente se a empresa analisada efetua as práticas de segurança da informação no requisito da conformidade da ISO/IEC 27002 (2013) relacionadas com as características qualitativas da informação contábil e conformidade da governança corporativa. Este objetivo foi atingido a partir de entrevistas com os gestores das áreas de contabilidade, fiscal, custos/planejamento, controladoria, financeiro e TI e, corroborado pela análise documental. Conclui-se que das 41 práticas apresentadas, a empresa analisada utiliza 27 práticas; 4 não são utilizadas e; 10 não há um consenso dos gestores quanto à utilização. As práticas utilizadas pela empresa referem-se às questões já apresentadas anteriormente na Tabela 11.

Por fim, analisou-se a contribuição destas práticas para a governança corporativa no requisito de conformidade. A pesquisa fornece evidências aos usuários das informações de como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade. Constatou-se que os controles; processos internos VSM; checklist; conciliações; restrição de acesso ao sistema, internet e pastas na rede; indicadores de desempenho; responsabilidades individuais; política de uso legal de produtos e software; termo de responsabilidade; aquisição de software somente por fontes conhecidas; restrição de instalação de software; firewall; políticas de segurança; servidores em local adequado; assinatura digital; criptografia; backup dos dados; única base de dados; assessora jurídica e auditoria externa contribuem proporcionando a acessibilidade, conformidade, confiabilidade, disponibilidade, integridade, responsabilidade, autenticidade, segurança da informação, bem como contribui para mitigar os riscos à organização.

Quanto às contribuições no âmbito acadêmico, esta pesquisa contribui na criação de um modelo teórico de pesquisa gerado a partir da revisão da literatura, apresentando os conceitos relevantes ao estudo. No âmbito profissional, contribui fornecendo evidências aos usuários das informações contábeis de que as práticas de segurança da informação contribuem para a governança corporativa no requisito de conformidade.

Por se tratar de um estudo de caso único, a presente pesquisa não permite generalizações ou inferências extensivas a todas as indústrias metalúrgicas, porém contribui por aprofundar o fenômeno estudado podendo ser transferível a outros contextos. Outra limitação refere-se às entrevistas, não foi possível identificar a

contribuição de 10 práticas, visto que não houve convergência entre os entrevistados.

Utilizou-se nesta pesquisa como percurso metodológico entrevistas e análise documental, portanto questões envolvendo o processo operacional e como se gera a informação podem ser realizadas a fim de servir como aprendizado.

Recomenda-se também a realização de pesquisas envolvendo estudos multicasos, acredita-se que estes podem contribuir na identificação de novos elementos, bem como estudos considerando empresas de outros setores. Estudos quantitativos envolvendo amostras grandes podem ser realizados com base nos instrumentos criados, no intuito de buscar uma efetiva generalização dos resultados.

Por fim, recomenda-se estudos envolvendo outros princípios da governança corporativa, como a transparência, equidade, prestação de contas ou responsabilidade corporativa, a fim de identificar como as práticas de segurança da informação podem contribuir para tal princípio.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **Norma Brasileira ISO/IEC 27002, 2013**. Rio de Janeiro: ABNT, 2013.

ADILOGLU, B.; VURAN, B. The relationship between the financial ratios and transparency levels of financial information disclosures within the scope of corporate governance: evidence from turkey. **Journal of Applied Business Research (JABR)**, v. 28, n. 4, p. 543-554, Jul-Aug. 2012.

AKBAR, S.; HUGHES, J.P; FAITOURI, R.E; SHAH, S.Z.A. More on the relationship between corporate governance and firm performance in the UK: Evidence from the application of generalized method of moments estimation. **Research in International Business and Finance**, v. 38, n. 3, p. 417-429, Sep. 2016.

ALBERTIN, A.L.; PINOCHET, L.H.C. **Política de segurança de informações:** uma visão organizacional para a sua formulação. São Paulo: Elsevier, 2010.

ÁLVARES, E.; GIACOMETTI, C.; GUSSO, E. **Governança corporativa**. 4.ed. Rio de Janeiro: Elsevier, 2008.

AZAD, R.; AZAD, R.; AZAD, K.; AKBARI, F. The effect of cost accounting system inventory on increasing the profitability of products. **Journal of Industrial and Intelligent Information Vol**, v. 4, n. 1, p. 83-87, Jan. 2016.

BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL – BNDES. Disponível em: <http://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Institucional/Apoio_Financeiro/porte.html>. Acesso em: 18 fev. 2016.

BANK FOR INTERNATIONAL STTLEMENTS – BIS. 1998. Disponível em: <http://www.bis.org/publ/bcbs41.pdf>. Acesso em: 14 jan. 2016.

BARBOSA, J.S.; SCHERER, L.M.; SCARPIN, J.E.; MURCIA, F.D.R. Construction of a metric of quality of accouting information from the perspective of fundamental analysts. **Revista de Contabilidade e Organizações**, v. 9, n. 24, p. 42-55, Jul. 2015.

BARDIN, L. Análise de conteúdo. Tradução: Luís Antero Reto. 3ª reimp. 1ª edição, São Paulo: Edições 70, 2016.

BERLE, A.A.J.; MEANS, G. C. **A moderna sociedade anônima e a propriedade privada**. Tradução: Dinah de Abreu Azevedo. 2ª edição, São Paulo: Nova Cultural, 1984.

BHASIN, M.L. Contribution of forensic accounting to corporate governance: an exploratory study of an Asian country. **International Business Management**, v. 10, n. 4, p. 479-492, Apr. 2016.

BRUM, M.C.S. **Controles internos e de tecnologia da informação na mitigação dos riscos de conformidade das informações contábeis**. 2014. Dissertação

(Mestrado em Ciências Contábeis). Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2014.

BUCCAFURRI, F.; FOTIA, L.; FURFARO, A.; GARRO, A.; GIACALONE, M.; TUNDIS, A. An analytical processing approach to supporting cyber security compliance assessment. **Proceedings of the 8th International Conference on Security of Information and Networks**, p. 46-53, Sep. 2015.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS quarterly**, v. 34, n. 3, p. 523-548, Sep. 2010.

CAI, J.; LIU, Y.; QIAN, Y.; YU, M. Information asymmetry and corporate governance. **The Quarterly Journal of Finance**, v. 5, n. 3, p. 1550014-1550046, May. 2015.

CARLESSO NETO, O.; RIBEIRO, K.C.S; OLIVEIRA NETO, O.J; ROGERS, D. Avaliação das performances das práticas de governança corporativa: uma análise multiperíodo em empresas listadas no Brasil. **RGC-Revista de Governança Corporativa**, v. 2, n. 1, p. 66-93, Abr. 2015.

CHAKRAVARTI, I.M; LAHA, R.G, (1967). **Handbook of Methods of Applied Statistics**. v I. John Wiley & Sons, 1967.

CHANG, C.S.; YU, S.W; HUNG, C.H. Firm risk and performance: the role of corporate governance. **Review of Managerial Science**, v. 9, n. 1, p. 141-173, Jan. 2015.

COLLIS, J.; HUSSEY, R. **Pesquisa em administração:** um guia prático para alunos de graduação e pós-graduação. Tradução: Lucia Simonini. 2ª edição, Porto Alegre: Bookman, 2005.

COMITÊ DE PRONUNCIAMENTOS CONTÁBEIS – CPC. CPC 00 R1: estrutura conceitual para elaboração e divulgação de relatório contábil-financeiro. 2011 Disponível em: <http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=80>. Acesso em: 22 out. 2015.

DAMODARAN, A. **Gestão estratégica do risco:** uma referência para a tomada de riscos empresariais. Tradução: Félix Nonnenmacher. Porto Alegre: Bookman, 2009.

DANCEY, Christine P.; REIDY, John. **Estatística sem matemática para psicologia**. Tradução: Lori Viali. 5ª edição, Porto Alegre: Penso, 2013.

DAROUNCO, J.M. **Análise de processo de controles internos e de TI no requisito de conformidade da governança corporativa**. 2013. Dissertação (Mestrado em Ciências Contábeis). Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2013.

DEDONATTO, O.; BEUREN, I.M. Análise dos impactos para a Contabilidade no processo de implantação da governança corporativa em uma empresa. **Revista Contabilidade e Controladoria**, v. 2, n. 3, p. 23-38, Dez. 2010.

DHILLON, G.; BACKHOUSE, J. Technical opinion: information system security management in the new millennium. **Communications of the ACM**, v. 43, n. 7, p. 125-128, Jul. 2000.

DISTERER, G. ISO/IEC 27000, 27001 and 27002 for information security management. **Journal of Information Security.** v. 4, n. 2, p. 1-9, Apr. 2013.

ELLUL, A. The role of risk management in corporate governance. **Annual Review of Financial Economics**, v. 7, n. 1, p. 279-299, Dec. 2015.

ELOFF, J.H.P; ELOFF, M. Information security management: a new paradigm. In: proceedings of the 2003 annual research conference of the south African institute of computer scientists and information technologists on enablement through technology. **South African Institute for Computer Scientists and Information Technologists**, p. 130-136, Sep. 2003.

FERREIRA, E.F.C.; MATOS, F.R.N.; MATOS, D.M.; BUGARIM, M.C.C.; MACHADO, D.Q. Governança corporativa na saúde suplementar: estudo de caso em uma operadora de plano de saúde. **Pensamento & Realidade. Revista do Programa de Estudos Pós-Graduados em Administração-FEA**, v. 29, n. 3, p. 19-39, Dez. 2015.

FONTES, E. **Políticas e normas para a segurança da informação:** como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. 1ª edição, Rio de Janeiro: Brasport, 2012.

GERARD, J.A.; WEBER, C.M. Compliance and corporate governance: theoretical analysis of the effectiveness of compliance based on locus of functional responsibility. **International Journal of Global Business**, v. 8, n. 1, p. 15-26, Jun. 2015.

GRIFFITH, S.J.; THEL, S.; BAER, M.; MILLER, G.P.; MANWAH, G.; BRESLOW, S.; COHEN, A.; GRANT, M.; KLEHM, H.; MEYER, A.; BAXTER JR, T.C. The Changing Face of Corporate Compliance and Corporate Governance. **Fordham Journal of Corporate & Financial Law**, v. 21, n. 1, p. 1- 71, Jan-Mar. 2016.

HENDRIKSEN, E.S.; VAN BREDA, M.F. **Teoria da contabilidade**. Tradução: Antonio Zoratto Sanvicente. 5ª edição, São Paulo: Atlas, 1999.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das melhores práticas de governança corporativa.** [S.I.], 4 ed., p. 73, 2009. Disponível em: <http://www.ibgc.org.br/userfiles/files/Codigo_Final_4a_Edicao.pdf>. Acesso em: 18 set. 2015.

IUDÍCIBUS, S. de. **Teoria da contabilidade.** 9ª edição, São Paulo: Atlas, 2009.

IUDÍCIBUS, S. de. **Manual de contabilidade e societária:** aplicável a todas as sociedades de acordo com as normas internacionais e do CPC. 1ª edição, São Paulo: Atlas, 2010.

JENSEN, M.C.; MECKLING, W.H. Theory of the firm: managerial behavior, agency costs and ownership structure. **Journal of financial economics**, v. 3, n. 4, p. 305-360, Oct. 1976.

JORISSEN, A. The IASB: from high quality accounting information towards information to foster trust and stability in global markets. **Revista Contabilidade & Finanças**, v. 26, n. 69, p. 243-246, Sep-Dec. 2015.

KANAPATHIPILLAI, S.; JOHL, S.; SUBRAMANIAM, N.; WINES, G. Remuneration committee existence and effectiveness: A study on their impact on voluntary narrative executive remuneration disclosure. In: **2015 Financial Markets & Corporate Governance Conference.** p. 1-43, Jan. 2015.

KEARNEY, W.D.; KRUGER, H.A. A framework for good corporate governance and organisational learning–an empirical study. **International Journal of Cyber-Security and Digital Forensics**, v. 2, n. 1, p. 36-47, Jan-Mar. 2013.

KHANNA, V.; KIM, E.; LU, Y. CEO connectedness and corporate fraud. **The Journal of Finance**, v. 70, n. 3, p. 1203-1252, May. 2015.

KLANN, R.C; BEUREN, I.M. Impacto da convergência contábil internacional na suavização de resultados em empresas brasileiras. (portuguese). **Brazilian Business Review**, v.12, n. 2, p. 1-25, Mar. 2015.

LEVIN, J. **Estatística aplicada a ciências humanas**. 2ª edição. São Paulo: Harbra Ltda, 1987.

LIMA, A.S.; CARVALHO, E.V.A; PAULO, E.; GIRÃO, L.F.D.A.P. Estágios do ciclo de vida e qualidade das informações contábeis no Brasil. **RAC-Revista de Administração Contemporânea**, v. 19, n. 3, p. 398-418, Fev. 2015.

LIU, N.; LAING, E.; YEU, C.; ZHANG, X. Institutional Investor and corporate transparency: empirical evidence from China. In: **2015 Financial Markets & Corporate Governance Conference**. p. 1-32, Feb. 2015.

LU, X.U.; WENCHANG, L.I. The study on relationship between internal control and enterprise culture-based on corporate governance mechanism. **International Business and Management**, v. 10, n. 1, p. 82-87, Feb. 2015.

MARTINS, V.G.; OLIVEIRA, A.S.; NIYAMA, J.K.; DINIZ, J.A. Níveis diferenciados de governança corporativa e a qualidade da informação contábil durante o processo de convergência às normas internacionais de contabilidade. **ConTexto**, v. 14, n. 27, p. 23-42, Mai-Ago. 2014.

MATEESCU, R.A. Corporate governance disclosure practices and their determinant factors in European emerging countries. **Journal of Accounting and Management Information Systems**, v. 14, n. 1, p. 170-192. 2015.

MIOT, H.A. Tamanho da amostra em estudos clínicos e experimentais. **J Vasc Bras**, v. 10, n. 4, p. 275-8, Dez. 2011.

MONTESDIOCA, G.P.Z; MAÇADA, A.C.G. Measuring user satisfaction with information security practices. **Computers & Security**, v. 48, n. 1, p. 267-280, Feb. 2015.

MORRIS, R.; SUSILOWATI, I.; GRAY, S.The impact of IFRS adoption versus non-adoption on corporate disclosure levels in the Asian region". In: **American Accounting Association Annual Meeting and Conference on Teaching and Learning in Accounting, Washington DC.** Working Paper. p. 1-42, Jul. 2012.

OLIVEIRA, D.; SILVA, M.P.; LIMA, T.A; SOUZA, M.M.M. Um estudo exploratório da gestão de pessoas na integração e disseminação da governança corporativa. **Augusto Guzzo Revista Acadêmica**, v. 2, n. 16, p. 241-268, Jul-Dez. 2015.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Principles of corporate governance**. Paris. 2004. Disponível em: < http://www.oecd.org/daf/ca/corporategovernanceprinciples/31557724.pdf>. Acesso em 18 set. 2015.

OZKAN, A.; TANÇ, S.G. The research for the awareness level of the hotel business about the social responsibility and accountability concepts. **Journal of US-China Public Administration**, v. 9, n. 1, p. 90-96, Jan. 2012.

PARSONS, K.M.; YOUNG, E.; BUTAVICIUS, M.A; MCCORMAC, A.; PATTINSON, M.R; JERRAM, C. The influence of organizational information security culture on information security decision making. **Journal of Cognitive Engineering and Decision Making**, v. 9, n. 2, p. 117-129, Jun. 2015.

REDDY, K.; ABIDIN, S.; YOU, L. Does corporate governance matter in determining CEO compensation in the publicly listed companies in New Zealand? An empirical investigation. **Managerial Finance**, v. 41, n. 3, p. 301-327, Mar. 2015.

RHEE, H.S; KIM, C.; RYU, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. **Computers & Security**, v. 28, n. 8, p. 816-826, May. 2009.

RIBEIRO FILHO, J.F; LOPES, J.; PEDERNEIRAS, M. **Estudando teoria da contabilidade**. 1ª edição, São Paulo: Atlas, 2009.

SAFA, N.S.; SOOKHAK, M.; VON SOLMS, R.; FURNELL, S.; GHANI, N.A.; HERAWAN, T. Information security conscious care behaviour formation in organizations. **Computers & Security**, v. 53, p. 65-78, Jun. 2015.

SAFA, N.S.; VON SOLMS, R.; FURNELL, S. Information security policy compliance model in organizations. **Computers & Security**, v. 56, p. 70-82, Feb. 2016.

SAITO, R.; SILVEIRA, A.D.M.D. Governança corporativa: custos de agência e estrutura de propriedade. **Revista de Administração de Empresas**, São Paulo, v. 48, n. 2, p. 79-86, Abr-Jun. 2008.

SANTANA, L.M.; GÓIS, A.D; LUCA, M.M.M.; VASCONCELOS, A.C. Relação entre disclosure socioambiental, práticas de governança corporativa e desempenho empresarial. **Revista Organizações em Contexto-online**, v. 11, n. 21, p. 49-72, Jan-Jun. 2015.

SANTOS, L.A.A.; LEMES, S. Desafios das empresas brasileiras na implantação da lei Sarbanes-Oxley. **Revista Base (Administração e Contabilidade) da UNISINOS**, v. 4, n. 1, p. 37-46, Jan-Abr. 2007.

SCHNEIDER, L.C.; VANTI, A.A.; COBO, A.; THOMAZ, J.L.P. Avaliação de processos de segurança da informação integrando as áreas de controladoria e tecnologia da informação. **Revista Universo Contábil**, v. 10, n. 4, p. 68-85, Out-Dez. 2014.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. 2ª edição, Elsevier Brasil, 2014.

SHAMALA, P.; AHMAD, R.; ZOLAIT, A.H.; SAHIB, S.B. Collective information structure model for information security risk assessment (ISRA). **Journal of Systems and Information Technology**, v. 17, n. 2, p. 193-219. Apr-Jun. 2015.

SILVEIRA, A.D.M.D. **Governança corporativa no Brasil e no mundo:** teoria e prática. 2ª edição, Elsevier Brasil, 2015.

SOLER, J.S.B.; MARIN, G.S. Executive compensation and corporate governance in Spanish listed firms: a principal–principal perspective. **Review of Managerial Science**, v. 9, n. 1, p. 115-140, Jan. 2015.

SOUZA, P.; CASTRO, J.K.; BORGERT, A.; FLACH, L.; LUNKES, R.J. Estudo sobre o uso dos atributos da contabilidade gerencial em empresas de capital aberto do setor de energia elétrica. **Revista Ambiente Contábil**-Universidade Federal do Rio Grande do Norte, v. 7, n. 2, p. 215-230, Jul-Dez. 2015.

SPRENT, P; SMEETON, C.N. **Applied Nonparametric Statistical Methods**. 4ª edição. CRC Press, 2016.

STEIN, M.; SALTERIO, S.; SHEARER, T. Transparency'in accounting and corporate governance: making sense of multiple meanings. **Available at SSRN 2565833**, p. 1-56, Feb. 2015.

TURRENT, G.D.C.B; ARIZA, L.R. Corporate governance ratings on listed companies: An institutional perspective in Latin America. **European Journal of Management and Business Economics**, v. 25, n. 2, p. 63-75, May. 2016.

UDDIN, M.; PRESTON, D. Systematic review of identity access management in information security. **Journal of Advances in Computer Networks**, v. 3, n. 2, p. 150-156, Jun. 2015.

YIN, R.K. **Estudo de caso:** planejamento e métodos. Tradução: Cristian Matheus Herrera. 5ª edição, Porto Alegre: Bookman, 2015.

YOUSUF, S.; ISLAM, M.A. The concept of corporate governance and its evolution in Asia. **Research Journal of Finance and Accounting**, v. 6, n. 5, p. 19-25. 2015.

ZAGORCHEV, A.; GAO, L. Corporate governance and performance of financial institutions. **Journal of Economics and Business**, v. 82, p. 17-41, Nov-Dec. 2015.

ZEMAN, J. Significado filosófico da noção de informação. **O conceito de informação na ciência contemporânea**: colóquios filosóficos internacionais de Royaumont. Tradução: Maria Helena Kuhner. Rio de Janeiro: Paz e Terra, 1970.

APÊNDICE A – PROTOCOLO DE PESQUISA

I – IDENTIFICAÇÃO

TÍTULO: Análise das práticas de segurança da informação contábil e sua contribuição para a governança corporativa no requisito de conformidade

PESQUISADOR RESPONSÁVEL:
Nome: Karen Hackbart Souza Fontana
E-mail: karen.hs@bol.com.br

INSTITUIÇÃO RESPONSÁVEL:
Universidade do Vale do Rio dos Sinos - UNISINOS.
Programa de Pós-Graduação em Ciências Contábeis.

ORIENTADOR: Prof. Dr. Tiago Wickstrom Alves

II - VISÃO GERAL

QUESTÃO DE PESQUISA: Como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade?

OBJETIVO GERAL: Analisar como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade.

FONTES DE INFORMAÇÃO:
Empresa “X” – Indústria metalúrgica.

LEITURAS APROPRIADAS:
Governança Corporativa
Características Qualitativas da Informação Contábil
Segurança da Informação/ ISO/IEC 27002

III – PROCEDIMENTOS DE COLETA E ANÁLISE DE DADOS

SELECIONAR OS PARTICIPANTES:

Selecionar as áreas que se relacionam diretamente com as informações contábeis;

Identificar os auxiliares, analistas, supervisores, coordenadores, gerentes e diretores envolvidos de forma direta na geração, processamento e envio de informações para a contabilidade;

Verificar o interesse em participar da pesquisa.

Solicitar *e-mail* da informante-chave.

QUESTIONÁRIO:

Confeccionar o instrumento de Pesquisa Apêndice C.

Contatar os participantes via *e-mail*;

Explicar os objetivos da pesquisa e enviar o questionário;

Efetuar o pré-teste;

Aplicar de forma presencial para os funcionários de nível operacional;

Aplicar via e-mail para os funcionários de nível gerencial;

Monitorar o retorno;

Calcular do tamanho da amostra;

Tabular dos dados;

Efetuar a análise descritiva;

Realizar testes estatísticos;

Analisar o nível de controle das práticas de segurança da informação dispostas na ISO/IEC 27002 (conformidade) relacionadas às características qualitativas da informação contábil e à governança corporativa no requisito de conformidade.

ENTREVISTAS:

Confeccionar o instrumento de Pesquisa Apêndice D.

Contatar a informante-chave (definir local, data e horário);

Cumprir pontualmente o horário marcado;

Explicar o objetivo da pesquisa e o método de condução das entrevistas;

Destacar que os nomes dos gestores não serão revelados, apenas seus cargos;

Solicitar autorização para gravar a entrevista;

Entrevistar os gestores;

Agradecer pela disponibilidade e cooperação no estudo;

Transcrever as gravações das entrevistas;

Analisar as entrevistas, confrontando-as com a teoria

DOCUMENTOS:

Identificar documentos que contribuem para a pesquisa;

Coletar os documentos;

Analisar os documentos pesquisados.

IV – CONVITE PARA PARTICIPAR DA PESQUISA

Enviar por e-mail o convite para participar da pesquisa Apêndice B.

APÊNDICE B – CONVITE PARA PARTICIPAR DA PESQUISA

Prezado *Entrevistado*

Esta mensagem tem como objetivo de reforçar o convite quanto à sua participação na pesquisa, na qual permitirá a elaboração de uma dissertação de mestrado no Programa de Pós-Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos - UNISINOS – São Leopoldo-RS. Para tanto, seguem alguns dados:

a) Título da dissertação: Análise das práticas de segurança da informação contábil e sua contribuição para a governança corporativa no requisito de conformidade.

b) Pesquisador responsável: Karen Hackbart Souza Fontana.

c) Professor Orientador: Prof. Dr. Tiago Wickstrom Alves.

d) Objetivo: Analisar como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade.

e) Fontes de informação: questionário, entrevistas e análise documental.

f) Para aplicação das entrevistas serão selecionadas os gestores das áreas contabilidade, fiscal, custos/planejamento, controladoria, financeiro e TI.

g) Provavelmente cada entrevista terá duração média de 1:30h.

h) As questões relacionam-se aos temas de segurança da informação, informação contábil e governança corporativa. Não será divulgada a identificação dos participantes. O pesquisador se compromete em manter sigilo sobre os dados e quaisquer informações que porventura vier a tomar conhecimento.

i) A unidade de análise (organização) receberá uma cópia da dissertação. Dessa forma, poderá fazer uso e proveito das informações obtidas.

j) Todas as entrevistas serão previamente agendadas de acordo com a disponibilidade dos respondentes, por meio de um informante-chave.

Desde já agradeço a atenção e sua disponibilidade em participar da pesquisa.

Atenciosamente,

Karen Hackbart Souza Fontana – karen.hs@bol.com.br
Mestranda em Ciências Contábeis - UNISINOS

APÊNDICE C – QUESTIONÁRIO

BLOCO 1 – CATEGORIZAÇÃO DO RESPONDENTE

A) Qual a sua área de atuação na empresa?

☐ Contabilidade
☐ Fiscal
☐ Custos
☐ Financeiro
☐ Tecnologia da Informação
☐ Recursos Humanos
☐ Diretoria Administrativa e Financeira

B) Quanto tempo você trabalha na empresa?

☐ Menos de 1 ano
☐ De 1 a 3 anos
☐ De 3 a 5 anos
☐ Mais de 5 anos

C) Qual é seu nível de escolaridade?

☐ Médio completo
☐ Superior incompleto
☐ Superior completo
☐ Pós-graduação
☐ Mestrado
☐ Doutorado

D) Qual a sua área de formação acadêmica?

☐ Administração de empresas
☐ Ciências contábeis
☐ Economia
☐ Engenharia
☐ Outra

BLOCO 2 - Objetivo identificar o nível de controle das práticas de segurança da informação dispostas na seção 18 - Conformidade ISO/IEC 27002 (2013) relacionadas às características da informação contábil e à governança corporativa. Os níveis de proteção de segurança da informação são os seguintes:

Proteção	Descrição
1 - Inadequada	Não há esforço da empresa para implementar os controles recomendados.
2 - Mínima	A empresa adota o mínimo de controles recomendados.
3 - Razoável	A empresa implementa a maioria dos controles a um nível razoável, satisfazendo os procedimentos escritos e processos.
4 - Adequada	A empresa implementa todos os controles recomendados pelo domínio.
Não aplicável	Considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Conformidade	Conceito Segurança da Informação	Conceito Informação Contábil	Conceito Governança Corporativa	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não aplicável
1. Identificação da legislação aplicável								
1.1 Os controles específicos e as responsabilidades individuais para atender aos requisitos estatutários, regulamentares, contratuais são definidos e documentados, permitindo ao usuário a identificação de diferenças e semelhanças com as normas no ambiente interno e externo.	Conformidade	Comparabilidade	Conformidade					
2. Direitos de propriedade intelectual								
2.1 A divulgação da política de uso legal de produtos de *software* e de informação é exposta de forma compreensível aos usuários atendendo às normas reguladoras no ambiente interno e externo.	Políticas de segurança	Compreensibilidade	Conformidade					
2.2 A aquisição de *software* somente por meio de fontes conhecidas e de reputação para assegurar que o direito autoral não está sendo violado ocorre de forma idêntica e uniforme prevenindo o risco por meio de monitoramento e supervisão de processos operacionais.	Confiabilidade	Uniformidade	Risco					
2.3 A conscientização das políticas para proteger os direitos de propriedade intelectual é considerada útil com vistas à responsabilidade pelas ações próprias ou dos outros.	Políticas de segurança	Utilidade	Responsabilidade					
2.4 A manutenção e identificação dos registros de ativos para proteger os direitos de propriedade intelectual ocorrem sem omissão ou distorção, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa.	Autenticidade	Materialidade	Legitimidade					
2.5 A manutenção de provas e evidências de propriedade (ex: licenças, manuais, acessos) evitam a omissão ou distorção nas decisões dos usuários, mediante a responsabilidade sobre as ações próprias ou dos outros.	Integridade	Materialidade	Responsabilidade					

2.6 Os controles neutralizam os vieses e asseguram que o número máximo de usuários permitidos não exceda o número de licenças adquiridas por meio do cumprindo normas de regulação do ambiente interno.	Conformidade	Neutralidade	Conformidade					
2.7 As verificações de aquisição e instalação de *softwares* autorizados e licenciados ocorre de forma mais completa possível, sem omissão de algum fato relevante, permitindo um clima de confiança.	Autenticidade	Integridade	Transparência					
2.8 A política para a manutenção das condições adequadas de licenças é exposta de forma compreensível ao usuário, contribuindo para uma boa imagem perante os *stakeholders*.	Políticas de segurança	Compreensibilidade	Criação de valor					
2.9 A política para disposição ou transferência de *software* é exposta de forma compreensível ao usuário contribuindo na prevenção de risco, monitoramento e supervisão contínua dos processos.	Políticas de segurança	Compreensibilidade	Risco					
2.10 O cumprimento de termos e condições para *software* e informação obtidos a partir de redes públicas pode ser verificável prevenindo o risco, monitoramento e supervisão contínua dos processos.	Conformidade	Verificabilidade	Risco					
2.11 Não copiar no todo ou em partes documentos em geral, além daqueles permitidos pela lei de direito autoral. Este procedimento evita as manipulações e deve considerar o comportamento ético e moral.	Autenticidade	Representação fidedigna	Ética					
3. Proteção de registros organizacionais								
3.1 Os registros são categorizados em tipos (ex: registros contábeis, registros de bases de dados, de transações) e são disponibilizados em tempo hábil para a tomada de decisão, permitindo um clima de confiança.	Disponibilidade	Tempestividade	Transparência					
3.2 Os registros armazenados possuem detalhes de proteção ao longo do tempo e estão disponíveis em local adequado.	Integridade	Disponibilidade	Locais funcionais					

3.3 As chaves de criptografia ou assinaturas digitais são armazenadas de forma a permitir a decifração de registros pelo período de tempo que os registros são mantidos. Elas estão livres de erros, vieses e manipulações, auxiliando na prevenção de riscos, monitoramento e supervisão contínua dos processos.	Disponibilidade	Representação fidedigna	Risco					
3.4 Os cuidados quanto a possibilidade de deterioração das mídias armazenadas ocorre de forma semelhante para itens afins dentro da estrutura organizacional.	Políticas de segurança	Consistência	Locais funcionais					
3.5 Os procedimentos para assegurar a capacidade de acesso aos dados contra perdas ocasionadas pelas futuras mudanças na tecnologia, permitem aos usuários identificar diferenças e semelhanças, interpretando e avaliando os regulamentos para limitar as perdas.	Integridade	Comparabilidade	Avaliação de risco					
3.6 O dado pode ser recuperado de forma aceitável, mais completa possível e sem omissão, por meio de monitoramento e supervisão contínua dos processos.	Autenticidade	Integridade	Risco					
3.7 A destruição apropriada dos registros, caso não sejam mais necessários à organização, ocorre com cautela cumprindo normas reguladoras no ambiente interno e externo.	Políticas de segurança	Prudência ou conservadorismo	Conformidade					
3.8 A emissão de diretrizes gerais para retenção, armazenamento, tratamento e disposição de registro de informações é capaz de predizer resultados futuros por meio de normas reguladoras no ambiente interno e externo.	Políticas de segurança	Preditiva	Conformidade					
3.9 A programação para retenção, precisa identificar os registros essenciais e o período que cada um deve ser mantido de forma disponível e acessível aos usuários.	Confiabilidade	Disponibilidade	Acessibilidade					
3.10 A manutenção de um inventário das fontes de informações-chave ocorre em tempo hábil permitindo o acesso às informações para a tomada de decisão.	Disponibilidade	Tempestividade	Acessibilidade					
4. Proteção e privacidade de informações de identificação pessoal								

4.1 A política de privacidade e proteção de dados da organização é relevante, pois permite interpretar e avaliar os regulamentos para limitar as perdas.	Confidencialidade	Relevância	Avaliação de risco					
4.2 A comunicação da política de privacidade e proteção de dados a todas as pessoas envolvidas no processo é exposta de forma mais compreensível possível ao usuário, possibilitando a construção de uma boa imagem perante os seus *stakeholders*.	Disponibilidade	Compreensibilidade	Reputação corporativa					
4.3 Existe uma pessoa responsável (*privacy officer*) que tem a função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos a serem seguidos. Essas orientações devem ser expostas de forma compreensível ao usuário, possibilitando um padrão de excelência operacional percebida pelos *stakeholders*.	Políticas de segurança	Compreensibilidade	Criação de valor					
5. Regulamentação de controles de criptografia								
5.1 As restrições quanto ao uso de criptografia ocorrem com cautela de acordo com o cumprimento de normas reguladoras internas.	Confidencialidade	Prudência ou conservadorismo	Conformidade					
5.2 A assessoria jurídica garante a conformidade com as legislações e regulamentações possibilitando a informação livre de erros, vieses e manipulações por meio do cumprimento de normas internas e externas.	Conformidade	Representação fidedigna	Conformidade					
6. Análise crítica independente da segurança da informação								
6.1 A análise crítica da segurança da informação é iniciada pela direção de forma confiável para que o usuário aceite a informação e a utilize, construindo uma boa imagem perante os *stakeholders*.	Políticas de segurança	Confiabilidade	Reputação corporativa					
6.2 A análise crítica inclui a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação, evidenciando suas diferenças e semelhanças para a busca de excelência operacional percebida pelos *stakeholders*.	Políticas de segurança	Comparabilidade	Criação de valor					

6.3 A análise crítica inclui política e objetivos de controle relevantes, capazes de fazer a diferença na gestão preventiva de riscos, monitoramento e supervisão contínua dos processos.	Políticas de segurança	Relevância	Risco					
6.4 A análise crítica é executada por pessoas independentes (ex: auditoria interna, gerente independente ou uma organização externa especializada em tais análises críticas), refletindo de fato o que ocorreu independente de um contrato. Deve fornecer evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever.	Políticas de segurança	Primazia da essência sobre a forma	Legitimidade					
6.5 Os resultados da análise crítica independente são registrados e relatados à direção, de forma neutra não havendo viés de resultado por meio de informações úteis aos usuários permitindo um clima de confiança.	Integridade	Neutralidade	Transparência					
6.6 A direção efetua ações corretivas quando os resultados da análise crítica forem inadequados ou não conforme pela segurança da informação, para garantir a confiança da informação e cumprir com obrigações de suas responsabilidades.	Conformidade	Confiabilidade	Responsabilidade					
7. Conformidade com as políticas e procedimentos de segurança da informação								
7.1 Os gestores identificam as causas quando há qualquer não conformidade, evidenciando as diferenças e semelhanças, por meio de um comportamento ético e moral.	Autenticidade	Comparabilidade	Ética					
7.2 Os gestores implementam ações corretivas após a detecção da não conformidade de forma mais completa possível, sem omissão de algum fato relevante, atuando com responsabilidade pelas ações próprias ou dos outros.	Integridade	Integridade	Responsabilidade					
7.3 Os gestores analisam criticamente as ações corretivas tomadas para predizer resultados futuros, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever.	Conformidade	Preditiva	Legitimidade					

7.4 Os resultados das análises críticas e das ações corretivas pelos gestores são registradas e mantidas mediante informações íntegras e tempestivas de acordo com as normas reguladoras internas e externas.	Disponibilidade	Oportunidade	Conformidade					
7.5 Os gestores relatam os resultados para as pessoas que estão efetuando a análise crítica independente, identificando as diferenças e semelhanças das informações permitindo um clima de confiança.	Confiabilidade	Comparabilidade	Transparência					
8. Análise crítica da conformidade técnica								
8.1 A verificação de conformidade técnica deve ter apoio de uma ferramenta automática para a interpretação do especialista técnico, proporcionando um consenso, interpretação e avaliação de regulamentos para limitar as perdas.	Confiabilidade	Verificabilidade	Avaliação de risco					
8.2 Os testes de invasão ou avaliações de vulnerabilidades são planejados, documentados e repetidos quando incertezas estiverem envolvidas, para prevenir riscos, monitorando e supervisionando continuamente os processos operacionais.	Autenticidade	Prudência ou conservadorismo	Risco					
8.3 A verificação de conformidade técnica somente é executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas, de forma a garantir a informação mais completa e sem omissão de algum fato relevante, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa.	Confidencialidade	Integridade	Legitimidade					

APÊNDICE D – PROTOCOLO DE ENTREVISTA

1. Identificação da legislação aplicável

1.1 Os controles específicos e as responsabilidades individuais para atender aos requisitos estatutários, regulamentares, contratuais são definidos e documentados, permitindo ao usuário a identificação de diferenças e semelhanças com as normas no ambiente interno e externo. (*Conformidade – Comparabilidade – Conformidade).*

Como são feitos os controles e responsabilidades individuais? Esses controles atendem os requisitos estatutários, regulamentares e contratuais? De que forma? Esses controles são definidos e documentados? De que forma? Esses controles permitem ao usuário a identificação de diferenças e semelhanças com as normas no ambiente interno e externo? De que forma?

De que forma você acha que essas práticas podem contribuir para a conformidade?

2. Direitos de propriedade intelectual

2.1 A divulgação da política de uso legal de produtos de *software* e de informação é exposta de forma compreensível aos usuários atendendo às normas reguladoras no ambiente interno e externo. (*Política de segurança – Compreensibilidade – Conformidade).*

Como ocorre a divulgação da política de uso legal de produtos de software e de informação? Os usuários a compreendem? Atendem às normas reguladoras no ambiente interno e externo?

2.2 A aquisição de *software* somente por meio de fontes conhecidas e de reputação para assegurar que o direito autoral não está sendo violado ocorre de forma idêntica e uniforme prevenindo o risco por meio de monitoramento e supervisão de processos operacionais. (*Confiabilidade – Uniformidade – Risco).*

A aquisição de software ocorre somente por meio de fontes conhecidas e de reputação? Há uma forma “uniformidade” do processo de compra de software? De que forma você acha que esta prática reduz o risco?

2.3 A conscientização das políticas para proteger os direitos de propriedade intelectual é considerada útil com vistas à responsabilidade pelas ações próprias ou dos outros. (*Política de segurança – Utilidade – Responsabilidade).*

Na sua opinião, existe uma conscientização das políticas para proteger os direitos de propriedade intelectual? De que forma ela é útil?

2.4 A manutenção e identificação dos registros de ativos para proteger os direitos de propriedade intelectual ocorrem sem omissão ou distorção, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa. (*Autenticidade – Materialidade – Legitimidade).*

Como ocorre a manutenção e identificação dos registros de ativos para proteger os direitos de propriedade? Pode existir omissão ou distorção mediante essa manutenção? Isso é percebido pelos *stakeholders*? De que forma?

2.5 A manutenção de provas e evidências de propriedade (ex: licenças, manuais, acessos) evitam a omissão ou distorção nas decisões dos usuários, mediante a responsabilidade sobre as ações próprias ou dos outros. (*Integridade – Materialidade – Responsabilidade).*

De que forma você acha que manter provas e evidências de propriedade podem evitar omissão ou distorção nas decisões dos usuários?

2.6 Os controles neutralizam os vieses e asseguram que o número máximo de usuários permitidos não exceda o número de licenças adquiridas por meio do cumprindo normas de regulação do ambiente interno. (*Conformidade – Neutralidade – Conformidade).*

Existe um número máximo de usuários permitidos para que não exceda o número de licenças adquiridas? Você sabe qual é esse número?

2.7 As verificações de aquisição e instalação de *softwares* autorizados e licenciados ocorre de forma mais completa possível, sem omissão de algum fato relevante, permitindo um clima de confiança. (*Autenticidade – Integridade – Transparência).*

Existe a verificação desta aquisição e instalação? Como ocorre?

2.8 A política para a manutenção das condições adequadas de licenças é exposta de forma compreensível ao usuário, contribuindo para uma boa imagem perante os *stakeholders*. (*Política de segurança – Compreensibilidade – Criação de valor).*

Existe uma política para a manutenção das condições adequadas de licenças? Como é exposta ao usuário? Os *stakeholders* conseguem perceber? De que forma eles percebem?

2.9 A política para disposição ou transferência de *software* é exposta de forma compreensível ao usuário contribuindo na prevenção de risco, monitoramento e supervisão contínua dos processos. (*Política de segurança – Compreensibilidade- Risco).*

Existe uma política para disposição ou transferência de software? De que forma o usuário tem conhecimento dessa política?

2.10 O cumprimento de termos e condições para *software* e informação obtidos a partir de redes públicas pode ser verificável prevenindo o risco, monitoramento e supervisão contínua dos processos. (*Conformidade- Verificabilidade- Risco).*

Os usuários têm acesso à rede pública? (ex: redes sociais, intenet...). O usuário consegue acessar a rede da organização com a rede pública ao mesmo tempo?

2.11 Não copiar no todo ou em partes documentos em geral, além daqueles permitidos pela lei de direito autoral. Este procedimento evita as manipulações e deve considerar o comportamento ético e moral. (*Autenticidade – Representação Fidedigna – Ética).*

Existe alguma proteção quanto à cópia de documentos em geral? Como ocorre?

De que forma você acha que essas práticas podem contribuir para a conformidade?

3. Proteção de registros organizacionais

3.1 Os registros são categorizados em tipos (ex: registros contábeis, registros de bases de dados, de transações) e são disponibilizados em tempo hábil para a tomada de decisão, permitindo um clima de confiança. (*Disponibilidade – Tempestividade – Transparência).*

Os registros são categorizados em tipos? (ex: registros contábeis, registro de base de dados, de transações). Você acha que estes registros são disponibilizados em tempo hábil para a tomada de decisão? Por quê? Você considera que estes registros possibilitam a confiança/transparência nas informações? Por quê?

3.2 Os registros armazenados possuem detalhes de proteção ao longo do tempo e estão disponíveis em local adequado. (*Integridade – Disponibilidade – Locais Funcionais).*

Como é feita a proteção dos registros que são armazenados? Eles estão disponíveis? Como é esse acesso aos registros? Você considera que esses registros estão armazenados em local adequado? Por quê?

3.3 As chaves de criptografia ou assinaturas digitais são armazenadas de forma a permitir a decifração de registros pelo período de tempo que os registros são mantidos. Elas estão livres de erros, vieses e manipulações, auxiliando na prevenção de riscos, monitoramento e supervisão contínua dos processos. (*Disponibilidade – Representação fidedigna – Risco).*

Comente sobre as chaves de criptografia ou assinaturas digitais? Como as assinaturas digitais são armazenadas/guardadas? Você acredita que elas estão livres de erros, vieses e manipulações? Por quê? Você acredita que estas chaves de criptogradia ou assinaturas digitais auxiliam na prevenção de riscos? De que forma?

3.4 Os cuidados quanto a possibilidade de deterioração das mídias armazenadas ocorre de forma semelhante para itens afins dentro da estrutura organizacional. (*Política de segurança – Consistência – Locais funcionais).*

De que forma ocorrem os cuidados sobre a deterioração das mídias armazenadas?

3.5 Os procedimentos para assegurar a capacidade de acesso aos dados contra perdas ocasionadas pelas futuras mudanças na tecnologia, permitem aos usuários identificar diferenças e semelhanças, interpretando e avaliando os regulamentos para limitar as perdas. (*Integridade – Comparabilidade – Avaliação de risco).*

Como são os procedimentos para garantir o acesso aos dados contra perdas ocasionadas pelas futuras mudanças tecnológicas? Esses procedimentos permitem a comparabilidade das informações? Você acredita que estes procedimentos conseguem limitar as perdas?

3.6 O dado pode ser recuperado de forma aceitável, mais completa possível e sem omissão, por meio de monitoramento e supervisão contínua dos processos. (*Autenticidade – Integridade – Risco).*

O dado pode ser recuperado de forma aceitável, mais completa possível e sem omissão? De que forma? Existe algum monitoramento e supervisão dos processos de recuperação? Como ocorre?

3.7 A destruição apropriada dos registros, caso não sejam mais necessários à organização, ocorre com cautela cumprindo normas reguladoras no ambiente interno e externo. (*Políticas de segurança – Prudência ou conservadorismo – Conformidade).*

Como ocorre a destruição dos registros, caso não sejam mais apropriados para a organização?

3.8 A emissão de diretrizes gerais para retenção, armazenamento, tratamento e disposição de registro de informações é capaz de predizer resultados futuros por meio de normas reguladoras no ambiente interno e externo. (*Política de segurança – Preditiva-Conformidade).*

A organização emite diretrizes para armazenamento, retenção, tratamento e disposição de registros de informações? Como ocorre?

3.9 A programação para retenção, precisa identificar os registros essenciais e o período que cada um deve ser mantido de forma disponível e acessível aos usuários. (*Confiabilidade – Disponibilidade – Acessibilidade).*

Como foram definidas a guarda de registros essenciais de processo e registros contábeis, bem como os respectivos períodos?

3.10 A manutenção de um inventário das fontes de informações-chave ocorre em tempo hábil permitindo o acesso às informações para a tomada de decisão. (*Disponibilidade – Transparência – Acessibilidade).*

Como as informações-chaves de diferentes sistemas são mantidos/armazenados, elas são transportadas a uma base de dados gerencial? Como?

De que forma você acha que essas práticas podem contribuir para a conformidade?

---

4. Proteção e privacidade de informações de identificação pessoal

4.1 A política de privacidade e proteção de dados da organização é relevante, pois permite interpretar e avaliar os regulamentos para limitar as perdas. (*Confidencialidade – Relevância – Avaliação de risco).*

Existe uma política de privacidade e proteção de dados da organização? Como você considera essa política? Como a mesma é atualizada?

4.2 A comunicação da política de privacidade e proteção de dados a todas as pessoas envolvidas no processo é exposta de forma mais compreensível possível ao usuário, possibilitando a construção de uma boa imagem perante os seus *stakeholders*. (*Disponibilidade – Compreensibilidade – Reputação corporativa).*

Como ocorre a divulgação dessa política aos funcionários/envolvidos no processo? Os *stakeholders* conseguem perceber isso? Como?

4.3 Existe uma pessoa responsável (*privacy officer*) que tem a função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos a serem seguidos. Essas orientações devem ser expostas de forma compreensível ao usuário, possibilitando um padrão de excelência operacional percebida pelos *stakeholders*. (*Políticas de segurança – Compreensibilidade – Criação de valor).*

Existe uma pessoa responsável que tem a função de fornecer orientações aos gestores e usuários sobre as suas responsabilidades individuais e procedimentos a serem seguidos?

De que forma você acha que essas práticas podem contribuir para a conformidade?

---

5. Regulamentação de controles de criptografia

5.1 As restrições quanto ao uso de criptografia ocorrem com cautela de acordo com o cumprimento de normas reguladoras internas. (*Confidencialidade – Prudência ou conservadorismo – Conformidade).*

Qual o nível de criptografia para proteger a informação? Existem níveis diferentes conforme os tipos de sistemas?

5.2 A assessoria jurídica garante a conformidade com as legislações e regulamentações possibilitando a informação livre de erros, vieses e manipulações por meio do cumprimento de normas internas e externas. (*Conformidade – Representação fidedigna – Conformidade).*

De que forma a assessoria jurídica garante a conformidade com as legislações e regulamentações? Você acredita que isso possibilita que a informação seja livre de erros, vieses e manipulações? Por quê?

De que forma você acha que essas práticas podem contribuir para a conformidade?

6. Análise crítica independente da SI

6.1 A análise crítica da segurança da informação é iniciada pela direção de forma confiável para que o usuário aceite a informação e a utilize, construindo uma boa imagem perante os *stakeholders*. (*Política de segurança – Confiabilidade – Reputação corporativa).*

A análise crítica da segurança da informação é iniciada pela direção? De que forma? Isso é percebido pelos funcionários e até pelos *stakeholders*? De que forma?

6.2 A análise crítica inclui a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação evidenciando suas diferenças e semelhanças para a busca de excelência operacional percebida pelos *stakeholders*. (*Política de segurança – Comparabilidade – Criação de valor).*

Como é feita a avaliação de oportunidades para melhorar a segurança da informação? Como os funcionários e *stakeholders* conseguem perceber?

6.3 A análise crítica inclui política e objetivos de controle relevantes, capazes de fazer a diferença na gestão preventiva de riscos, monitoramento e supervisão contínua dos processos. (*Política de segurança – Relevância – Risco).*

Você acredita que essa auditoria é capaz de fazer a diferença na gestão preventiva de riscos, monitoramento e supervisão dos processos? Por quê?

6.4 A análise crítica é executada por pessoas independentes (ex: auditoria interna, gerente independente ou uma organização externa especializada em tais análises críticas), refletindo de fato o que ocorreu independente de um contrato. Deve fornecer evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever. (*Política de segurança- Primazia da essência sobre a forma – Legitimidade).*

Quem executa a análise crítica (ex: auditoria interna, gerente independente ou uma organização externa especializada em tais análises críticas)? Como ele fornece evidências aos stakeholders que está cumprindo com seu dever? Consequentemente isso ocorre na informação contábil evidenciada?

6.5 Os resultados da análise crítica independente são registrados e relatados à direção, de forma neutra não havendo viés de resultado por meio de informações úteis aos usuários permitindo um clima de confiança. (*Integridade – Neutralidade – Transparência).*

Os resultados da análise crítica independente são registrados e relatados à direção? Como é feito? Esses resultados refletem/proporcionam a transparência das informações? De que forma?

6.6 A direção efetua ações corretivas quando os resultados da análise crítica forem inadequados ou não conforme pela segurança da informação, para garantir a confiança da informação e cumprir com obrigações de suas responsabilidades. (*Conformidade – Confiabilidade – Responsabilidade).*

Como a direção efetua ações corretivas quando os resultados da análise crítica forem inadequados ou não conforme?

De que forma você acha que essas práticas podem contribuir para a conformidade?

7. Conformidade com as políticas e proced. SI

7.1 Os gestores identificam as causas quando há qualquer não conformidade, evidenciando as diferenças e semelhanças, por meio de um comportamento ético e moral. (*Autenticidade – Comparabilidade – Ética).*

Os gestores conseguem identificar as causas quando há qualquer não conformidade do tipo comportamental? Como ocorre essa identificação?

7.2 Os gestores implementam ações corretivas após a detecção da não conformidade de forma mais completa possível, sem omissão de algum fato relevante, atuando com responsabilidade pelas ações próprias ou dos outros. (*Integridade – Integridade – Responsabilidade).*

Como ocorre a implementação de ações corretivas após a detecção da não conformidade?

7.3 Os gestores analisam criticamente as ações corretivas tomadas para predizer resultados futuros, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa, cumprindo com seu dever. (*Conformidade – Preditiva – Legitimidade).*

Você acredita que essas análises conseguem predizer resultados futuros? Os *stakeholders* conseguem perceber? De que forma?

7.4 Os resultados das análises críticas e das ações corretivas pelos gestores são registradas e mantidas mediante informações íntegras e tempestivas de acordo com as normas reguladoras internas e externas. (*Disponibilidade – Oportunidade – Conformidade).*

Elas são registradas e mantidas as análises críticas? As informações são tempestivas e íntegras?

7.5 Os gestores relatam os resultados para as pessoas que estão efetuando a análise crítica independente, identificando as diferenças e semelhanças das informações permitindo um clima de confiança. (*Confiabilidade – Comparabilidade – Transparência).*

Os gestores relatam os resultados para as pessoas que estão efetuando a análise crítica independente? Como ocorre?

De que forma você acha que essas práticas podem contribuir para a conformidade?

8. Análise crítica da conformidade técnica

8.1 A verificação de conformidade técnica deve ter apoio de uma ferramenta automática para a interpretação do especialista técnico, proporcionando um consenso, interpretação e avaliação de regulamentos para limitar as perdas. (*Confiabilidade – Verificabilidade – Avaliação de risco).*

Existe apoio de uma ferramenta automática para ajudar na interpretação do especialista técnico? Como é essa ferramenta? Você acredita que ela auxilia a limitar as perdas? De que forma?

8.2 Os testes de invasão ou avaliações de vulnerabilidades são planejados, documentados e repetidos quando incertezas estiverem envolvidas, para prevenir riscos, monitorando e supervisionando continuamente os processos operacionais. (*Autenticidade – Prudência ou Conservadorismo – Risco).*

Como ocorrem os testes de invasão ou avaliação de vulnerabilidades?

8.3 A verificação de conformidade técnica somente é executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas, de forma a garantir a informação mais completa e sem omissão de algum fato relevante, fornecendo evidências aos *stakeholders* sobre o atendimento de uma expectativa. (*Confidencialidade - Integridade – Legitimidade).*

A verificação de conformidade somente é executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas?

De que forma você acha que essas práticas podem contribuir para a conformidade?